Online ISSN : 0975-4172
Print ISSN : 0975-4350

Global Journal

of Computer Science and Technology

Public Auditing System

Virtual Routing Topologies

Highlights

Design Landing-Elastic

MANET Routing Attacks

Discovering Thoughts, Inventing Future

VOLUME 13 ISSUE S1 VERSION 1.0

Global Journal of Computer Science and Technology:
Special

Global Journal of Computer Science and Technology: Special

Volume 13 Issue 1 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals Inc., Headquarters Corporate Office,
Cambridge Office Center, II Canal Park, Floor No.
5th, ***Cambridge (Massachusetts)***, Pin: MA 02141
United States
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Association of Research, Marsh Road,
Rainham, Essex, London RM13 8EU
United Kingdom.

Packaging & Continental Dispatching

Global Journals, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investers@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Editorial Board Members (HON.)

Dr. Bart Lambrecht
Director of Research in Accounting and FinanceProfessor of Finance
Lancaster University Management School
BA (Antwerp); MPhil, MA, PhD (Cambridge)

Dr. Carlos García Pont
Associate Professor of Marketing
IESE Business School, University of Navarra
Doctor of Philosophy (Management), Massachusetts Institute of Technology (MIT)
Master in Business Administration, IESE, University of Navarra
Degree in Industrial Engineering, Universitat Politècnica de Catalunya

Dr. Fotini Labropulu
Mathematics - Luther College
University of ReginaPh.D., M.Sc. in Mathematics
B.A. (Honors) in Mathematics
University of Windso

Dr. Lynn Lim
Reader in Business and Marketing
Roehampton University, London
BCom, PGDip, MBA (Distinction), PhD, FHEA

Dr. Mihaly Mezei
ASSOCIATE PROFESSOR
Department of Structural and Chemical Biology, Mount Sinai School of Medical Center
Ph.D., Etvs Lornd University
Postdoctoral Training,
New York University

Dr. Söhnke M. Bartram
Department of Accounting and FinanceLancaster University Management SchoolPh.D. (WHU Koblenz)
MBA/BBA (University of Saarbrücken)

Dr. Miguel Angel Ariño
Professor of Decision Sciences
IESE Business School
Barcelona, Spain (Universidad de Navarra)
CEIBS (China Europe International Business School).
Beijing, Shanghai and Shenzhen
Ph.D. in Mathematics
University of Barcelona
BA in Mathematics (Licenciatura)
University of Barcelona

Philip G. Moscoso
Technology and Operations Management
IESE Business School, University of Navarra
Ph.D in Industrial Engineering and Management, ETH Zurich
M.Sc. in Chemical Engineering, ETH Zurich

Dr. Sanjay Dixit, M.D.
Director, EP Laboratories, Philadelphia VA Medical Center
Cardiovascular Medicine - Cardiac Arrhythmia
Univ of Penn School of Medicine

Dr. Han-Xiang Deng
MD., Ph.D
Associate Professor and Research Department Division of Neuromuscular Medicine
Davee Department of Neurology and Clinical NeuroscienceNorthwestern University
Feinberg School of Medicine

President Editor (HON.)

Chief Author (HON.)

Dean & Editor-in-Chief (HON.)

Contents of the Volume

i. Copyright Notice
ii. Editorial Board Members
iii. Chief Author and Dean
iv. Table of Contents
v. From the Chief Editor's Desk
vi. Research and Review Papers

1. Different Models for MANET Routing Attacks. *1-7*
2. Enhancement of Secure and Dependable Storage Services and Security using Third Party Auditing. *9-15*
3. Virtual Routing Topologies for Flexible Traffic Engineering System. *17-20*
4. Semantic Approach to Discover Topic Over Mail Data. *21-25*
5. Survey on Defense against Insider Misuse Attacks in the Cloud. *27-31*
6. Public Auditing System of Data Storage Securing Nature in Cloud Computing. *33-37*
7. Design and Analysis of Leaf Spring. *39-43*
8. Dynamic Simulation of Transport Aircraft 3D Design Landing-Elastic Leg Shock Absorb ER Loads. *45-49*
9. Verification of Storage Integraty using PDP Technique. *51-55*
10. Economical Efficient for High Scalable Applications. *57-62*
11. An efficient Operations and Management Challenges of Next Generation Network (NGN). *63-70*

vii. Auxiliary Memberships
viii. Process of Submission of Research Paper
ix. Preferred Author Guidelines
x. Index

Different Models for MANET Routing Attacks

Yuvaraj Kawale [α] & A. Raghavendra Rao [σ]

Abstract - **Mobile ad-hoc networks are becoming ever more popular due to their flexibility, low cost, and ease of deployment. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET Early proposed routing protocols were not designed to operate in the presence of attackers. There have been many subsequent attempts to secure these protocols, each with its own advantages and disadvantages. Even though there exist several intrusions response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or native fuzzy response decisions. To allow for a comparison of these secure protocols, a single common attacker model is needed. Our first contribution in this work is to develop a comprehensive attacker model categorizing attackers based on their capabilities. This is in contrast to the existing models which seek to categorize attacks and then map that categorization back onto the attackers. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and native fuzzy responses could lead to uncertainty in countering routing attacks in MANET. Our second contribution is an analysis of the SAODV routing protocol using our new model, which demonstrates the structured approach inherent in our model and its benefits compared to existing work.**

I. Introduction

Mobile ad-hoc networks (MANETs) allow for wireless devices to form a network without the need for central infrastructure. While the lack of need for infrastructure allows the network to be very flexible, it also makes routing a critical concern in the network. The original proposals for MANET routing such as DSR, DSDV, and AODV did not take security into consideration. As a result, many attacks have been found which can disrupt the functioning of a MANET. Subsequent protocol proposals were designed to address one or more of these attacks, yet no protocol has proven secure against all attackers In order to allow for an accurate comparison of the security properties of these proposals, a common attacker model is necessary which allows for proper evaluation.

Unfortunately, no suitable model has yet been developed. Instead, authors analyze their protocol in a scenario of their choice with restrictions designed to ease their proof of security. These models are typically developed by looking at the attack or attacks under consideration and trying to categorize attackers based on the characteristics of these attacks while placing topological restrictions on the network.

Due to this, unforeseen vulnerabilities can arise when the protocol is applied to real-world scenarios that cannot be molded to fit the topological constraints. In addition to bordering on contrived, each model uses a different set of restrictions, considers different topologies, or addresses different attacks. This makes accurate comparison of protocols and their security properties impossible. In contrast, developing models starting from the attackers' capabilities removes the topological constraints and the resultant overlooked networks that can present a new vulner ability. In fact, working from attacker capabilities to attacks is not only topology-agnostic, but also protocol-agnostic . In addition, once attackers are categorized by their capabilities, specific attacks can be mapped to the categories of attackers with sufficient capabilities to perform such attacks.

Similarly, the necessary capabilities for performing a specific attack can be determined by comparing categories of attackers that can and cannot perform the attack. In this work, we use this alternative approach to develop a novel attacker model focusing on categorizing attacker capabilities. To the best of our knowledge, this is the first attacker model of this form for MANET routing. Our new model allows for simplified determination of necessary and sufficient capabilities for performing specific attacks. In addition, due to the complete coverage of our model, real-world scenarios are included in the analysis, ensuring that vulnerabilities will be found during analysis and thus before deployment. Our proposed model is both topology- and protocol-agnostic. As such it allows for comparison of various protocols in one common model. Finally, the ability to combine our model with BAN logic or other formalization frameworks allows for a structured, comprehensive analysis of protocol security. In addition to our first main contribution of the new attacker model, our second main contribution is an example application of our new model to the SAODV protocol, showing how our structured approach exposes a serious, though previously known vulnerability automatically during analysis. Outline: In Section 2 we first discuss existing attacker models and their attack-based approach. Then, we focus on our first contribution, a new attacker model developed with the capabilities-based approach. We detail the attacker's communication and computation capabilities as well as the application of our model. Section 3 is our second main contribution, an example

Author α : M.Tech CSE Dept, ASRA Hyderabad.
E-mail : raj.yuvi9@gmail.com
Author σ : M.Tech (CSE), Associate Professor, Hyderabad.
E-mail : raghavamay15@gmail.com

application of our model to analyze the security mechanism of hash chains as used in the SAODV routing protocol.

MOBILE Ad hoc Networks (MANET) are utilized to set up wireless communication in improvised environments without a predefined infrastructure or centralized administration. Therefore, MANET has been normally deployed in adverse and hostile environments where central authority point is not necessary. Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Furthermore, each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks.

Several work addressed the intrusion response actions in MANET by isolating uncooperative nodes based on the node reputation derived from their behaviors. Such a simple response against malicious nodes often neglects possible negative side effects involved with the response actions. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated.

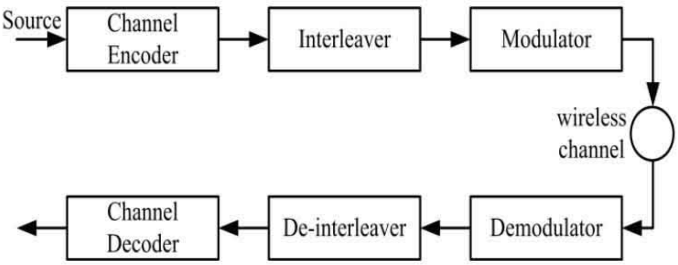
II. Risk Aware Response Mechanism Overview

a) Network System

We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in uncast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using preshared pair wise keys or asymmetric cryptography.

b) Real Time Packet Classification

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved, and decoded, to recover the original packet m.



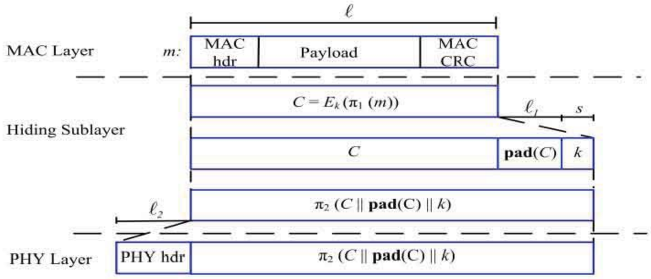
Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

c) Selective Jamming System

We illustrate the impact of selective jamming attacks on the network performance. implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block.

d) Strong Hiding Commitment Scheme (SHCS)

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.

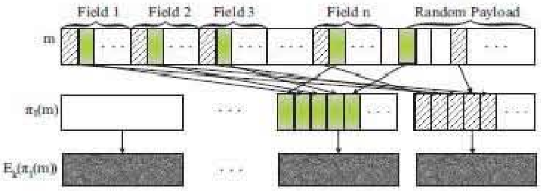


The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header Information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver.

e) Cryptographic Puzzle Hiding Scheme (CPHS)

We present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead.

We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.



Application of permutation π_1 on packet m.

III. Development Environment

How does the Java API support all of these kinds of programs? With packages of software components that provide a wide range of functionality. The core API is the API included in every full implementation of the Java platform. The core API gives you the following features:

a) The Essentials

Objects, strings, threads, numbers, input and output, data structures, system properties, date and time, and so on.

b) Applets

The set of conventions used by Java applets.

c) Networking

URLs, TCP and UDP sockets, and IP addresses.

d) Internationalization

Help for writing programs that can be localized for users worldwide. Programs can automatically adapt to specific locales and be displayed in the appropriate language.

e) Security

Both low-level and high-level, including electronic signatures, public/private key management, access control and certificates.

f) Software Components

Known as JavaBeans, can plug into existing component architectures such as Microsoft's OLE/COM/Active-X architecture, OpenDoc and Netscape's Live Connect.

g) Object Serialization

Allows lightweight persistence and communication via Remote Method Invocation (RMI).

h) Java Database Connectivity (JDBC)

Provides uniform access to a wide range of relational databases. Java not only has a core API, but also standard extensions. The standard extensions define APIs for 3D, servers, collaboration, telephony, speech, animation, and more.

i) How Will Java Change My Life?

Java is likely to make your programs better and requires less effort than other languages. We believe that Java will help you do the following:

i. *Get started quickly*

Although Java is a powerful object-oriented language, it's easy to learn, especially for programmers already familiar with C or C++.

ii. *Write less code*

Comparisons of program metrics (class counts, method counts, and so on) suggest that a program written in Java can be four times smaller than the same program in C++.

iii. *Write better code*

The Java language encourages good coding practices, and its garbage collection helps you avoid memory leaks. Java's object orientation, its JavaBeans component architecture, and its wide-ranging, easily extendible API let you reuse other people's tested code and introduce fewer bugs.

iv. *Develop programs faster*

Your development time may be as much as twice as fast versus writing the same program in C++. Why? You write fewer lines of code with Java and Java is a simpler programming language than C++.

v. *Avoid platform dependencies with 100% Pure Java*

You can keep your program portable by following the purity tips mentioned throughout this book and avoiding the use of libraries written in other languages.

vi. *Write once, run anywhere*

Because 100% Pure Java programs are compiled into machine-independent byte codes, they run consistently on any Java platform.

vii. *Distribute software more easily*

You can upgrade applets easily from a central server. Applets take advantage of the Java feature of allowing new classes to be loaded "on the fly," without recompiling the entire program.

We explore the java.net package, which provides support for networking. Its creators have called Java "programming for the Internet." These networking classes encapsulate the "socket" paradigm pioneered in the Berkeley Software Distribution (BSD) from the University of California at Berkeley.

IV. Related Work

Intrusion detection and response in MANET. Some research efforts have been made to seek preventive solutions for protecting the routing protocols in MANET. Although these approaches can prevent unauthorized nodes from joining the network, they introduce a significant overhead for key exchange and verification with the limited intrusion elimination. Besides, prevention-based techniques are less helpful to cope with malicious insiders who possess the legitimate credentials to communicate in the network. Numerous IDSs for MANET have been recently introduced. Due to the nature of MANET, most IDS are structured to be distributed and have a cooperative architecture. Similar to signature-based and anomaly based IDS models for the wired network; IDSs for MANET use specification-based or statistics-based approaches. Specification-based approaches, such as DEMEM monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. On the other hand, statistics-based approaches, such as Watchdog compare network activities with normal behavior patterns, which result in higher false positives rate than specification-based ones. Because of the existence of false positives in both MANET IDS models, intrusion alerts from these systems always accompany with alert confidence, which indicates the possibility of attack occurrence. Intrusion response system (IRS) for MANET is inspired by MANET IDS. In malicious nodes are isolated based on their reputations. Their work fails to take advantage of IDS alerts and simple isolation may cause unexpected network partition. Wang et al. brought the concept of cost-sensitive intrusion response which considers topology dependency and attack damage. The advantage of our solution is to integrate evidences from IDS, local routing table with expert knowledge, and countermeasures with a mathematical reasoning approach. Risk-aware approaches. When it comes to make response decisions there always exists inherent uncertainty which leads to unpredictable risk, especially in security and intelligence arena. Risk-aware approaches are introduced to tackle this problem by balancing action benefits and damage trade-offs in a quantified way. Cheng et al. presented a fuzzy logic control model for adaptive risk-based access control. Teo et al. applied dynamic risk-aware mechanism to determine whether an access to the network should be denied or permitted. However, risk assessment is still a nontrivial challenging problem due to its involvements of subjective knowledge, objective evidence, and logical reasoning. Wang et al. proposed a nai¨ve fuzzy cost-sensitive intrusion response solution for MANET. Their cost model took subjective knowledge and objective evidence into account but omitted a seamless combination of two properties with logical reasoning. Mu et al. adopted Dempster-Shafer theory to measure the risk of attacks and responses. However, as identified their model with Dempster's rule treats evidences equally without differentiating them from each other. To address this limitation, we propose a new Dempster's rule of combination with a notion of importance factors in D-S evidence model.

a) *Attacks on Ad hoc Networks*

An ad hoc network is a type of wireless local area network (WLAN) that is primarily characterized as dynamic and infrastructure less. Nodes in an ad hoc network have to compensate for the lack of infrastructure by cooperating in key network functionalities such as routing. Each node is assumed to function as a router for its neighbors' traffic to allow for multi-hop communication. The need for node cooperation as a key to network survival is a unique feature of ad hoc networks. Other networks, such as infrastructure-based WLANs and wire line networks, rely on existing infrastructure and special-purpose hardware to provide key network functionalities such as routing. Previous work in surveyed the security issues in ad hoc networks indicating that the significance of node cooperation in ad hoc networks makes network survival particularly sensitive to insider node behavior, making it an important security consideration. The threat model identifies and classifies types of node misbehavior in ad hoc networks into four different types: failed nodes, badly failed nodes, selfish nodes, and malicious nodes. These four classes can be differentiated with respect to the node's intent and action. A failed node exhibits unintentional passive behavior, where it is unable to participate in cooperation-based functionalities, due to power failures, for example. A badly failed node, on the other hand, indicates unintentional active behavior, where a node may inadvertently advertise inactive routes or unnecessarily overload the network with routing updates. Selfishness is intentional passive misbehavior, where a node chooses not to fully participate in the packet forwarding functionality to conserve its resources. Selfish nodes are motivated only by their self-interest in conserving their resources and may drop some or all packets forwarded through them accordingly. Selfish nodes do not collude with each other or exert additional effort to camouflage their behavior, such as slander attacks. Finally, maliciousness is intentional active misbehavior, where a node's aim is to deliberately disrupt network operations. Malicious nodes may attack the link layer, taking advantage of the cooperative nature of the medium access control (MAC) protocol. The protocol requires each pair of communicating nodes to seek a unanimous promise from all other nodes within range to have an exclusive access to the channel. This characteristic is exploited in a number of denial-of-service (DoS) attacks including collision attacks and virtual jamming attacks. In a collision attack, a malicious node ignores the MAC protocol specifications by accessing the medium when other nodes within range are transmitting or receiving data, which causes collisions.

b) Proposed Solutions

Previous work noted the importance of securing ad hoc networks against attacks such as the ones. To address the problem of node misbehavior in ad hoc networks, three classes of solutions have been proposed: secure routing protocols, cooperation incentives, and node behavior evaluation.

i. *Secure Routing Protocols*

The merit of this class of solutions is to secure the establishment and maintenance of routes in routing protocols such as Ad hoc On-Demand Distance Vector Routing (AODV) and Dynamic Source Routing (DSR) against tampering. The attack model classifies misbehavior on the routing functionality into passive and active attackers. A passive attacker may eavesdrop on the network, which is a threat to privacy and anonymity. An active attacker may inject incorrect routing information into the network to cause routing disruption by creating routing loops, black holes, greyholes, or even partitioning the network. An active attacker may also attempt to consume resources belonging to other nodes by injecting extra packets in the network, consuming bandwidth and other nodes' energy. ARIADNE is introduced in to protect DSR against active attacks using TESLA. Any node within the established route must meet the predetermined trust level. A protocol is introduced to protect route discovery against fabricated, compromised, or replayed routing control packets. This protocol assumes a security association exists between the source and destination nodes only and does not make any assumption about intermediate nodes (they may exhibit malicious behavior). The scheme may fail in the presence of colluding nodes. In general, securing routing protocols can protect the network against malicious misbehavior at the network layer only, in particular with respect to route discovery and maintenance. It does not protect the network against selfish misbehavior at any layer (including the network layer) or malicious misbehavior at layers other than the network layer.

ii. *Byzantine Fault Tolerance Techniques*

The Byzantine Generals Problem is an agreement problem in which a group of generals must decide independently but unanimously whether or not to attack the army of their enemy. The generals are geographically separated. Hence, they must communicate with each other using message in order to unanimously decide whether to attack or not. The problem complication stems from the assumption that some traitors may be present amongst the generals and may attempt to corrupt the generals' decision. For example, the traitors may forge messages to trick other generals into making a decision that is not consistent with their desires or that of others, or confusing some generals so that conflicting decisions are made (i.e. some generals attack and some do not). The requirements for a solution to the problem is that all loyal generals decide upon the same plan of action (i.e. attack or not) and that a small number of traitors cannot corrupt a unanimous decision by the generals.

iii. *Cooperation Incentives*

This class of solutions applies to nodes that are rational (i.e. nodes that adopt the behavior that benefits them most). The goal of this class of solutions is to provide incentives for nodes to cooperate in such a way that rational nodes lose if they do not cooperate. In an environment where nodes are autonomous, a node's cooperation level in key network functionalities is influenced by factors like energy consumption. This is shown in , where node cooperation in ad hoc networks is studied assuming that nodes' actions are strictly determined by self-interest and that each node has a minimum lifetime constraint. Credit based systems have been proposed to incentivize nodes to cooperate in packet forwarding by offering them payments in return. Every time a node forwards a packet on behalf of another node it receives a payment from that node. Nodes are also charged when they request others to forward packets on their behalf. For a node to be able to pay others it must have enough credit, and it can obtain credit by forwarding other's packets, SPRITE, a credit-based system is introduced. A node loses credit for all packets where it is the source and gains credit when it routes packets for other nodes. This system assumes a centralized server that accounts for all packets received, transmitted, and dropped in the network and takes care of making payments to nodes for their forwarding services and collecting payments from nodes that request forwarding services. A node using this strategy will initially cooperate, and then respond in kind to other nodes' actions. The node cooperates with other nodes that were previously cooperative, but does not cooperate with others that were not. Recent work has shown that the threat of retaliation may be effective as an incentive for node cooperation. Mechanism design is a branch of game theory that studies the design of incentives for rational nodes to act in a manner that is conducive to reaching the outcome desired by the designer. Typically, each user has a utility that may be different from the overall network utility.

iv. *Behavior Assessment*

The main goal of this class of solutions is to evaluate other nodes' behavior and build a reputation for each accordingly. This reputation can then be used to build trust in other nodes, make decisions about which nodes to interaction with, and possibly punish a node when needed. Hence, systems that fall under this class of solutions are commonly known as reputation management systems. The goal of a reputation management system in ad hoc networks is to evaluate node behavior, identify misbehaving nodes, and appropriately react to their misbehavior. Reputation nature distinguishes a reputation according to the nature of the entity it is associated with (e.g. a person, a group of people, a product, a service, an event, etc.).

Reputation role identifies the roles of the entities that participate in formation and propagation of reputation. Mainly, these entities are the evaluator, the target, the beneficiaries, and the propagators. The evaluator evaluates the behavior of a target and identifies its reputation accordingly, the beneficiaries are the entities to whom the evaluation of the target is valuable, and the propagators are the ones that propagate reputation information about a target to other entities. Information source of a reputation identifies the source of information used for evaluation. We call such a metric the evaluation metric. Reputation management systems rely on two types of evaluation metrics. The authors develop a model to stimulate cooperation in autonomous ad hoc networks in the presence of selfish and malicious nodes. In an approach that mixes between a reputation-based system and a payment-based system is introduced. Nodes monitor and evaluate their neighbors' behavior. Through a localized collaborative approach, credit is issued to nodes whose neighbors agree are cooperative. Once misbehaving nodes are detected by the majority of their neighbors, they are issued no credit and hence isolated from the network. In a sequential probability ratio test based algorithm was introduced to detect uncooperative behavior at the MAC layer in ad hoc networks. The problem of misbehavior at the MAC layer is introduced and formulated as a min max robust sequential detection problem.

c) *Evaluation Metrics for Reputation Management Systems*

In this section we discuss the evaluation metrics used to assess the performance of reputation management systems. We classify the performance metrics used to evaluate reputation management systems into efficiency metrics and effectiveness metrics. Efficiency metrics measure the impact of the reputation management system on the performance of the network. Reputation management systems may require exchange of control information amongst nodes (e.g. information used by second-hand metrics). They also perform reputation related tasks (e.g. evaluation of node behavior, isolation of misbehaving nodes) and may store reputation related information. This results in communication, computational, and storage overhead which may impact node as well as network performance. On the other hand, effectiveness metrics measure the ability of a reputation management system to reduce the impact of misbehavior as well as its accuracy in detecting misbehaving nodes. In most cases, the effectiveness as well as the efficiency of evaluation metrics is only defined qualitatively.

V. Conclusion

In this paper we have proposed a risk-aware response solution for mitigating MANET routing attacks and a novel approach to modeling attackers for ad-hoc routing protocol analysis. We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Our new model looks at attacker capabilities rather than network topology and specific attack characteristics. In doing so, our approach considered the potential damages of attacks and countermeasures and for better comparison of the security properties of existing routing protocols, as well as easier, more structured analysis of protocols developed in the future. Extensive future work remains to be done including further exploring the universal implications of specific attacker capabilities, categorizing known attacks based on the minimum attacker capabilities required, analysis of additional existing protocols, and expression of the security properties of these protocols in our model for comparative purposes Based on the promising results obtained through these experiments, we would further seek more systematic way to accommodate node reputation and attack frequency in our adaptive decision model.

References Références Referencias

1. Y. Sun, W. Yu, Z. Han, and K. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.
2. M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, "Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks," IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719, May 2010.
3. P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control," Proc. 28th IEEE Symp. Security and Privacy, 2007.
4. S. Wang, C. Tseng, K. Levitt, and M. Bishop, "Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks," Proc. 10th Int'l Symp. Recent Advances in Intrusion Detection.
5. G. Shafer, A Mathematical Theory of Evidence. Princeton Univ., 1976. [6] L. Sun, R. Srivastava, and T. Mock, "An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions," J. Management Information Systems, vol. 22, no. 4, pp. 109-142, 2006.
6. C. Mu, X. Li, H. Huang, and S. Tian, "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," Proc. 13th European Symp. Research in Computer Security (ESORICS '08), pp. 35-48, 2008.
7. K. Sentz and S. Ferson, "Combination of Evidence in Dempster- Shafer Theory," technical report, Sandia Nat'l Laboratories, 2002.
8. L. Zadeh, "Review of a Mathematical Theory of Evidence," AI Magazine, vol. 5, no. 3, p. 81, 1984.
9. R. Yager, "On the Dempster-Shafer Framework and New Combination Rules_1," Information Sciences, vol. 41, no. 2, pp. 93-137, 1987.
10. H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, "Sensor Fusion Using Dempster-Shafer Theory," Proc. IEEE Instrumentation and Measurement Technology Conf., vol. 1, pp. 7-12, 2002.
11. T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol," Network Working Group, 2003.
12. C. Perkins, E. Belding-Royer, and S. Das, "Ad Hoc On-Demand Distance Vector Routing," Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.
13. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks," IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.
14. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28- 39, May/June 2004.
15. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A Survey of Routing Attacks in Mobile Ad Hoc Networks," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.
16. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315, 2003.
17. M. Yamada and M. Kudo, "Combination of Weak Evidences by D-S Theory for Person Recognition," Knowledge-Based Intelligent Information and Engineering Systems, pp. 1065-1071, Springer, 2004.
18. K. Fall and K. Varadhan, "The NS Manual," 2010.
19. F. Ros, "UM-OLSR Implementation (version 0.8.8) for NS2," 2007.
20. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, no. 1, pp. 21-38, 2005.
21. B. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02), pp. 78-88, 2002.
22. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, vol. 1, no. 1, pp. 175-192, 2003.
23. B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An On-Demand Secure Byzantine Resilient Routing Protocol for Wireless Ad Hoc Networks," ACM Trans. Information and System Security, vol. 10, no. 4, pp. 1-35, 2008.
24. C. Tseng, S. Wang, C. Ko, and K. Levitt, "DEMEM: Distributed Evidence-Driven Message Exchange Intrusion Detection Model for Manet," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06), pp. 249-271, 2006.
25. C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt, "A Specification-Based Intrusion Detection Model for OLSR," Proc. Ninth Int'l Symp. Recent Advances in Intrusion Detection (RAID '06), pp. 330-350, 2006.
26. N. Mohammed, H. Otrok, L. Wang, M. Debbabi, and P. Bhattacharya, "Mechanism Design-Based Secure Leader Election Model for Intrusion Detection in MANET," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan./Feb. 2011.
27. J. Felix, C. Joseph, B.-S. Lee, A. Das, and B. Seet, "Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA," IEEE Trans. Dependable and Secure Computing, vol. 8, no. 2, pp. 233-245, Mar./Apr. 2011.
28. S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom, pp. 255-265, 2000.

This page is intentionally left blank

Enhancement of Secure and Dependable Storage Services and Security using Third Party Auditing

T Mahesh [α] & A. Raghavendra Rao [σ]

Abstract - **Cloud Computing is the long dreamed vision of computing as a utility, Cloud storage facilitates users to store the data remotely and enjoy the on-demand high quality cloud servers without the burden of local software and hardware systems. By outsourcing the data, users can be comforted from the burden of local data storage and maintenance. By having these many benefits, such a service is also abandon users' physical control of their outsourced data, which unavoidably posture new security risks towards the accuracy of the data in cloud. In order to address this new problem and further achieve a secure and dependable cloud storage service, we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data. The proposed design allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization, i.e., the identification of misbehaving server. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.**

I. Introduction

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data constancy. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, our scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s). Our work is among the first few ones in this field to consider distributed data storage in Cloud Computing. Our contribution can be summarized as the following three aspects:

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.
2. Unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data blocks, including: update, delete and append.
3. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

II. Problem Statement

a) *The System and Threat Model*

We consider a cloud data storage service involving three different entities, as illustrated in Fig. 1: the cloud user (U), who has large amount of data files to be stored in the cloud; the cloud server (CS), which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter.); the third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS in the sense that in most of time it behaves properly and does not deviate from the prescribed protocol execution. While providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation. We

Authors α σ : M.Tech CSE Dept, ASRA, Hyderabad.
E-mails : mahi06538@gmail.com, raghavamay15@gmail.com

assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users. However, any possible leakage of user's outsourced data towards TPA through the auditing protocol should be prohibited. Note that to achieve the audit delegation and authorize CS to respond to TPA's audits, the user can sign a certificate granting audit rights to the TPA's public key, and all audits from the TPA are Authenticated against such a certificate.

b) *Design Goals*

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee: 1) Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users; 2) Storage correctness: to ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact; 3) Privacy-preserving: to ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process; 4) Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously; 5) Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

III. System Development

a) *System Model*

User: users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations. Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems. Third Party Auditor (TPA): an optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

b) *File Retrieval and Error Recovery*

Since our layout of file matrix is systematic, the user can reconstruct the original file by downloading the data vectors from the first m servers, assuming that they return the correct response values. Notice that our verification scheme is based on random spot-checking, so the storage correctness assurance is a probabilistic one. We can guarantee the successful file retrieval with high probability. On the other hand, whenever the data corruption is detected, the comparison of pre-computed tokens and received response values can guarantee the identification of misbehaving server(s).

c) *Third Party Auditing*

As discussed in our architecture, in case the user does not have the time, feasibility or resources to perform the storage correctness verification, he can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable. However, as pointed out by the recent work, to securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy. Namely, TPA should not learn user's data content through the delegated data auditing.

d) *Cloud Operations*

i. *Update Operation*

In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, we refer this operation as data update. In other words, for all the unused tokens, the user needs to exclude every occurrence of the old data block and replace it with the new one.

ii. *Delete Operation*

Sometimes, after being stored in the cloud, certain data blocks may need to be deleted. The delete operation we are considering is a general one, in which user replaces the data block with zero or some special reserved data symbol. From this point of view, the delete operation is actually a special case of the data update operation, where the original data blocks can be replaced with zeros or some predetermined special blocks.

iii. *Append Operation*

In some cases, the user may want to increase the size of his stored data by adding blocks at the end of the data file, which we refer as data append. We anticipate that the most frequent append operation in cloud data storage is bulk append, in which the user needs to upload a large number of blocks (not a single block) at one time.

iv. *Insert Operation*

An insert operation to the data file refers to an append operation at the desired index position while maintaining the same data block structure for the whole data file, i.e., inserting a block F[j] corresponds to shifting all blocks starting with index $j + 1$ by one slot. Thus, an insert operation may affect many rows in the logical data file matrix F, and a substantial number of computations are required to renumber all the subsequent blocks as well as re-compute the challenge-response tokens. Hence, a direct insert operation is difficult to support.

IV. The Proposed Schemes

In the introduction we motivated the public auditability with achieving economies of scale for cloud computing. This section presents our public auditing scheme for cloud data storage security. We start from the overview of our public auditing system and discuss two straightforward schemes and their demerits. Then we present our main result for privacy-preserving public auditing to achieve the aforementioned design goals. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users. Finally, we discuss how to adapt our main result to support data dynamics.

a) Definitions and Framework of Public Auditing System

We follow the similar definition of previously proposed schemes in the context of remote data integrity checking and adapt the framework for our privacy-preserving public auditing system. A public auditing scheme consists of four algorithms (KeyGen, SigGen, Gen Proof, Verify Proof). KeyGen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate verification metadata, which may consist of MAC, signatures, or other related information that will be used for auditing. Gen Proof is run by the cloud server to generate a proof of data storage correctness, while Verify Proof is run by the TPA to audit the proof from the cloud server. Our public auditing system can be constructed from the above auditing scheme in two phases, Setup and Audit:

i. *Setup*

The user initializes the public and secret parameters of the system by executing KeyGen, and pre-processes the data file F by using SigGen to generate the verification metadata. The user then stores the data file F at the cloud server, delete its local copy, and publish the verification metadata to TPA for later audit. As part of pre-processing, the user may alter the data file F by expanding it or including additional metadata to be stored at server.

ii. *Audit*

The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive a response message from a function of the stored data file F by executing Gen Proof. Using the verification metadata, the TPA verifies the response via Verify Proof. Note that in our design, we do not assume any additional property on the data file, and thus regard error-correcting codes as orthogonal to our system. If the user wants to have more error-resiliency, he/she can first redundantly encode the data file and then provide us with the data file that has error-correcting codes integrated.

b) The Basic Schemes

Before giving our main result, we first start with two warm up schemes. The first one does not ensure privacy-preserving guarantee and is not as lightweight as we would like. The second one overcomes the first one, but suffers from other undesirable systematic demerits for public auditing: bounded usage and auditor state fullness, which may pose additional on-line burden to users as will be elaborated shortly. We believe the analysis of these basic schemes will lead us to our main result, which overcomes all these drawbacks.

Basic Scheme I The cloud user pre-computes MACs _i = MACsk(i||mi) of each block mi (i ∈ {1, . . . , n}), sends both the data file F and the MACs {_i}1≤i≤n onto the cloud server, and releases the secret key sk to TPA. During the Audit phase, the TPA requests from the cloud server a number of randomly selected blocks and their corresponding MACs to verify the correctness of the data file. The insight behind this approach is that auditing most of the file is much easier than the whole of it. However, this simple solution suffers from the following severe drawbacks:

1. The audit from TPA demands retrieval of users' data, which should be prohibitive because it violates the privacy-preserving guarantee;
2. Its communication and computation complexity are both linear with respect to the sampled data size, which may result in large communication overhead and time delay, especially.

When the bandwidth available between the TPA and the cloud server is limited. Basic Scheme II To avoid retrieving data from the cloud server, one may improve the above solution as follows: Before data outsourcing, the cloud user chooses s random message authentication code keys {sk_}1≤_≤s, pre-computes s MACs, {MACsk_ (F)}1≤_≤s for the whole data file F, and publishes these verification metadata to TPA. The TPA can each time reveal a secret key sk_ to the cloud server and ask for a fresh keyed MAC for comparison, thus achieving privacy-preserving auditing. However, in this method: 1) the number of times a particular data file can be audited is limited by the number of secret keys that must be a fixed priori. Once all possible secret keys are exhausted, cloud user then has to retrieve data from the server in order to re-compute and re-publish new MACs to TPA. 2) The TPA has to maintain and update state between audits, i.e., keep a track on the possessed MAC keys. Considering the potentially large number of audit delegations from multiple users, maintaining such states for TPA can be difficult and error prone. Note that another common drawback of the above basic schemes is that they can only support the case of static data, and none of them can deal with data dynamics. For the reason of brevity and clarity, our main result will focus on the static data, too. In Section 3.5, we will show how to adapt our main result to support dynamic data update.

c) The Privacy-Preserving Public Auditing Scheme

To effectively support public audit ability without having to retrieve the data blocks themselves, we resort to the homomorphic authenticator technique. Homomorphic authent-icators are unforgivable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. However, the direct adoption of these techniques is not suitable for our purposes, since the linear combination of blocks may potentially reveal user data information, thus violating the privacy-preserving guarantee. Specifically, if enough number of the linear combinations of the same blocks are collected, the TPA can simply derive the user's data content by solving a system of linear equations. Overview To achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF). With random mask, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user's data content, no matter how many linear combinations of the same set of file blocks can be collected. Meanwhile, due to the algebraic property of the homomorphic authenticator, the correctness validation of the block-authenticator pairs will not be affected by the randomness generated from a PRF, which will be shown shortly. Note that in our design, we use public key based homomorphic authenticator, specifically, the one in which is based on BLS signature, to equip the auditing protocol with public audit ability. Its flexibility in signature aggregation will further benefit us for the multitask auditing.

V. Multiple Levels Of Security

a) Virtual Private Cloud

Each VPC is a distinct, isolated network within the cloud. At creation time, an IP address range for each VPC is selected by the customer. Network traffic within each VPC is isolated from all other VPCs; therefore, multiple VPCs may use overlapping (even identical) IP address ranges without loss of this isolation. By default, VPCs have no external connectivity. Customers may create and attach an Internet Gateway, VPN Gateway, or both to establish external connectivity, subject to the controls below.

b) API

Calls to create and delete VPCs, change routing, security group, and network ACL parameters, and perform other functions are all signed by the customer's Amazon Secret Access Key, which could be either the AWS Accounts Secret Access Key or the Secret Access key of a user created with AWS IAM. Without access to the customer's Secret Access Key, Amazon VPC API calls cannot be made on the customer's behalf. In addition, API calls can be encrypted with SSL to maintain confidentiality. Amazon recommends always using SSL protected API endpoints. AWS IAM also enables a customer to further control what APIs a newly created user has permissions to call.

c) Subnets

Customers create one or more subnets within each VPC; each instance launched in the VPC is connected to one subnet. Traditional Layer 2 security attacks, including MAC spoofing and ARP spoofing, are blocked.

d) Route Tables and Routes

Each Subnet in a VPC is associated with a routing table, and all network traffic leaving a subnet is processed by the routing table to determine the destination.

e) VPN Gateway

A VPN Gateway enables private connectivity between the VPC and another network. Network traffic within each VPN Gateway is isolated from network traffic within all other VPN Gateways. Customers may establish VPN Connections to the VPN Gateway from gateway devices at the customer premise. Each connection is secured by a preshared key in conjunction with the IP address of the customer gateway device.

f) Internet Gateway

An Internet Gateway may be attached to a VPC to enable direct connectivity to Amazon S3, other AWS services and the Internet. Each instance desiring this access must either have a n Elastic IP associated with it or route traffic through a NAT instance. Additionally, network routes are configured to direct traffic to the Internet Gateway. AWS provides reference NAT AMIs that can be extended by customers to perform network logging, deep packet inspection, application layer filtering.

VI. Input Design

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded. The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.
2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.
3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow.

VII. Output Design

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system. The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

VIII. Related Work

Juels et al. described a formal "proof of irretrievability" (POR) model for ensuring the remote data integrity. Their scheme combines spot-checking and error correcting code to ensure both possession and irretrievability of files on archive service systems. Shacham et al. built on this model and constructed a random linear function based homomorphic authenticator which enables unlimited number of challenges and requires less communication overhead due to its usage of relatively small size of BLS signature. Bowers et al. proposed an improved framework for POR protocols that generalizes both Juels and Shacham's work. Later in their subsequent work, Bowers et al. extended POR model to distributed systems.

However, all these schemes are focusing on static data. The effectiveness of their schemes rests primarily on the preprocessing steps that the user conducts before outsourcing the data file F. Any change to the contents of F, even few bits, must propagate through the error-correcting code and the corresponding random shuffling process, thus introducing significant computation and communication complexity. Recently, Dodis et al. gave theoretical studies on generalized framework for different variants of existing POR work. Ateniese et al. defined the "provable data possession" (PDP) model for ensuring possession of file on untrusted storages. Their scheme utilized public key based homomorphic tags for auditing the data file. However, the pre-computation of the tags imposes heavy computation overhead that can be expensive for an entire file. In their subsequent work, Ateniese et al. described a PDP scheme that uses only symmetric key based cryptography. This method has lower-overhead than their previous scheme and allows for block updates, deletions and appends to the stored file, which has also been supported in our work. However, their scheme focuses on single server scenario and does not provide data availability guarantee against server failures, leaving both the distributed scenario and data error recovery issue unexplored. The explicit support of data dynamics has further been studied in the two recent work and. Wang et al. proposed to combine BLS based homomorphic authenticator with Markel Hash Tree to support fully data dynamics, while Erway et al. developed a skip list based scheme to enable provable data possession with fully dynamics support. The incremental cryptography work done by Bellare et al. also provides a set of cryptographic building blocks such as hash, MAC, and signature functions that may be employed for storage integrity verification while supporting dynamic operations on data. However, this branch of work falls into the traditional data integrity protection mechanism, where local copy of data has to be maintained for the verification. It is not yet clear how the work can be adapted to cloud storage scenario where users no longer have the data at local sites but still need to ensure the storage correctness efficiently in the cloud. In other related work, Curtmola et al. aimed to ensure data possession of multiple replicas across the distributed storage system. They extended the PDP scheme to cover multiple replicas without encoding each replica separately, providing guarantee that multiple copies of data are actually maintained. Lilli bridge et al. presented a P2P backup scheme in which blocks of a data file are dispersed across m + k peers using an (m, k)- erasure code. Peers can request random blocks from their backup peers and verify the integrity using separate keyed cryptographic hashes attached on each block. Their scheme can detect data loss from free-riding peers, but does not ensure all data is unchanged. Filho et al. proposed to verify data integrity using RSA-based hash to demonstrate uncheatable data possession in peerto-peer file sharing networks. However, their proposal requires exponentiation over the entire data file, which is clearly impractical for the server whenever the file is large. Shah et al. proposed allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric keyed hashes over the encrypted data to the auditor.

However, their scheme only works for encrypted files, and auditors must maintain long-term state. Schwarz et al. proposed to ensure static file integrity across multiple distributed servers, using erasure-coding and block level file integrity checks. We adopted some ideas of their distributed storage verification protocol. However, our scheme further support data dynamics and explicitly studies the problem of misbehaving server identification, while theirs did not. Very recently, Wang et al. gave a study on many existing solutions on remote data integrity checking, and discussed their pros and cons under different design scenarios of secure cloud storage services. Portions of the work presented in this paper have previously appeared as an extended abstract in. We have revised the article a lot and add more technical details as compared to. The primary improvements are as follows: Firstly, we provide the protocol extension for privacy-preserving third-party auditing, and discuss the application scenarios for cloud storage service. Secondly, we add correctness analysis of proposed storage verification design. Thirdly, we completely redo all the experiments in our performance evaluation part, which achieves significantly improved result as compared to. We also add detailed discussion on the strength of our bounded usage for protocol verifications and its comparison with state-of-the-art.

IX. Conclusion

In this paper, we examine the complications of the data stored in the cloud storage and security of the data in cloud data storage system, To achieve the affirmation of cloud data goodness and availability and accomplish the quality of dependable cloud storage service for users, we propose an adequate and formative allocated scheme with explicit dynamic data support, including block update, delete, append and insert. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data constancy. By utilizing the homomorphic token with allocated verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the allocated servers, we can almost guarantee the simultaneous identification of the misbehaving server(s). Considering the time, computation resources, and even the related online burden of users, we also provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to third-party auditors and be worry-free to use the cloud storage services. Through detailed security and extensive experiment results, we show that our scheme is highly efficient and resilient to Byzantine failure, malicious data modification attack, and even server colluding attacks.

References Références Referencias

1. C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security in cloud computing,” in Proc. of IWQoS’09, July 2009, pp. 1–9.
2. Amazon.com, “Amazon web services (aws),” Online at http://aws.amazon.com/, 2009.
3. Sun Microsystems, Inc., “Building customer trust in cloud computing with transparent security,” Online at https://www.sun.com/offers/details/suntransparency.xml, November 2009.
4. M. Arrington, “Gmail disaster: Reports of mass email deletions,” Online at http://www.techcrunch.com/2006/12/28/ Gmail-disaster reports-of-mass-email-deletions/,December 2006.
5. J.Kincaid, “Media ax/The Linkup Closes Its Doors,” Online at http://www.techcrunch.com/2008/07/10/mdiamaxthelinkup-closes-its-doors/, July 2008.
6. Amazon.com, “Amazon s3 availability event: July 20, 2008,” Online at http://status.aws.amazon.com/s3-20080720.html, July 2008.

7. S. Wilson, "Appengine outage," Online at http://www.cio-weblog.com/50226711/appengineoutage.php, June 2008.
8. B. Krebs, "Payment Processor Breach May Be Largest Ever," Online http://voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.
9. A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.
10. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.

This page is intentionally left blank

Virtual Routing Topologies for Flexible Traffic Engineering System

Ch. Roja [α] & M. Madhavi [σ]

Abstract - **Contemporary network management system is, managing traffic flow in order to avoid network bottlenecks and consecutive service interruptions are one of the major tasks performed. Accustomed the simple but forwarding and rigid routing functionalities in Internet Protocol based environments, dynamic resource management and control clarifications against high traffic conditions is still yet to be accomplish. In this article, we introduce AMPLE — An Efficient Traffic Engineering and Management system that performs robust traffic control by using more number of virtualized routing techniques. The proposed system consists of two conclusive parts: "offline link weight optimization" that takes as input from the environmental network topology and tries to produce maximum routing path redirect across more number of constructive routing topologies for distant future operation through the customized setting of link weights. Based on these different paths, "adaptive traffic control" performs inventive traffic splitting across distinctive routing topologies in reaction to the monitored network dynamics at short time period. According to our assessment with real network topologies and traffic evidence, the proposed system is able to manage almost optimally with unexpected traffic dynamics and, as such, it constitutes a new presentation for action for accomplishing better quality of service and overall network performance in Internet Protocol networks.**

I. Introduction

Mobile ad hoc network (MANET) is a group of two or terminals or nodes or more devices with an efficiency of wireless communications and networking which accomplish them able to communicate with each other without the support of any centralized system. This is an independent system in which nodes are connected by wireless links and send data to each other. As we know that there is no any centralized system so routing is done by node itself. Due to its mobility and self routing efficiency nature, there are many defects in its security. To solve the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection and anomaly-based intrusion detection. In Signature-based intrusion detection there are some earlier detected signature or patron are stored into the data base of the IDS if any distraction is found in the network by IDS it matches it with the earlier saved patron and if it is matched than IDS found attack. But if there is an attack and its patron is not in IDS database then IDS cannot be able to identify attacks. For this periodically updating of database is compulsory. To resolve this defect anomaly based IDS are invented, in which mainly the IDS accomplish the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

II. System Overview

The below figure represents an overall view of the proposed AMPLE TE system, with Offline MT-IGP Link Weight Optimization (OLWO) and Adaptive Traffic Control (ATC) completes the key components. As discussed, the final objective of OLWO is to provision offline maximum Intra-domain path difference in the routing plane, allowing the ATC component to adjust at short timescale the traffic assignment across distinctive VRTs in the forwarding plane. An important novelty is that the optimization of the MT-IGP link weights does not depend on the availability of the traffic matrix a priori, which afflicts existing offline TE solutions due to the typical inaccuracy of traffic matrix estimations. Instead, our offline link weight optimization is only based on the characteristics of the network itself, i.e. the physical topology. The computed MT-IGP link weights are configured in distinctive routers and the corresponding IGP paths within each VRT are populated in their local

Author α : M.Tech, CSE Dept, ASRA Hyderabad.
E-mail : roja.chinnam@gmail.com
Author σ : Asst. Prof., M.Tech CSE Dept, ASRA Hyderabad.
E-mail : madhavi_3101@yahoo.co.in

routing information bases (MT-RIBs). While OLWO focuses on static routing configuration in a long timescale (e.g. weekly or monthly), the ATC component provides complementary functionality to enable short timescale (e.g. hourly) control in response to the behavior of traffic that cannot be usually anticipated.

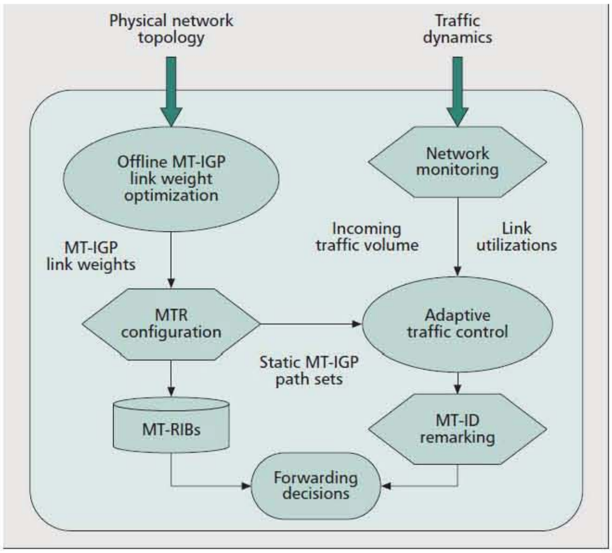


Figure 1 : AMPLE System Overview

As shown in the figure, the input for ATC includes: (1) the diverse MT-IGP paths according to the link weights computed by OLWO, and (2) monitored network and traffic data such as incoming traffic volume and link utilizations. At each short-time interval, ATC computes new traffic splitting ratio across distinctive VRTs for re-assigning traffic in an optimal way to the diverse IGP paths between each S-D pair. This functionality is handled by a centralized TE manager who has complete knowledge of the network topology and periodically gathers the up-to-date monitored traffic conditions of the operating network. These new splitting ratios are then configured by the TE manager to distinctive source PoP nodes who use this configuration for remarking the multi-topology identifiers (MT-IDs) of their locally originated traffic accordingly. The TE manager function can be realized as a dedicated server, but for robustness and resilience it can be implemented in a distributed replicated manner for avoiding the existence of a single point of failure. In the next section we present the detailed design of distinctive components in the AMPLE system.

III. Development Environment

a) Virtual Traffic Allocation

In this Module, the diverse MT-IGP paths according to the link weights computed by OLWO. Monitored network and traffic data such as incoming traffic volume and link utilizations. At each short-time interval, ATC computes a new traffic splitting ratio across individual VRTs for re-assigning traffic in an optimal way to the diverse IGP paths between each S-D pair. This functionality is handled by a centralized TE manager who has complete knowledge of the network topology and periodically gathers the up-to-date monitored traffic conditions of the operating network. These new splitting ratios are then configured by the TE manager to individual source PoP nodes, which use this configuration for remarking the multi-topology identifiers (MTIDs) of their locally originated traffic accordingly.

b) Offline Link Weight Optimization

In this module, to determine the definition of "path diversity" between PoPs for traffic engineering. Let's consider the following two scenarios of MT-IGP link weight configuration. In the first case, highly diverse paths (e.g. end-to-end disjoint ones) are available for some Pop-level S-D pairs, while for some other pairs individual paths are completely overlapping with each other across all VRTs. In the second case, none of the S-D pairs have disjoint paths, but none of them are completely overlapping either. Obviously, in the first case if any "critical" link that is shared by all paths becomes congested, its load cannot be alleviated through adjusting traffic splitting ratios at the associated sources, as their traffic will inevitably travel through this link no matter which VRT is used. Hence, our strategy targets the second scenario by achieving "balanced" path diversity across all S-D pairs.

c) Network Monitoring

In this Module, Network monitoring is responsible for collecting up-to-date traffic conditions in real-time and plays an important role for supporting the ATC operations. AMPLE adopts a hop-by-hop based monitoring mechanism that is similar to the proposal.

The basic idea is that a dedicated monitoring agent deployed at every PoP node is responsible for monitoring:

- ✓ The volume of the traffic originated by the local customers toward other PoPs (intra- PoP traffic is ignored).
- ✓ The utilization of the directly attached inter-PoP links

d) Adaptive Traffic Control

In this Module, Measure the incoming traffic volume and the network load for the current interval as compute new traffic splitting ratios at individual PoP source nodes based on the splitting ratio configuration in the previous interval, according to the newly measured traffic demand and the network load for dynamic load balancing.

IV. Brief Survey on Networks

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things are satisfied, then next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

a) *What is Wireless Networking?*

The term refers to any kind of networking that does not involve cables. It is a technique that helps entrepreneurs and telecommunications networks to save the cost of cables for networking in specific premises in their installations. The transmission system is usually implemented and administrated via radio waves where the implementation takes place at physical level.

b) *What are the Types of Wireless Connections?*

The types of networks are defined on the bases of their size (that is the number of machines), their range and the speed of data transfer.

c) *Wireless PAN - Personal Area Network Wireless Personal Area Networks*

Such networks interconnect devices in small premises usually within the reach of a person for example invisible infra red light and Bluetooth radio interconnects a headphone to a laptop by the virtue of WPAN. With the installation of Wi-Fi into customer electronic devices the Wi-Fi PANs are commonly encountered.

d) *Wireless LAN - Local Area Network*

The simplest wireless distribution method that is used for interlinking two or more devices providing a connection to wider internet through an access point. OFDM or spread-spectrum technologies give clients freedom to move within a local coverage area while remaining connected to the LAN. LAN's data transfer speed is typically 10 Mbps for Ethernet and 1 Gbps for Gigabit Ethernet. Such networks could accommodate as many as hundred or even one thousand users.

e) *Wireless MAN - Metropolitan Area Networks*

The wireless network that is used to connect at high speed multiple wireless LANs that are geographically close (situates anywhere in a few dozen kilometers). The network allows two or more nodes to communicate with each other as if they belong to the same LAN. The set up makes use of routers or switches for connecting with high-speed links such as fiber optic cables. WiMAX described as 802.16 standard by the IEEE is a type of WMAN.

f) *Wireless WAN*

WAN is the wireless network that usually covers large outdoor areas. The speed on such network depends on the cost of connection that increases with increasing distance. The technology could be used for interconnecting the branch offices of a business or public internet access system. Developed on 2.4GHz band these systems usually contain access points, base station gateways and wireless bridging relays. Their connectivity with renewable source of energy makes them stand alone systems. The most commonly available WAN is internet.

g) *Mobile Devices Networks*

The advent of smart phones has added a new dimension in telecommunications; today's telephones are not meant to converse only but to carry data.

h) *GSM - Global System for Mobile*

Communications Global System for Mobile Communications is categorized as the base station system, the operation and support system and the switching system. The mobile phone is initially connected to the base system station that establishes a connection with the operation and support station that later on connects to the switching station where the call is made to the specific user. PCS - Personal Communications Service is a radio band that is employed in South Asia and North America; the first PCS service was triggered by Sprint.

i) *D-AMPS Digital Advanced Mobile Phone Service*

Is the upgraded version of AMPS that is faded away due to technological advancements. TAN - Tiny Area Network and CANs - Campus Area Networks are two other types of networks. TAN is similar to LAN but comparatively smaller (two to three machines) where CAN resemble MAN (with limited bandwidth between each LAN network).

j) *The Utility of Wireless Networks*

The development of wireless networks is still in progress as the usage is rapidly growing. Personal communications are made easy with the advent of cell phones where radio satellites are used for networking between continents. Whether small or big, businesses uses wireless networks for fast data sharing with economical means. Sometimes compatibility issues with new devices might arise in these extremely vulnerable networks but the technology has made the uploading and the downloading of huge data a piece of cake with least maintenance cost. WEP - Wired Equivalent Privacy as well as firewalls could be used for securing the network. Wireless networks are the future of global village. For referring to security of wireless LAN networks you can refer to related articles in section below.

V. Conclusion

In this article we have introduced AMPLE, a novel TE system based on virtualized IGP routing that enables short timescale traffic control against unexpected traffic dynamics using multi topology IGP-based networks. The framework encompasses two major components, namely, Offline Link Weight

Optimization (OLWO) and Adaptive Traffic Control (ATC). The OLWO component takes the physical network topology as the input and aims to produce maximum IGP path diversity across multiple routing topologies through the optimized setting of MT-IGP link weights.

Based on these diverse paths, the ATC component performs intelligent traffic splitting adjustments across individual routing topologies in reaction to the monitored network dynamics at short timescale. As far as implementation is concerned, a dedicated traffic engineering manager is required, having a global view of the entire network conditions and being responsible for computing optimized traffic splitting ratios according to its maintained TE information base.

Our experiments based on the GEANT and Abilene networks and their real traffic traces have shown that AMPLE has a high chance of achieving near-optimal network performance with only a small number of routing topologies, although this is yet to be further verified with traffic traces data from other operational networks when available. A potential direction in our future work is to consider a holistic TE paradigm based on AMPLE, which is passable to simultaneously tackle both traffic and network dynamics, for instance network failures.

References Références Referencias

1. An adaptive traffic engineering system based on virtual routing topologies by Ning Wang University of Surrey, United Kingdom Kin Hon Ho.
2. User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.
3. Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.
4. Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.
5. Data Communications and Networking, by Behrouz A Forouzan.
6. Computer Networking: A Top-Down Approach, by James F. Kurose.
7. Operating System Concepts, by Abraham Silberschatz.
8. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
9. "The apache cassandra project," http://cassan dra.apache.org/.
10. L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.
11. N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds,".
12. Wang, N., et al.: An Overview of Routing Optimization for Internet Traffic Engineering. IEEE Communications Surveys and Tutorials (to appear, 2008).
13. Kvalbein, A., et al.: Post-Failure Routing Performance with Multiple Routing Configurations. In: Proc. IEEE INFOCOM (2007).
14. Zhang, C., et al.: On Optimal Routing with Multiple Traffic Matrices. In: Proc. IEEE INFOCOM (2005)
15. Nucci, A., et al.: IGP Link Weight Assignment for Operational Tier-1 Backbones. IEEE/ACM Transactions on Networking 15(4), 789–802 (2007).
16. Menth, M., Martin, R.: Network Resilience through Multi-topology Routing. In: Proc. International Workshop on Design of Reliable Communication Networks (DRCN) (2005).
17. The GEANT topology: http://www.geant.net/upload/pdf/GEANT_Topology_12-2004.pdf

Semantic Approach to Discover Topic over Mail Data

D. A. Kiran Kumar[α] & M. Saidi Reddy[σ]

Abstract - **Text sequences or Time stamped texts, are ever-present in real-world applications. Multiple text sequences are frequently connected to each other by distributing common topics. The correspondence between these sequences provides more significant and comprehensive clues for topic mining than those from every individual sequence. However, it is non retrieval to explore the equivalence with the existence of asynchronism among multiple sequences, i.e., documents from different sequences about the same topic may have different time stamps. In this paper, we properly addressed the problem and suggested a new algorithm based on the generative topic model. The proposed algorithm consists of two alternate steps: the first step retrieves common data from multiple sequences based on the arranged time stamps provided by the second step; the second step arranges the time stamps of the documents according to the time distribution of the topics found by the first step. We accomplish these two steps simultaneously and after number retrievals a monotonic convergence of our objective function can be extracted. The effectiveness and advantage of our approach were justified through extensive practical studies on two real data sets consisting of six research paper repositories and two news article feeds, respectively.**

I. Introduction

MORE and more text sequences are being generated in various forms, such as news streams, weblog articles, emails, instant messages, research paper archives, web forum discussion threads, and so forth. To discover valuable knowledge from a text sequence, the first step is usually to extract topics from the sequence with both semantic and temporal information, which are described by two distributions, respectively: a word distribution describing the semantics of the topic and a time distribution describing the topic's intensity over time In many real-world applications, we are facing multiple text sequences that are correlated with each other by sharing common topics. Intuitively, the interactions among these sequences could provide clues to derive more meaningful and comprehensive topics than those found by using information from each individual stream solely. The intuition was confirmed by very recent work, which utilized the temporal correlation over multiple text sequences to explore the semantic correlation among common topics. The method proposed therein relied on a fundamental assumption that different sequences are always synchronous in time, or in their own term coordinated, which means that the common topics share the same time distribution over different sequences.

However, this assumption is too strong to hold in all cases. Rather, asynchronism among multiple sequences, i.e, documents from different sequences on the same topic have different time stamps, is actually very common in practice. For instance, in news feeds, there is no guarantee that news articles covering the same topic are indexed by the same time stamps. There can be hours of delay for news agencies, days for newspapers, and even weeks for periodicals, because some sources try to provide first-hand flashes shortly after the incidents, while others provide more comprehensive reviews afterward. Another example is research paper archives, where the latest research topics are closely followed by newsletters and communications within weeks or months, then the full versions may appear in conference proceedings, which are usually published annually and at last in journals, which may sometimes take more than a year to appear after submission.

To visualize it, we have the relative frequency of the occurrences of two terms warehouse and mining, respectively, in the titles of all research papers published in SIGMOD (ACM International Conference on Management of Data), a database-related conference, and TKDE (IEEE Transactions on Knowledge and Data Engineering) from 1992 to 2006, a database-related journal. The first term identifies the topic data warehouse and the second data mining, which are two common topics shared by the two sequences. As shown in Fig. 1a, the bursts of both terms in SIGMOD are significantly earlier than those in TKDE, which suggests the presence of asynchronism between these two sequences. Thus, in this paper, we do not assume that given text sequences are always synchronous. Instead, we deal with text sequences that share common topics yet are temporally asynchronous. We apparently expect that multiple correlated sequences can facilitate topic mining by generating topics with higher quality. However, the asynchronism among sequences brings new challenges to conventional topic mining methods. If we overlook the asynchronism and apply the conventional topic mining methods directly, we are very likely to fail in identifying data mining and/or data warehouse as common topics

Author α : (M.Tech), CSE Dept, MRCET, Hyderabad.
E-mail : kiran.dingari@gmail.com
Author σ : Ph.D., CSE Dept, MRCET, Hyderabad.
E-mail : msreddy33@gmail.com

of the two sequences, since the bursts of the topics do not coincide (therefore, the relative frequency of the topical words becomes too low as compared to other words). As a contrast, after adjusting the time stamps of documents in the two sequences using our proposed method, the relative frequency of both warehouse and mining are boosted over a certain range of time, relatively. Thus, we are more likely to discover both topics from the synchronized sequences. It proves that fixing asynchronism can significantly benefit the topic discovery process. However, as desirable as it is to detect the temporal asynchronism among different sequences and to eventually synchronize them, the task is difficult without knowing the topics to which the documents belong beforehand. A native solution is to use coarse granularity of the time stamps of sequences so that the asynchronism among sequences can be smoothed out. This is obviously dissatisfactory as it may lead to unbearable loss in the temporal information of common topics and different topics would inevitably be mixed up.

A second way, shifting or scaling the time dimension manually and empirically, may not work either because the time difference of topics among different sequences can vary largely or irregularly, of which we can never have enough prior knowledge. In this paper, we target the problem of mining common topics from multiple asynchronous text sequences and propose an effective method to solve it. We formally define the problem by introducing a principled probabilistic framework, based on which a unified objective function can be derived. Then, we put forward an algorithm to Optimize this objective function by exploiting the mutual impact between topic discovery and time synchronization. The key idea of our approach is to utilize the semantic and temporal correlation among sequences and to build up a mutual reinforcement process.

We start with extracting a set of common topics from given sequences using their original time stamps. Based on the extracted topics and their word distributions, we update the time stamps of documents in all sequences by assigning them to most relevant topics. This step reduces the asynchronism among sequences. Then after synchronization, we refine the common topics according to the new time stamps. These two steps are repeated alternately to maximize a unified objective function, which provably converges monotonically. Besides theoretical justification, our method was also evaluated empirically on two sets of real-world text sequences. We show that our method is able to detect and fix the underlying asynchronism among different sequences and effectively discover meaningful and highly discriminative common topics. To sum up, the main contributions of our work are. We address the problem of mining common topics from multiple asynchronous text sequences. To the extent of our knowledge, this is the first attempt to solve this problem. We formalize our problem by introducing a principled probabilistic framework and propose an objective function for our problem. We develop a novel alternate optimization algorithm to maximize the objective function with a theoretically guaranteed (local) optimum. The effectiveness and advantage of our method are validated by an extensive empirical study on two real-world data sets.

II. System Development

a) Titles Pre-Processing (Dataset1)

- Collection of titles from research journals
  i. E.g.: DEXA, ICDE, IS, SINMOD, TKDE, and VLDB.
- Timestamp for each title words.
- Timestamp is the Volume, SNO, Month, and Year of publication.
  i. Ex: Title (d1) = “Topic Mining over Asynchronous Text Sequences” Timestamp (t1) = “24, 1, JANUARY, 2012”.
- Titles Dataset is prepared for all the documents collected.

b) Stemming: Eliminating Stop Words

- The Dataset1 consists of large number of titles.
- The words in all the titles may consists of stop words such as “an”, “the” etc,.
- For eliminating stop words from the titles, there is a need of stop words list.
- The stop words list in the proposed approach is “TMG” list.

c) Word Pre-Processing

- Title consists of sequence of words (w).
- Each word is assigned with the timestamp as title sequence (z).
- The order of sequence of words produces meaningful and suitable topical words for the context that they have.

d) Unique Topical Words

- The dataset1 consists of all the titles.
- Unique words of all the titles becomes topical words
- Each topical word sequence is equal the title.
- The module identifies all the topical words.

e) Dataset2: Document Pre-Processing

- Research Articles can be in pdf format or word format in general.
- The Proposed method requires the documents in the text format.
- Hence, pdf or doc files have to be converted to text format.

f) Frequency of Unique Topical Words

- When a pdf is given, the pdf document may consist of unique topical words (dataset1).

- Unique Topical Words Frequency for the given pdf document will be calculated.
- If a unique topical word is present, it means that the document is relevant to the topical word and impact will be based on its frequency that the unique topical word occurred.

g) Finding High Frequency Unique Words

- The document may contain more number of topical words with some frequency.
- Frequently Occurred Unique Topical Words are most relevant to the document data.
- The module identifies the high listed unique topical words.

III. Related Work

a) Dynamic Topic Models

While traditional time series modeling has focused on continuous data, topic models are designed for categorical data. Our approach is to use state space models on the natural parameter space of the underlying topic multinomial's, as well as on the natural parameters for the logistic normal distributions used for modeling the document-specific topic proportions. First, we review the underlying statistical assumptions of a static topic model, such as latent Dirichlet allocation (LDA) (Blei et al., 2003). Let fi1:K be K topics, each of which is a distribution over a fixed vocabulary. In a static topic model, each document is assumed drawn from the following generative process:

1. Choose topic proportions fi from a distribution over the (K − 1) simplex, such as a Dirichlet.
2. For each word: (a) Choose a topic assignment Z fi Mult (fi). (b) Choose a word W _ Mult (fiz).

b) Data Sets

The first data set used in our experiment is six research paper repositories extracted from DBLP, 2 namely, DEXA, ICDE, Information Systems (journal), SIGMOD, TKDE (journal), and VLDB. These repositories mainly consist of research papers on database technology. Each repository is considered as a single text sequence where each document is represented by the title of the paper and time stamped by its publication year. The second data set is two news articles feeds, which consist of the full texts of daily news reports published on the websites of International Herald Tribune3 and People's Daily Online, 4 respectively, from 1 April 2007 to 31 May 2007. Each document is time stamped by its publication date. Text sequences are preprocessed by TMG5 for stemming and removing stop words. Words that appear too many (appear in over 15 percent of the documents) or too few (appear in less than 0.5 percent of the documents) times are also removed. After preprocessing, the literature repositories have a vocabulary of 1,686 words and news feeds of 3,358 words.

c) The Local Search Strategy

In some real-world applications, we can have a quantitative estimation of the asynchronism among sequences so it is unnecessary to search the entire time dimension when adjusting the time stamps of documents. This gives us the opportunity to reduce the complexity of time synchronization step without causing substantial performance loss, by setting a upper bound for the difference between the time stamps of documents before and after adjustment in each iteration.

d) Hierarchical Structure and E-mail Streams

Extracting hierarchical structure. From an algorithm to compute an optimal state sequence, one can then define the basic representation of a set of bursts, according to a hierarchical structure. For a set of messages generating a sequence of positive inter-arrival gaps x = (x1; x2; : : : ; xn), suppose that an optimal state sequence q = (qi1 ; qi2 ; : : : ; qin) in Afis; has been determined.

Following the discussion of the previous section, we can formally define a burst of intensity j to be a maximal interval over which q is in a state of index j or higher. More precisely, it is an interval [t; t0] so that it; : : : ; it0 fi j but it □1 and it0+1 are less than j (or undaunted if t □ 1 < 0 or t0 + 1 > n).

It follows that bursts exhibit a natural nested structure: a burst of intensity j may contain one or more sub-intervals that are bursts of intensity j + 1; these in turn may contain sub-intervals that are bursts of intensity j+2; and so forth. This relationship can be represented by a rooted tree □, as follows. There is a node corresponding to each burst; and node v is a child of node u if node u represents a burst Bu of intensity j (for some value of j), and node v represents a burst By of intensity j + 1 such that By fi Bu. Note that the root of □ corresponds to the single burst of intensity 0, which is equal to the whole interval [0; n]. Thus, the tree □ captures hierarchical structure that is implicit in the underlying stream.

The transformation from an optimal state sequence, to a set of nested bursts, to a tree. Hierarchy in an e-mail stream. Let us now return to one of the initial motivations for this model, and consider a stream of e-mail messages. What does the hierarchical structure of bursts look like in this setting?

I applied the algorithm to my own collection of saved e-mail, consisting of messages sent and received between June 9, 1997 and August 23, 2001. (The cut-ofi dates are chosen here so as to roughly cover four academic years.) First, here is a brief summary of this collection. Every piece of mail I sent or received during this period of time, using my cs.cornell.edu e-mail address, can be viewed as belonging to one of two categories: rest, messages consisting of one or more large files, such as drafts of papers mailed between co-authors (essentially, E-mail as file transfer); and second, all other messages. The collection I am considering here consists simply of all messages belonging to the second, much larger category; thus, to a rough approximation, it is all the mail I sent and received during this period, unaltered by content but excluding long files. It contains 34344 messages in UNIX mailbox format, totaling 41.7 megabytes of ASCII text, excluding message headers.1

e) Enumerating Bursts

Given a framework for identifying bursts, it becomes possible to perform a type of enumeration: for every word w that appears in the collection, one computes all the bursts in the stream of messages containing w. Combined with a method for computing a weight associated with each burst, and for then ranking by weight, this essentially provides a way to and the terms that exhibit the most prominent rising and falling pattern over a limited period of time. This can be applied to e-mail, and it can be done very efficiently even on the scale of the e-mail corpus from the previous section; roughly speaking, it can be performed in a single pass over an inverted index for the collection, and it produces a set of bursts that correspond to natural episodes of the type suggested earlier. In the present section, however, I focus primarily on a different setting for this technique: extracting bursts in term usage from the titles of conference papers. Two distinct sources of data will be used here: the titles of all papers from the database conferences SIGMOD and VLDB for the years 1975-2001; and the titles of all papers from the theory conferences STOC and FOCS for the years 1969-2001. The first issue that must be addressed concerns the underlying model: unlike e-mail messages, which arrive continuously over time, conference papers appear in large batches essentially, twenty to sixty new papers appear together every half year. As a result, the automaton A_S; is not appropriate, since it is fundamentally based on analyzing the distribution of inter-arrival gaps. Instead, one needs to model a related kind of phenomenon: documents arrive in discrete batches; in each new batch of documents, some are relevant (in the present case, their titles contain a particular word w) and some are irrelevant. The idea is thus to find an automaton model that generates batched arrivals, with particular fractions of relevant documents. A sequence of batched arrivals could be considered bursty if the fraction of relevant documents alternates between reasonably long periods in which the fraction is small and other periods in which it is large.

IV. Conclusion

In this paper, we tackle the problem of mining common topics from multiple asynchronous text sequences. We propose a novel method which can automatically discover and fix potential asynchronism among sequences and consequentially extract better common topics. The key idea of our method is to introduce a self-refinement process by utilizing correlation between the semantic and temporal information in the sequences. It performs topic extraction and time synchronization alternately to optimize a unified objective function. A local optimum is guaranteed by our algorithm. We justified the effectiveness of our method on two real-world data sets, with comparison to a baseline method. Empirical results suggest that 1) our method is able to find meaningful and discriminative topics from asynchronous text sequences; 2) our method significantly outperforms the baseline method, evaluated both in quality and in quantity; 3) the performance of our method is robust and stable against different parameter settings and random initialization.

References Références Referencias

1. D.M. Blei and J.D. Lafferty, "Dynamic Topic Models," Proc. Int'l Conf. Machine Learning (ICML), pp. 113-120, 2006.
2. G.P.C. Fung, J.X. Yu, P.S. Yu, and H. Lu, "Parameter Free Bursty Events Detection in Text Streams," Proc. Int'l Conf. Very Large Data Bases (VLDB), pp. 181-192, 2005.
3. J.M. Kleinberg, "Bursty and Hierarchical Structure in Streams," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD), pp. 91-101, 2002.
4. A. Krause, J. Leskovec, and C. Guestrin, "Data Association for Topic Intensity Tracking," Proc. Int'l Conf. Machine Learning (ICML), pp. 497-504, 2006.
5. Z. Li, B. Wang, M. Li, and W.-Y. Ma, "A Probabilistic Model for Retrospective News Event Detection," Proc. Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 106-113, 2005.
6. Q. Mei, C. Liu, H. Su, and C. Zhai, "A Probabilistic Approach to Spatiotemporal Theme Pattern Mining on Weblogs," Proc. Int'l Conf. World Wide Web (WWW), pp. 533-542, 2006.
7. Q. Mei and C. Zhai, "Discovering Evolutionary Theme Patterns from Text: An Exploration of Temporal Text Mining," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD), pp. 198-207, 2005.
8. R.C. Swan and J. Allan, "Automatic Generation of Overview Timelines," Proc. Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 49-56, 2000.
9. X. Wang and A. McCallum, "Topics over Time: A Non-Markov Continuous-Time Model of Topical Trends," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD), pp. 424- 433, 2006.

10. T.L. Griffiths and M. Steyvers, "Finding Scientific Topics," Proc. Nat'l Academy of Sciences USA, vol. 101, no. Suppl 1, pp. 5228-5235, 2004.
11. X. Wang, C. Zhai, X. Hu, and R. Sproat, "Mining Correlated Bursty Topic Patterns from Coordinated Text Streams," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD), pp. 784-793, 2007.
12. J. Allan, R. Papka, and V. Lavrenko, "On-Line New Event Detection and Tracking," Proc. Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 37- 45, 1998.
13. Y. Yang, T. Pierce, and J.G. Carbonell, "A Study of Retrospective and On-Line Event Detection," Proc. Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 28-36, 1998.
14. T. Hofmann, "Probabilistic Latent Semantic Indexing," Proc. Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 50-57, 1999.

This page is intentionally left blank

Survey on Defense against Insider Misuse Attacks in the Cloud

J Venkata Subbarayudu [α] & Shaik Jakeer Hussain [σ]

Abstract - **Cloud computing provides highly scalable services for the purpose of online usage as daily premises. A key thing in cloud services is that users keeps processing in the unknown fashion where they are not aware of machines working on which are not operating by them. After all with the new technology they are adopted to now users' scares of their data which was uploaded in cloud. This appears a significant barrier due to adoptability nature of cloud network. For exploring this problem or threat we prefers a novel perfectly decentralized data computational framework for the records of accessing details of the users' information in the cloud. Clearly, we prefers or proposes an object-centered schema which makes active of accessing together with users' data and policies. We makes benefit the JAR programmable features to both develop a dynamic and random object, and to provide accessing to users' information will contains the authenticating formalities and automated accessing local to the JARs. For the improvement of user's maintenance, and also providing distributed auditing mechanisms. In additional we gave researches information which are practically done that explains the efficiency and effectiveness of this way of approaching.**

I. Introduction

Cloud computing is the network that which provides its services among online. There are no particular restrictions in the cloud computing each and every normal user can utilizes this thing at the same time big organizations are capable to use software and hardware that are under by third parties from different localities. Cloud applications in reality are so many they are used everywhere in social networking sites, search engines etc. This is cause of flexible nature of cloud computing people can get through connected anywhere anytime with simple internet connection. Cloud computing gives restriction less of resources like data base where the information stores, networks, computer processing power, and commercial organizations and customer apps.

Cloud computing explores a new path for the users for the random development in the technology, by making dynamically scalable and virtualized resources as a service through online applications. A recent Microsoft survey found that almost more than half of the people are placing or using the cloud for their transmissions but they are afraid of security of their data which was placed. At last, users are not aware of machines working on which are not operating by them.

Now users' scares of their data which was uploaded in cloud. The data which was present on clouds consist of different types of categories such as financial, business and may be personal information. This creates a significant barrier due to adoptability nature of cloud network.

a) Features

The features of cloud computing contains on-demand self service, huge network access, resource stream, flexibility and efficient service. On-demand self service is the feature that user is capable of maintaining their own computing resources. Huge network access gives services over the online or organization individual networks. Pooled resources means users draw from a pool of computing resources, from remote data centers. Services will gone be provided to the user based upon the payments by the particular user.

b) Service Methods

The service methods are:

1) Software as a Service (SaaS): It is a system application that comes along with system itself. In PaaS, an operating system, hardware, and network are provided, and if any other external application has to be install it will be done by user itself.
2) Infrastructure as a Service (IaaS): The IaaS model is used for organization equipment to help operations; those operations are nothing but storage, hardware, servers and networking components. The service provider contains itself equipment and takes care of maintenance. The user pays for it as per usage basis.

c) Deployment of cloud services

Cloud services are available by different ways a cloud for private organizations, group cloud, general cloud or hybrid cloud. Public clouds are nothing but the social services through online and are operated by a cloud provider. Those apps targeted at the general, like online photo storage in search engine services, electronic mail, and social net working sites. Any have, services for enterprises have chances offered in a general/public cloud. In a cloud of private organizations, the cloud architecture is maintained solely for a particular organization, and is observed or maintained by the organization itself or by a third party. In a community/group cloud, the service is shared by different organizations and gives access to those

Authors α σ : M. Tech, CSE Dept, ASRA Hyderabad
E-mails : venkat07509@gmail.com, jakeerhussiansk@gmail.com

particular groups only. The infrastructure /architecture will be maintained under organizations or by a cloud service provider.

II. Insider Misuse Detection Systems Overview

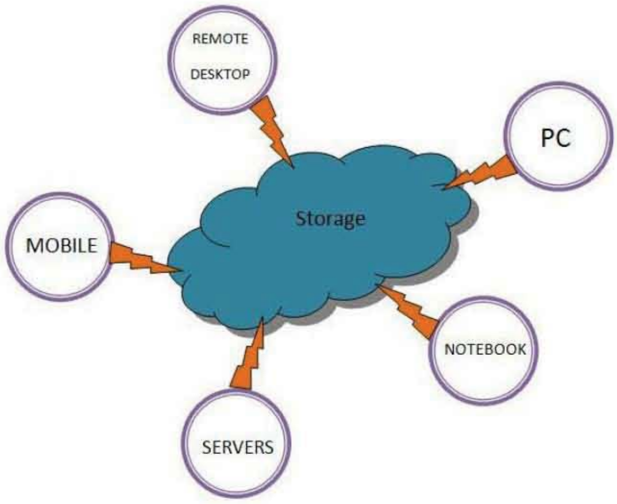
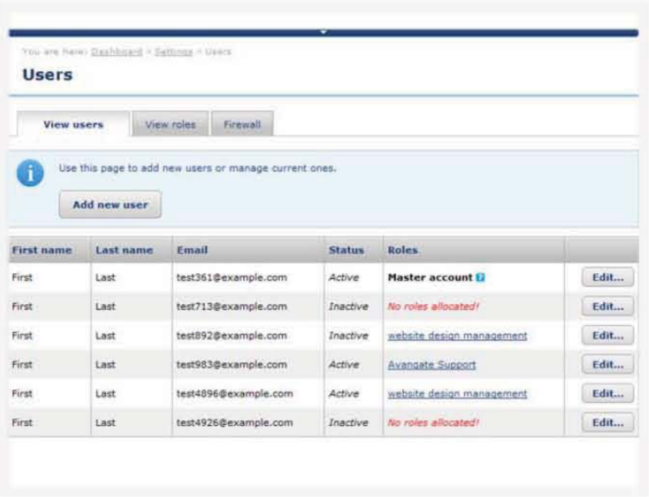


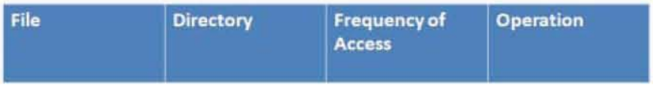
Figure 1 : Fog Computing for File Storage



Use this page to add new users or manage current ones.

First name	Last name	Email	Status	Roles	
First	Last	test361@example.com	Active	Master account	Edit...
First	Last	test713@example.com	Inactive	No roles allocated!	Edit...
First	Last	test892@example.com	Inactive	website design management	Edit...
First	Last	test983@example.com	Active	Avangate Support	Edit...
First	Last	test4896@example.com	Active	website design management	Edit...
First	Last	test4926@example.com	Inactive	No roles allocated!	Edit...

Figure 2 : User Access Profiling



File	Directory	Frequency of Access	Operation

Figure 3 : User Access Profiling Fields

III. Survey on Insider Misuse Attack Detection

a) Top Threats to Cloud Computing V1.0

This research aims at providing the assistance to organizations to educate on risk management decisions when adopting to cloud strategies. There were seven top threats identified by the research and these threats were evaluated. It discusses the threats in detail with public examples and offers public examples and offers remediation for these threats along with Impact and CSA guidance reference. The threats discussed are:

1. Abuse and Nefarious use of cloud computing.
2. Insecure Interfaces and APIs.
3. Malicious Insiders.
4. Shared Technology Issues.
5. Data loss or leakage.
6. Account or service Hijacking.
7. Unknown Risk Profile.

b) Van Dijk et al Approach

In the authors highlights the shift towards thin clients and centralized provision of computing resources in the era of cloud computing. It is also highlighted that due to lack of direct resource control there is data privacy violations, abuse or leakage of sensitive information by service providers. The most powerful tool of cryptography i.e Fully Homomorphic Encryption (FHE) is one the promising tool to ensure data security. However, the author argues that cryptography alone can't enforce the privacy demanded by common cloud computing services by defining a hierarchy of natural classes of private cloud applications and no cryptographic protocol can implement those classes where data is shared among clients. The author further lays emphasis on the relying on other forms of private enforcement viz tamperproof hardware, distributed computing and complex trust eco systems.

c) Iglesias et al Approach for User Profiling

In an adaptive approach for creating behavior profiles and recognizing computer users. It presents an evolving method for updating and evolving user profiles and classifying an observed user. As behavior of the user evolves with time, the behavior is described by fuzzy rules to make them dynamic. It uses the incremental classifier implemented by using trie for automatic clustering, classifier design and classification of the behavior profiles of users. It makes use of Evolving- Profile-Library. As a user behavior changes and evolves, the proposed classifier is able to keep up to date the created profiles using an Evolving systems approach. It is a one pass, non- interactive recursive and can be used in interactive mode. It is computationally very efficient and fast as its structure is simple and interpretable. EVABCD can perform almost as well as other offline classifiers in an online environment in terms of correct classification on validation data, and that it can adapt extremely quickly to new data and can cope with huge amounts of data in a real environment with rapid changes.

d) Rocha et al Method

In the authors propose that a malicious insider can steal any confidential data of the cloud user inspite of provider taking precaution steps like.

1. Not to allow physical access.

2. Zero tolerance policy for insiders that access the data storage.
3. Logging all accesses to the services and later use for internal audits to find the malicious insider.

It proposes to show four attacks that a malicious insider could do to: (i) Compromise passwords. (ii) Cryptographic keys. (iii) Files and other confidential data.

He does it by: (a) Clear text passwords in memory snapshots. (b) Obtaining private keys using memory snapshots. (c) Extracting confidential data from the hard disk. (d) Virtual machine relocation. None of these methods ensure to achieve holistic security in the cloud. And the attacker need not be having high technical skills.

e) Salem et al Methods

The focuses on Masquerade detection to serve as a means of building more secure and dependable systems that authenticate legitimate users by their behavior. The author has assumed that each individual user knows his own file system well enough to search in a limited and unique fashion to find information. Masqueraders, on the other hand, will likely not know the file system and layout, and would likely search more extensively and broadly in a manner that is different than the victim user being impersonated. A categorization of Windows applications and user commands that are used to abstract sequences of user actions and identify actions linked to search activities is devised. The use of search behavior profiling for masquerade attack detection permits limiting the range and scope of the profiles we compute about a user, thus limiting potentially large sources of error in predicting User search behavior modeling produces better accuracy. With the use of the RUU dataset, the best results achieved and reported in literature to date: 100% masquerade detection rate with only 1.1% of false positives. The limited set of features used for search behavior modeling also results in large performance gains over the same modeling techniques that use larger sets of features. The author has proposed an approach to profile a user's behavior based on taxonomy of Windows applications.

f) Salem et al Decoy File Management

In the concluded as masquerade attacks pose a grave security problem and detecting masqueraders is very hard. The use of trap-based mechanisms as a means for detecting insider attacks is used in general. In this paper, the author has investigated the use of such trap-based mechanisms for the detection of masquerade attacks. We evaluate the desirable properties of decoys deployed within a user's file space for detection. The author further investigates the trade-offs between these properties through two user studies, and propose recommendations for effective masquerade detection using decoy documents based on findings from the user studies. The author has presented an experimental evaluation of the different deployment-related properties of decoy documents and a guide to the deployment of decoy documents for effective masquerade detection.

g) Godoy et al Survey on User Profiling

In the Godoy et al stated the profiling strategies for user profiling. Personal information agents have emerged in the last decade to help users to cope with the increasing amount of information available on the Internet. These agents are intelligent assistants that perform several information- related tasks such as finding, filtering and monitoring relevant information on behalf of users or communities of users. In this paper the author presents a summary of the state-of-the-art in user profiling in the context of intelligent information agents. In addition the author discusses the existing approaches and lines of research in the main dimensions of user profiling such as acquisition learning adaptation and evaluation are discussed. The author has discussed in detail the success of personal agents in satisfying user information which intensely relies on the learning approach to acquire user profiles as well as the adaptation strategy to cope with changes in user interests. To better understand user profiling the authors have surveyed the literature regarding the main dimensions involved in the construction of user profiles acquisition learning adaptation and evaluation. Most user-profiling approaches in the agents surveyed had only partially addressed the characteristics that distinguish user profiling of related tasks such as text categorization or supervised learning in general. Future focus on user-profiling approaches for successful information agents not only on the above aspects but also on the assessment of comprehensible semantically enriched user profiles which will take information agents to the next level .The authors have explained the approaches proposed and developed in current personal agents for the main dimensions of user profiling.

h) Godoy et al Profiling Strategy

The author have helped to address the pressing problems with information overload, the research has developed personal agents to provide assistance to the users in navigating the Web. In addition to provide suggestions, such agents rely on user profiles representing interests and preferences, which makes acquiring and modeling interest categories a critical component in their design. The existing profiling approaches have also been evaluated and they have been found only to be partially tackling the characteristics that distinguish user profiling from related tasks. The author's technique has generated readable user profiles that have been able to accurately capture the interests, starting from observations of user behavior on the Web. The user-profiling technique which has been demonstrated helps toward the assessment of more comprehensible semantically enhanced user profiles, the application of which can lead to more powerful personal agents, like Personal Searcher, that can accurately identify user interests and adapt their behavior to interest changes. In addition, this technique presents new possibilities regarding user's interaction with their profiles as well as collaboration with other agents at a conceptual level.

IV. Cloud Insider Attack Detection Proposal

The Fog Computing Validation requires

a) System 1: Test Web Application

1. The application should be deployed on a cloud server (VMWare ESX Server). 2. The Application is used to test and to validate the Fog Computing System Detection. The Test Web Applications are the basic inputs for Fog Computing. All the applications should provide the following options It should store user name, password, confirm password and at least ten secrete questions at the time of account creation It should allow forgot password option by querying the user with randomly selected secret question.

b) System 2: Fog Computing System

1. To profile or store the user access behavior. 2. It analyzes the present behavior with the past profile The system has to process The system is an interface to view the anomalous user accesses. It allows the administrators to enforce allow/reject policies for the remote users. It provides logs of anomaly detection system 1. User Access Behavior Profiling, 2. Decoy File System Maintenance, 3. Anomaly Detection, 4. Challenge Requests.

c) User Access Behavior Profiling

The module is concerned about storing the user's request to files on the web application. The module records how many files read and how often. The operations include create, read, write, delete Fig. 3.

d) Decoy File System Maintenance

For each newly created folder or a file, corresponding decoy file will be maintained. The directory and file structure are same for both the decoy file system and the original file system. The information contained in the decoy file is not original.

e) Anomaly Detection

The current logged in user access behavior is compared with the past behavior of the user. If the user behavior is exceeding the threshold value or a limit, then the remote user is suspected to be anomaly. If the current user behavior is as the past behavior, the user is allowed to operate on the original data.

f) Challenge Requests

If the current user's behavior seems anomalous, then the user is asked for randomly selected secret questions. If the user fails to provide correct answers for a certain limits or threshold, the user is provided with decoy files. If the user provided correct answers for a limit, the user is treated as normal user. Sub subsection System 3: Web Server It provides an environment to deploy the application. On every access, it stores or log the following details Client IP, Uid, PID, Time Stamp, Request, Response Code, Response Length, Referrer and User-Agent.

Example :

```
192.168.1.1 - - [14/Aug/2012:11:34:57 -0700] "POST/cw
t/installation/index.php HTTP/1.1" 200 214
"http://www.abc.com/index.php" "Mozilla/5.0 (Windows
NT 5.1) AppleWebKit/537.1 (KHTML, like Gecko) Chro
me/21.0.1180.75 Safari/537.1"
```

g) System 4: Internet Users

The users of the cloud can be from anywhere of the internet.

h) System 5: Administration System (Sphere/Web Interface)

The system is an interface to view the anomalous user accesses. It allows the administrators to enforce allow/reject policies for the remote users. It provides logs of anomaly detection system. The system is an interface to view the anomalous user accesses. It allows the administrators to en- force allow/reject policies for the remote users. It provides logs of anomaly detection system

V. Conclusion

Monitoring the activity of the cloud storage user in Infrastructure as a service (IaaS) cloud environments is important work. The authors proposed several proposals for identifying the misuse or attacker. But there are no efficient profiling strategies for clearly distinguishing the attacker's activity. Hence proposing an efficient strategy for quickly adopting the user's behavior.

References Références Referencias

1. P. Ammann and S. Jajodia, "Distributed Timestamp Generation in Planar Lattice Networks," ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.
3. E. Barka and A. Lakas, "Integrating Usage Control with SIP-Based Communications," J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.

4. D. Boneh and M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.
5. R. Bose and J. Frew, “Lineage Retrieval for Scientific Data Processing: A Survey,” ACM Computing Surveys, vol. 37, pp. 1-28, Mar. 2005.
6. P. Buneman, A. Chapman, and J. Cheney, “Provenance Management in Curated Databases,” Proc. ACM SIGMOD Int’l Conf. Management of Data (SIGMOD ’06), pp. 539-550, 2006.
7. B. Chun and A.C. Bavier, “Decentralized Trust Management and Accountability in Federated Systems,” Proc. Ann. Hawaii Int’l Conf. System Sciences (HICSS), 2004.
8. OASIS Security Services Technical Committee, “Security Assertion Markup Language (saml) 2.0,” http://www.oasis-open.org/committees/tchome.php ?wg abbrev=security, 2012.
9. R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, “A Logic for Auditing Accountability in Decentralized Systems,” Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.
10. B. Crispo and G. Ruffo, “Reasoning about Accountability within Delegation,” Proc. Third Int’l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.
11. Y. Chen et al., “Oblivious Hashing: A Stealthy Software Integrity Verification Primitive,” Proc. Int’l Workshop Information Hiding, F. Petitcolas, ed., pp. 400-414, 2003.
12. S. Etalle and W.H. Winsborough, “A Posteriori Compliance Control,” SACMAT ’07: Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 11-20, 2007.
13. X. Feng, Z. Ni, Z. Shao, and Y. Guo, “An Open Framework for Foundational Proof-Carrying Code,” Proc. ACM SIGPLAN Int’l Workshop Types in Languages Design and Implementation, pp. 67-78, 2007.
14. Flickr, http://www.flickr.com/, 2012.

This page is intentionally left blank

Public Auditing System of Data Storage Securing Nature in Cloud Computing

P. Ramanjaneya Prasad [α] & M. Madhavi [σ]

Abstract - **Cloud computing, large number of computers that are connected through a real-time communication network. The users are flexible while storing their information in cloud network. At any time period they are capable of accessing their information from network. By this application the way of storage of users reduces the maintenance complexity. It works on providing the access to the users in the cloud network audit ability for cloud data storage security is key importance so that users can stay to there will be third party auditor to keep data efficiently. With the secure introduce an effective third party auditor (TPA); there are the two fundamental requirements. 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.**

I. Introduction

Cloud computing features are cost efficient, usage efficiency, comfortable managing, and service providing at any moment and importantly a key challenge is to used build secrecy that the cloud is capable of maintaining user data securely. Users needs privacy of their data, and also want to benefit from the rich computational applications that application developers will offer using that data. So, the cloud gives little platform-level support or standardization for user data protection not upto level data encryption at rest. Protecting user information while even through rich computations needs both specialized expertise and resources that may not be spot available to most developers. Keeping the platform layer protected is: the platform can gain economies of scale by less costs and distributing sophisticated security solutions in various applications and their developers. In users way of thinking organizations and normal pc user use flexibly this is advantage to them. No need to bother about personnel maintenances like hardware, software etc. While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' updated data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate privacy control on user's profile and their data which is stored in cloud computing or cloud network previously. This is the way where the efficiency of data increases. The attractive features of cloud computing they are most powerful and reliable than the normal pc, they have problems for data integrity and external threats of the broad range of both internal. And there is threat of security attacks more than the cloud services appear from time to time. And another one is for CSP untrust fully to customers of cloud in situation of their updated data. The way of working in reality, CSP might reclaim storage for monetary reasons by deleting data which was not accessed much, or may be encrypting the data that keeps reputation. In short, although outsourcing data to the cloud is economically attractive for massive data storage over a huge time period, it won't work immediately offer any guarantee on data integrity and accessibility. If this cause is not perfectly mentioned may blocks service of cloud architecture. If there is no hard disk memory with the users, for the security purpose traditional cryptographic primitives will e used. In particular, simply downloading all the data for its integrity verification is in reality it is too expensive on I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those un accessed data and might be too 2 late to backup of data. Under taking huge amount of the updated data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud network can be complex and high cost for the cloud users. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that user does not need to perform too many operations to use the data (in additional to retrieving the data). For example, it is desirable that users do not need to worry about the need to verify the integrity of the data before or after the data retrieval. The TPA, the people having good experience with the users that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to explore the risks to the customers of their subscribed cloud data services, the cloud service providers to improve their cloud based service platform, and even serve for independent arbitration purposes. In a word, enabling public auditing services will become a part to create cloud economy completely developed;

Authors α σ : M.Tech, CSE Dept, ASRA Hyderabad.
E-mail : karu197903@yahoo.com, madhavi_3101@yahoo.co.in

then customers get security among the risks and keeps trust in the cloud. Recently, the notion of public audit ability was explored in the context of ensuring remotely stored data integrity under different system and security models. Public audit ability allows another third party along with the user to modify the data which was stored in the cloud. A lot of schemes will not work out on privacy protection of users' data against external auditors. Indeed, Server gives the complete information to customers' information to the auditors. This severe drawback greatly affects the privacy schemas in Cloud network. In the case of protecting data privacy, the normal user which stores their general information won't need any of these schemas or auditing process and also exploring of threats of unauthorized accessing towards their data privacy. There are so many external or so called private organizations keeps restrictions on their data which was placed in the cloud not to share to third parties. Usage of data encryption while before uploading the data is one of privacy protecting by the cloud, this is what was best way to the privacy preserving public auditing scheme that was explored in this paper. If there is no perfect designed auditing protocol, encryption won't work out data from "flowing away" by UN authorized persons during the auditing process. Means it completely solves the problem of protecting data privacy but just reduces it to the key management. The persons which are not having permissions are accessing the information is a critical problem cause of decrypting the keys. So keeping the privacy-preserving third-party auditing protocol, not based on data encryption, is the threat which we are going to work in this paper. The workouts are on supporting on privacy-preserving public auditing in Cloud network, taking key as data storage. Apart of this, with the popularity of Cloud Computing, a increase of auditing tasks from different users may be delegated to TPA. Result of individual auditing of increasing rate can be annoying and bulky; a normal curious task is how to enable the TPA to efficiently work large number of auditing tasks in a batch parallel. Identifying these problems, our work use the of schema public key based Homomorphic linear authenticator which enables TPA to do auditing without need of data which was stored locally and computations as compared to the straightforward data auditing approaches. By integrating the HLA with random masking, our protocol guarantees that the TPA doesn't contain any records about the data stored in the cloud network during auditing.

II. Problem Statement

Those are 1) TPA should be able to efficiently does auditing job in the cloud data base with no need of additional local copy of data. This gives advantages that makes user comfortable. Mostly, our addition in this work is:

1. Creating interest public auditing system of data storage securing nature in Cloud Computing and providing a privacy-storing, auditing protocol.
2. This method is the premier one that gives flexibility of scalable and efficient public auditing in the Cloud Computing. In particular, our scheme achieves batch auditing where multiple assigned auditing actions from different users can be performed concurrently by using TPA.
3. We prove the security and advocate the efficiency of our methodology through concrete experiments and comparisons with the state-of-the-art.

a) Security and Privacy Challenges

It's is not that easy to create a data-protection solution for the threats in the cloud, cause of cloud network itself includes so many various elements. Result of work done will be stored in particular domain accordingly; main spot will be on widely used apps such as e-mail, personal financial management, social networks, and business tools such as word processors and spread sheets. The following are the class of applications used.

- ➢ Provide services to a huge quantity of various end users, as against to huge data workflow management for a single entity.
- ➢ Use a data model consisting mostly of sharable units, where all data objects have access control lists (ACLs) with one or more users.
- ➢ Developers are capable of performing the operations of apps in another computing platform those are the physical infrastructure, job scheduling, user authentication, and the base software environment, which makes easy to perform but not for in the same platform.

Overly rigid security is as detrimental to cloud service value as inadequate security. A primary challenge in designing a platform-layer solution useful to many applications is ensuring that it enables rapid development and maintenance. To ensure a practical solution, we considered the following goals relating to data protection as well as ease of development and maintenance.

- ➢ Integrity. The user's stored data won't be corrupted.
- ➢ Privacy. Private data won't be leaked to any unauthorized entity.
- ➢ Access transparency. Logs will clearly indicate who or what accessed any data.
- ➢ Ease of verification. Users will be able to easily verify what platform or application code is running, as well as whether the cloud has strictly enforced their data's privacy policies.
- ➢ Rich computation. The platform will allow efficient, rich computations on sensitive user data.
- ➢ Development and maintenance support. Because they face a long list of challenges bugs to find and

fix, frequent software upgrades, continuous usage pattern changes, and user demand for high performance developers will receive both development and maintenance support.

Any credible data protection approach must grapple with these issues, several of which are often overlooked in the literature.

III. System Development

a) *Privacy-Preserving Public Auditing*

Homomorphism based authenticators are outstanding metadata outlet from each data block individually, which can be protected in the way to assure an auditor that a linear clubbed of data blocks is correctly calculated by verifying only the aggregated authenticator. Complete view to achieve privacy-preserving public auditing, we prefers to uniquely integrate the Homomorphic authenticator with the help of technique random mask. In our study, the linear combination of sampled blocks in the server's response is masked with randomness produced by a pseudo random function (PRF).

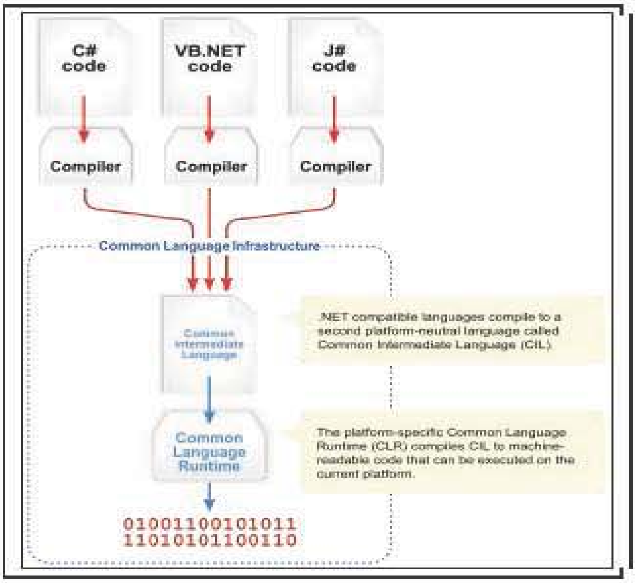
The proposed scheme is as follows:

- Setup level
- Audit level

i. *Batch Auditing*

By using privacy-preserving public auditing in Cloud Computing, TPA may concurrently manages a lot auditing delegations according to various users' requests. The each auditing of these operations for TPA can be clumsy and not efficient. Batch auditing not only allows TPA to perform the various auditing tasks parallel, but also efficiently reduces the computation cost on the TPA side.

Architecture


C# code
VB.NET code
J# code
Compiler
Compiler
Compiler
Common Language Infrastructure
Common Intermediate Language
.NET compatible languages compile to a second platform-neutral language called Common Intermediate Language (CIL).
Common Language Runtime
The platform-specific Common Language Runtime (CLR) compiles CIL to machine-readable code that can be executed on the current platform.
01001100101011
11010101100110

Visual Overview of the Common Language Infrastructure

ii. *Data Dynamics*

At last, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Here we explored how our scheme can be adapted to do operations on already existing work to support data dynamics, including block level operations of alterations, deletion and insertion. We are capable of using this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

IV. Related Work

The defined "provable data possession" (PDP) model for ensuring possession of data files on harmful storages. Their scheme uses the RSA based Homomorphic linear authenticators for auditing already stored data and prefers randomly sampling a few blocks of the file. Moreover, the general audit ability in their scheme requires the linear combination of sampled blocks shown to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor. In "proof of retrieve ability' (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrieve ability" of data files on re- mote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public audit ability is not supported in their main scheme. Although they describe a straight forward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Dodis et al. give a study on different variants of PoR with private auditability.

Design an improved PoR scheme built from BLS signatures with full proofs of security in the security model defined in. Similar to the construction in, they use publicly verifiable homomorphic linear authenticators that are built from provably secure BLS signatures. Based on the elegant BLS construction, a compact and public verifiable scheme is obtained. Again, their approach does not support privacy-preserving auditing for the same reason as. Shah et al. propose allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies both the integrity of the data file and the server's possession of a previously committed decryption key. This scheme only works for encrypted files and it suffers from the auditor statefulness and bounded usage, which may potentially bring in online burden to users when the keyed hashes are used up. In other related work, Ateniese et al. Propose a partially dynamic version of the prior PDP scheme, using only symmetric key cryptography but with a bounded number of audits. In, Wang et al. consider a similar support for partial dynamic data storage in a distributed scenario with additional feature of data error localization. In a subsequent work, Wang et al. propose to combine BLS-based HLA with MHT to support both public audit ability and full data dynamics. Almost simultaneously, Erway et al. Developed a skip lists based scheme to enable provable data possession with full dynamics support. However, the verification in these two protocols requires the linear combination of sampled blocks just as, and thus does not support privacy- preserving auditing. While all the above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy preserving public auditing in cloud computing. More importantly, none of these schemes consider batch auditing, which can greatly reduce the computation cost on the TPA when coping with a large number of audit delegations.

a) Virtual Administration

The advent of cloud has changed the role of System Administrator to a "Virtual System Administrator". This simply means that daily tasks performed by these administrators have now become even more interesting as they learn more about applications and decide what's best for the business as a whole. The System Administrator no longer has a need to provision servers and install software and wire up network devices since all of that grunt work is replaced by few clicks and command line calls. The cloud encourages automation because the infrastructure is programmable. System administrators need to move up the technology stack and learn how to manage abstract cloud resources using scripts.

Likewise, the role of Database Administrator is changed into a "Virtual Database Administrator" in which he/she manages resources through a web-based console, executes scripts that add new capacity programmatically in case the database hardware runs out of capacity and automates the day-to-day processes. The virtual DBA has to now learn new deployment methods (virtual machine images), embrace new models (query parallelization, geo-redundancy and asynchronous replication, rethink the architectural approach for data and leverage different storage options available in the cloud for different types of datasets. In the traditional enterprise company, application developers may not work closely with the network administrators and network administrators may not have a clue about the application. As a result, several possible optimizations in the network layer and application architecture layer are overlooked. With the cloud, the two roles have merged into one to some extent. When architecting future applications, companies need to encourage more cross-pollination of knowledge between the two roles and understand that they are merging.

V. Conclusion

In this paper, we explore a Cloud Computing new entity privacy-preserving public auditing system for the purpose of data storage security, where TPA works on auditing details without need of data which was stored locally. Here we uses the authenticator with feature of homomorphism and also using technique random mask to create trust on cloud that used TPA will not get or bother about the information which was stored by the user while auditing process, it also reduces the workflow to cloud user from the annoying and cost efficient auditing task, but also take the edge off the users to decrease the fear of their uploaded data privacy. Under taking TPA may concurrently handle different audit levels from various users for their updated data files, in addition we extend our privacy-preserving public auditing protocol from single user to multi-user, here TPA workouts on various number of auditing tasks parallel. Efficient security and performance analysis gives reports that the proposed techniques are secure and highly efficient. The mighty features of the proposed schemes reduce the burden of economies in future for Cloud Computing.

References Références Referencias

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
2. N. Gohring, "Amazon's s3 down for several hours," Online.http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.
3. Amazon.com, "Amazon s3 availability event: July 20, 2008," Online at http://status.aws.amazon. Com/s3-20080720.html, July 2008.
4. S. Wilson, "Appengine outage," Online at http:// www.cio-weblog.com/50226711/appengineou tage. Php, June 2008.
5. B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.Washing onpost.Com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.
6. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Cryptology ePrint Archive, Report 2007/202, 2007, http://eprint.iacr. org/.
7. M. A. Shah, R. Swaminathan and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.
8. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for

storage security in cloud computing," in Proc. of ESORICS'09, Saint Malo, France, Sep. 2009.

9. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www.cloudsecurityalliance.org.
10. H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.
11. A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.
12. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.
13. 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996, last access: July 16, 2009.
14. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. of Eurocrypt 2003, volume 2656 of LNCS. Springer-Verlag, 2003, pp. 416–432.

This page is intentionally left blank

Design and Analysis of Leaf Spring

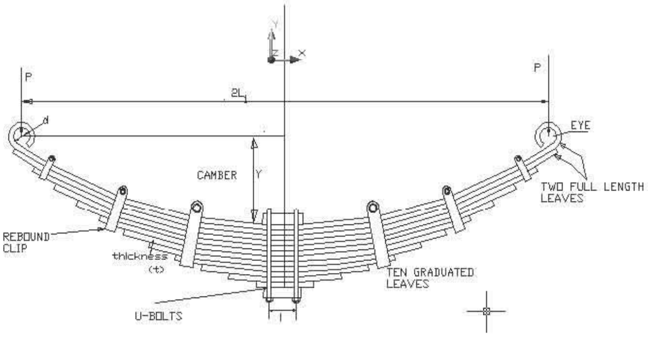
Sunil Chintha [α] & N. Jeevan Kumar [σ]

Abstract - **Leaf springs are unique kind of springs used in automobile suspension systems. The benefit of leaf spring over helical spring is that the ends of the spring may be leaded along a definite path as it deflects to act as a structural member in addition to energy absorbing device. The main work of leaf spring is not only to give support to vertical load but also to isolate road induced vibrations. It is subjected to millions of load cycles leading to fatigue failure. Static analysis gives the safe stress and with corresponding pay load of the leaf spring and also to research the behavior of structures under practical situations. The existing work attempts to examine the safe load of the leaf spring, which will represent the speed at which a comfortable speed and safe drive is available. A typical leaf spring configuration of TATA-407 light commercial vehicle is selected for research. Finite element analysis has been carried out to determine the safe stresses and pay loads.**

I. Introduction

A spring is explored in the form of elastic body, where the working criterion alters when it is loaded then used for recovering its original shape and then load is flushed out. Leaf springs absorb the vehicle vibrations, shocks and bump loads by means of spring deflections, so that the potential energy is kept in stock in the leaf spring and then explored slowly. Capability to store and absorb more amount of strain energy ensures the availability suspension system. Semielliptic leaf springs are most universally used for break in all type of vehicles. In case of cars also, these are widely used in rear suspension. The spring consists of a number of leaves known as blades. The blades are differs in length. The blades are normally given an initial curvature then it will be set to straight. The leaf spring is based on theory of a beam of uniform strength. The largest blade has eyes on its ends. This blade is referred master leaf; the rest are known as graduated leaves. All the blades are bound together by means of steel straps.

The spring is placed on vehicle's axle. The complete vehicle load rests on the leaf spring. The front end of the spring is attached to the frame with a simple pin joint, while the rear end of the spring is attached with a shackle. Shackle is the flexible link one that which connects between leaf spring rear eye and frame. And when vehicle comes across a projection on the road surface, the wheel moves up, leading to deflection of the spring. This modifications the length between the spring eyes. If two ends are fixed, the spring will not be able to accommodate this change of length. So, to accommodate this change in length shackle is given at one end, which gives a flexible connection. The leaf spring's front eye is constrained in every direction, where as rear eye is not in X-direction. This rare eye is linked to the shackle. While loading the spring deflects and moves in the direction perpendicular to the load applied. When the leaf spring deflects, the upper side of each leaf tips slides against the lower side of the leaf. This gives some damping which reduces spring vibrations, but since this available damping may change with time, it is not advised to avail of the same. Moreover, it produces squeaking sound. In any further if moisture is also present, such inter-leaf friction will gives fretting corrosion which reduces the fatigue Strength of the spring, phosphate paint may reduce this problem fairly of the load W from the cantilever end.



II. Manufacturing Process of Leaf Springs

Step 1 : By identifying your specific requirements, our sales department firstly picks up the appropriate specification sheet, which is then issued to the production team to proceed with the manufacturing process. We give a unique reference number to each specification sheet so that we can track the process all through the working life cycle of sundry item or spring.

Author α : M.Tech, Mech. Dept, HITS, Hyderabad, India.
E-mail : sunilchintha430@gmail.com
Author σ : (PhD), Professor Mech. Dept, HITS, Hyderabad, India.
E-mail : jknaini@rediffmail.com

Step 2 : Spring steel to BS970 is then cut off along the length and made to go through required operations incorporating eye-forming, nibbing, beating, taper-rolling and wrapping. Then, the leaves are heated up at temperature 1000 to 1, 0500 C, oil quenched in order to provide the temperature 8900C, or above. Once the draining is done, they are re heated at about 500 to 5600C so as to obtain the Brinell solidity reading of 356 to 440 HBS 10/3000, before the closing alterations are made to give adequate arc and shape.

Step 3 : When assembling the entire unit, the required components including center bolts, clips and bushes are added. The final unit manufactured is again evaluated against the specifications given in specs sheet. To complete the spring, it is coated with a protective covering, and then goes through final inspection according to quality control standards.

Step 4 : The Locomotive Springs also implement the similar manufacturing course, but are made according to BR 148 and BR 166.

III. System Development

In computer-aided design, geometric modeling is concerned with the computer compatible mathematical description of the geometry of an object. The mathematical description allows the Model of the object to be displayed and manipulated on a graphics terminal through signals from the CPU of the CAD system. The software that provides geometric modeling capabilities must be designed for efficient use both by the computer and the human designer. Usage of geometric modeling, the designer develops the graphical model taking object as a lead on CRT screen which was part of ICG system. It gives three types of inputs of commands system. The first one among those commands creates static geometric elements which includes points, lines, and circles. And second command which was used to achieve scaling, rotation, or other transformations of these elements. The third command results the different elements have to get attached into the referred shape of the object which was developed on the ICG system. While geometric process, system automatically alters the commands into a math level, stored in computer data files, and then shows it form of image on CRT screen. The model can consequently call as from the data files for analysis or alteration. The advanced method of geometric modeling is solid one in three dimensions.

Modeling Flow for Leaf Spring

1. Initially have to create the key point 100 at origin.
   x, y, z = (0, 0, 0).
2. Next to make another key point 200 where arbitrary distance in Z-direction.
   x, y, z = (0, 0, 200).
3. Attach above two key points 100 and 200 for reference axis.
4. With the usage of data from math analysis develop the key point one according to distance of radius of curvature R1 in vertically decreasing down direction.
   x, y, z = (0, -R1, 0).
5. In that way only key points 2 and 3 according to R2.
   x, y, z = (0, -R2, 0)
   Key points 4 and 5 correspond to R3.
   x, y, z = (0, -R3, 0).
6. Key point 20 according to R11. i.e. x, y, z = (0, -R11, 0).
7. Attach the pair of key point's sequentially as follows Key points above.
8. Line1 created by key points 1 and 2, line2 created by key points 2 and 3 and line10 created by the key points 19 and 20.
9. Dismiss the above lines with respect to reference axis stated in step3 as follows:
   Extrude line1 with an angle Φ1, will get area1
   Extrude line2 with an angle Φ2, will get area2 ... and
   Extrude line10 with an angle Φ10, will get area10.
10. After discarding all the lines, the semi area of the spring without eye will form on XY- plane with significant degeneracy.
11. To avoid degeneracy, extend the right side line of smallest area i.e. area 10 to some extent such that it cross the top most area i.e. area1.Now divide area by line. For this, select the areas left to extended line1and divide with that line. Similarly, extend the right side line of second smallest area i.e. area9 to some extent such that it cross the top most area i.e. area1. Again divide area by line. For this select the areas left to extended line2 and divide with that line.
12. The above process is to be done up to extension of line of area9 and divide area by extension line9.
13. Now perfect half area of leaf spring without eye will form.
14. Eye construction: Extend the right side line of top most area i.e. area1 to the length equal to the radius of eye. Delete lines only, so that key point of that line will remain. Shift the origin to that key point. Create another key point say some key point300 in

z-direction. Join the above two key points to get reference axis to rotate the right side line of area1. Extrude the line with respect to reference axis to an angle 2750 to 2800. Delete all reference lines. So half area of leaf spring with eye is created.

15. For gaining full area of the leaf spring. Shift the origin to the top left most area key point i.e. key point1. Reflect the complete area with respect to YZ – plane.
16. And also to retrieve the solid model of the leaf spring, extrude the area by Z-offset to a length equal to the width of the leaf spring.
17. To make a cylindrical hole at centre of the leaf spring to provide bolting for all the leaves, so that all the leaves are in perfect alignment: Create centre key point of the leaf spring on the top view i.e. XY-plane, by using key points between key points' command. Shift the origin to that key point. Choose the proper work plane by using work plane Create a cylinder along Z-axis in vertically downward direction. Subtract the cylinder from the solid leaf spring. So that leaf spring with hole to provide bolt will obtain.

a) *Static Analysis*

For the above given requirement of the leaf spring, the static analysis is performed using ANSYS to find the maximum safe stress and the corresponding pay load. After geometric modeling of the leaf spring with given requirements it is subjected to analysis. The Analysis involves the following discritization known as meshing, boundary conditions and loading. For this model analysis loading is not needed.

i. *Meshing*

Meshing involves division of the complete of model into small pieces known as elements. This was made of meshing. Thos was flexible to choose the free mesh because the leaf spring has sharp curves, so that shape of the object will not get modify. For meshing the leaf spring the element type have to select first. It is represented; the element type is solid 72. The element edge length is taken as 15 and is refined the area of centre bolt to 2. Fig 7.2 shows the meshed model of the leaf spring.

The following are the material properties of the given leaf spring. Material = Manganese Silicon Steel, Young's Modulus E = 2.1E5 N/mm2, Density ρ = 7.86E-6 kg/mm3,
Poisson's ratio = 0.3 and Yield stress = 1680 N/mm2.

ii. *Boundary Limitations*

The spring is placed on vehicle's axle. The complete vehicle load rests on the leaf spring. The front end of the spring is attached to the frame with a simple pin joint, while the rear end of the spring is attached with a shackle. Shackle is the flexible link one that which connects between leaf spring rear eye and frame. And when vehicle comes across a projection on the road

centre bolt to 2. Fig 7.2 shows the meshed model of the leaf spring.

The following are the material properties of the given leaf spring. Material = Manganese Silicon Steel, Young's Modulus E = 2.1E5 N/mm2, Density ρ = 7.86E-6 kg/mm3,
Poisson's ratio = 0.3 and Yield stress = 1680 N/mm2.

iii. *Boundary Limitations*

The spring is placed on vehicle's axle. The complete vehicle load rests on the leaf spring. The front end of the spring is attached to the frame with a simple pin joint, while the rear end of the spring is attached with a shackle. Shackle is the flexible link one that which connects between leaf spring rear eye and frame. And when vehicle comes across a projection on the road

surface, the wheel moves up, leading to deflection of the spring. This modifications the length between the spring eyes. If two ends are fixed, the spring will not be able to accommodate this change of length. So, to accommodate this change in length shackle is given at one end, which gives a flexible connection. The leaf spring's front eye is constrained in every direction, where as rear eye is not in X-direction. This rare eye is linked to the shackle. While loading the spring deflects and moves in the direction perpendicular to the load applied. When the leaf spring deflects, the upper side of each leaf tips slides against the lower side of the leaf. This gives some damping which reduces spring vibrations, but since this available damping may change with time, it is not advised to avail of the same.

The link oscillates during load applied and flushed out. Therefore the nodes of rear eye of the leaf spring are constrained in all translational degrees of freedom, and constrained the two rotational degrees of freedom. So the front eye is constrained as UX, UY, UZ, ROTX, ROTY and the nodes of the rear eye are constrained as UY, UZ, and ROTX, ROTY. Figure 4 shows the boundary conditions of the leaf spring.

iv. *Loads Applied*

The load is distributed equally by all the nodes associated with the center bolt. The load is applied along FY direction as shown in Figure 4. To apply load, it is necessary to select the circumference of the bolt hole and consequently the nodes associated with it. It is necessary to observe the number of nodes associated with the circumference of the bolt hole, because the applied load need to divide with the number of nodes associated with the circumference of the center bolt.

IV. Related Work

Research results from testing the leaf springs under static loading containing the stresses and deflection are placed in the Table 4. These are compared with FEA. Testing done for unidirectional Epoxy mono composite leaf spring only. From where composite leaf spring is able to withstand the static load, it is finales that there is no argument from strength point of view also, in the process of replacing the conventional leaf spring by composite leaf spring. From the time composite spring is designed for same stiffness as that of steel leaf spring, both the springs are considered to be almost equal in vehicle stability. The main drawbacks of composite leaf spring are of chipping resistance. The matrix one is likely to chip off when it is for bad environments which causes breakage some fibers in the lower portion of the spring. This may result in a loss of capability to share flexural stiffness. Case is it depends on the condition of the road. In casual road condition, this type of problem will not be there. Composite leaf springs made of polymer matrix composites have good strength retention on ageing at critical environments. A composite one replaces with steel leaf spring. Theme was to get a spring with minimum weight which is capable of carrying given static external forces by constraints limiting stresses and displacements. The weight of the leaf spring is reduced considerably about 85 % by replacing steel leaf spring with composite leaf spring. Thus, the objective of the UN sprung mass is achieved to a larger extent. The stresses in the Composite leaf springs are much lower than that of the steel spring.

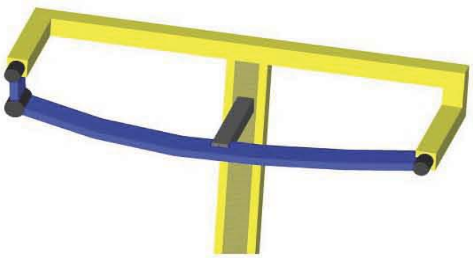


Figure 1 : Leaf Spring Test Rig

The validation of the standard leaf spring has been carried out by comparing the model to a reference multi-body model. A test rig, from above figure, has been used to generate the dynamic and kinematic comparison.

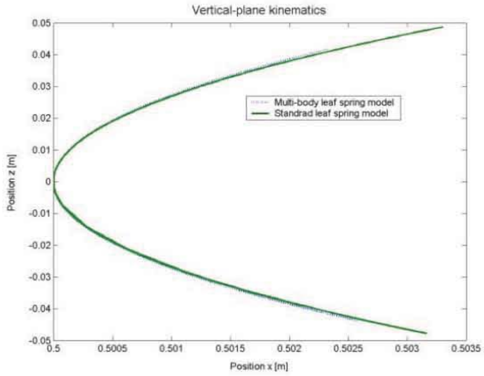


Figure 2 : Vertical plane kinematics comparison

The vertical plane kinematics of the leaf spring modeled with rigid elements are virtually the same as for the model described by Lagrange's equation. Both models are damped via viscous damping over each generalized coordinate and corresponding revolute joint for the multi-body model. The vertical plane dynamics for the different models are very similar to each other as long as the excitation does not consist of high frequency components. The fact that the standard model has both stiffness and damping in the mount positions makes it a bit complicated to compare these results, but without fine tuning of the stiffness and damping they perform. The differences can easily be related to the bushings in the mount positions and the mass less approximation used in the standard leaf spring.

A suspension assembled as in figure 10 simulates approximately 18 times faster than the reference suspension. A comparison of the kinematic and dynamic behavior of two multi body leaf springs with five versus nine links. The differences between the models are small which implies that the five link leaf spring meets the requirements for vehicle handling simulations. The shackle has big influence on the leaf spring's kinematics. The shape of the leaf spring in the comparison results in larger deflection in bounce than in rebound. This because the shackle's lower mount towards the spring always moves upwards with deflection. Other geometries would give different results.

And as per different case studies the differences of deflections and bending stresses in E-Glass/Epoxy finish mono leaf spring and spring with bonded attachments. Adhesively bonded end joints impacts the performance level of composite leaf spring in comparing with bolted joints since, delamination; matrix cracking and stress ability at the holes are observed in bolted joints. Scarf type of bonded joints enhances the strength considerably without peel splitting compared to the lap type of bonded joints. Induced peel and shear stresses are under yield limits. FEA results give the necessary link between mechanical properties, component design and fabrication to achieve performance optimization. Composite mono leaf spring with integral eye is economical and explored good performance. Harmonic analysis has been done on composite leaf spring to know the modal frequency. The first five natural frequencies are explored. The natural frequency of composite leaf spring is higher than that of the steel leaf spring and is far enough from the road frequency to avoid the resonance.

The construction of a composite mono leaf spring having constant cross sectional area, where the stress level at any station in the leaf spring is considered constant due to the parabolic type of the thickness of the spring, has proved to be very effective. The study demonstrated that composites can be used for leaf springs for light weight vehicles and meet the requirements, together with substantial weight savings.

V. Conclusion

The automobile chassis is placed on the axles, which is not direct but with some form of springs. This is to isolate the vehicle body from the road shocks which might be in the form of bounce, pitch, etc. These tendencies give rise to an uncomfortable ride and also cause extra stress in the automobile frame and body. Every part which performs the function of isolating the automobile from the road shocks are bunch of collection referred as a suspension system. Leaf spring is a device which is used in suspension system to keep safe the vehicle and the occupants. For safe and comfortable riding in the sense to prevent the road shocks from being transmitted to the vehicle components and to guard for safety the occupants from road shocks it is mandatory to determine the maximum safe load of a leaf spring. So in the present work, leaf spring is developed and static analysis is moved out by using ANSYS software and it is for the given requirements of the leaf spring, the max safe load is 7700N. Observation gives that the maximum stress is developed at the inner side of the eye sections, so have to take care in eye design and fabrication and also material selection. The selected material should contain good ductility, resilience and toughness to reduce sudden fracture for providing safety and comfort.

References Références Referencias

1. Senthil Kumar and Vijayarangan, "Analytical and Experimental studies on Fatigue life Prediction of steel leaf soring and composite leaf multi leaf spring for Light passenger veicles using life data analysis" ISSN 1392 1320 material science Vol. 13 No.2 2007.
2. Shiva Shankar and Vijayarangan "Mono Composite Leaf Spring for Light Weight Vehicle Design, End Joint, Analysis and Testing" ISSN 1392 Material Science Vol. 12, No.3, 2006.
3. Niklas Philipson and Modelan AB "Leaf spring modeling" ideon Science Park SE-22370 Lund, Sweden.
4. Zhi'an Yang and et al "Cyclic Creep and Cyclic Deformation of High-Strength Spring Steels and the Evaluation of the Sag Effect: Part I. Cyclic Plastic Deformation Behavior" Material and Material Transaction A Vol. 32A, July 2001-1697.
5. Muhammad Ashiqur Rahman and et al "Inelastic deformations of stainless steel leaf springs-experiment and nonlinear analysis" Meccanica Springer Science Business Media B.V. 2009.
6. C.K. Clarke and G.E. Borowski "Evaluation of Leaf Spring Failure" ASM International, Journal of Failure Analysis and Prevention, Vol5 (6) Pg. No. (54-63).
7. J.J. Fuentes and et al "Premature Fracture in Automobile Leaf Springs" Journal of Science Direct, Engineering Failure Analysis Vol. 16 (2009) Pg. No. 648-655.
8. Mouleeswaran Senthil Kumar and Sabapathy Vijayarangan (2007). Analytical and experimental studies on fatigue life prediction of steel and composite multi-leaf spring for light passenger vehicles using life data analysis. Materials Science 13(2) 141-146.
9. HA Al-Qureshi (2001). Automobile leaf springs from composite materials. Journal of Material Processing Technology 118 58-61.
10. JJ Fuentes, HJ Agulilar, JA Rodriguez and EJ Herrera (2008). Premature fracture in automobile leaf springs. Engineering Failure Analysis 16 648-655.
11. I Rajendran and S Vijayarangan (2002). Design and Analysis of a Composite Leaf Spring. Journal of Institute of Engineers India 82 180 –187.
12. RM Mayer, JP Hou, JY Cherruault, I Nairne and G Jeronimidis (2007). Evolution of the eye-end design of a composite leaf spring for heavy axle loads. Composite Structures 64 351-358.
13. A Skrtz, T.Paszek, (1992) "Three dimensional contact analysis of the car leaf spring", Numerical methods in continuum mechanics 2003, Zilina, Skrtz republic.
14. Cheng Wang, (1999) "Design and Synthesis of Active and Passive vehicle suspensions".

This page is intentionally left blank

Dynamic Simulation of Transport Aircraft 3D Design Landing-Elastic Leg Shock Absorb ER Loads

Kurathota Praveen Kumar [α] & N. Jeevan Kumar [σ]

Abstract - **In the paper, dynamic simulation of landing impact of a large transport aircraft, based on a non-linear dynamical model that allows for touchdown analysis of an aircraft 3D landing is presented. The aircraft model is shaped as a multibody system with variable kinematical structure. The model includes discontinuous dynamics of the main landing gear shock absorber, tire dynamics and wheel spin-up effect. The aerodynamic loads are considered, too. Because of its great influence on an aircraft ground dynamical behavior and landing gear subparts loads determination, dynamical model of the main gear shock absorber is presented in more details. Based on the developed model, the touchdown impacts of a transport aircraft for different 3D flight-landing parameters (one gear landing cases) are simulated with the focus on the main gear shock absorbers loads determination.**

I. Introduction

During landing and taxi, a transport aircraft landing gear and parts of an airframe can be exposed to high dynamical loading. In the extreme situations even damages and loss of the stability of an airplane may be expected. Since during more common large airplane tail-down landing conditions all of dynamical loads are carried on the main gears first, dynamical characteristics of the main gear are of the most significant importance for the safe touchdown during which an airframe load factors should be kept in the prescribed range. However, when the most critical landing conditions and dynamic loads on the main gear are being determined, the simplifications are often made: an airplane aerodynamic loads are oversimplified, aircraft pitching and rolling motion are neglected or tire dynamics and wheel spin-up forces are not taken into consideration. Although the basic characteristics of a landing aircraft dynamical response can be determined by simplified linear dynamic analysis, the more accurate time simulation or determination of subsystems dynamical loads

Require full-scale nonlinear multibody approach. In the paper, an aircraft multibody model that allows for dynamic simulation of an aircraft landing cases as well as determination of the main gear dynamical loads is shortly described. The model includes aircraft aerodynamic loads, discontinuous dynamics of a shock absorber oleo-pneumatic element and an aircraft tire dynamics including wheel spin-up effect. Because of its great influence on aircraft ground dynamical behavior and landing gear subparts loads determination, dynamical model of the main gear shock absorber is presented in more details. Based on the developed model, the touchdown impacts of a transport aircraft for different 3D flight-landing parameters are simulated with the focus on the main gear shock absorbers loads determination.

II. System Study

a) Landing Aircraft Dynamical Model

i. *Multibody Dynamical Model*

The aircraft dynamical model that allows for non-linear dynamic simulation of 3D landing and taxi is designed as a multibody system with variable kinematical structure. The model comprises aircraft main body, a main landing gear consisting of two elastic legs with an upper part (the upper part of shock absorber + additional masses) and a lower par (the lower part of shock absorber + wheel and tire + additional masses) and nose landing gear consisting of two parts of the same structure. The upper part and lower part of landing gear is connected *via* non-linear force coupler, modeled according to the shock absorber dynamical characteristics. Another non-linear force coupler is added to model aircraft tire dynamics. The aircraft global multibody system and part of shock absorber assembly is depicted in Figure 1. Basically, global model possess 12 spatial degrees of freedom (DOF). During kinematical modeling it is assumed that landing gear elastic legs stay in upright vertical position and do not change their orientation during landing.

The designed model allows for dynamic simulation of an aircraft three-dimensional landing situations such as one-gear landing case, which may happen during lateral wind landing conditions.

ii. *Aircraft tire dynamics*

It is assumed that the main gear is equipped with the four tires of the conventional type, which are in use in the modern transport aviation. Mechanical properties of tires are estimated after and manufacturer data. The applied tire dynamical model considers its

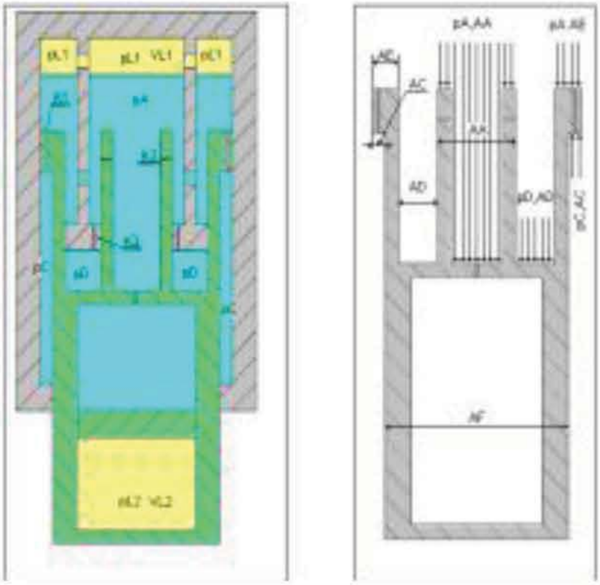
Author α : Mech. Dept., HITS, Hyderabad.
E-mail : kpraveen5ps@gmail.com
Author σ : Professor Mech. Dept, HITS, Hyderabad.
E-mail : madhavi_3101@yahoo.co.in

dynamical behavior (inertia effects, centrifugal growth of tire radius, side loads), but hysteresis effects is neglected for this type of simulations. A calculation of the tire contact dynamics spin-up force is based on tire variable slip-friction characteristics and a slippage factor defined according. It is assumed (and verified by the simulation results) that tire-bottoming deflections will not occur during analyzed motion.

III. System Environment

a) Landing Gear Shock Absorber

Most commonly, a telescopic main landing gear of a transport aircraft comprises a shock absorber of oleo-pneumatic type. Considering a contemporary design, it is a several stage unit and contains four chambers: a first-stage oleo-pneumatic chamber containing low pressure gas and hydraulic fluid, a recoil chamber and compression chamber containing hydraulic fluid and a second-stage pneumatic chamber that contains high pressure gas (nitrogen). The floating piston in the second-stage cylinder separates hydraulic fluid and high pressured nitrogen. During a compression stroke, the floating piston does not become active until the gas pressures of the first-stage and second-stage chambers are equal, which happens during system increased dynamical loading. Dynamical characteristics of the shock absorber are strongly influenced by the system of orifices that controls a hydraulic flow and by means of which net hydraulic resistance can be tuned. Considering different possibilities of the activation of floating piston and orifices as the absorber closes, it can be shown that four operation stages can be identified during the Compression stroke. During return stroke, primary control of the shock absorber recoil consists of the fluid flow from the recoil chamber into the oleo-pneumatic chamber and from the oleo-pneumatic chamber to the compression chamber. To prevent unit (and airplane!) excessive rebound, the orifices hydraulic resistance increases significantly during the absorber recoil stroke.

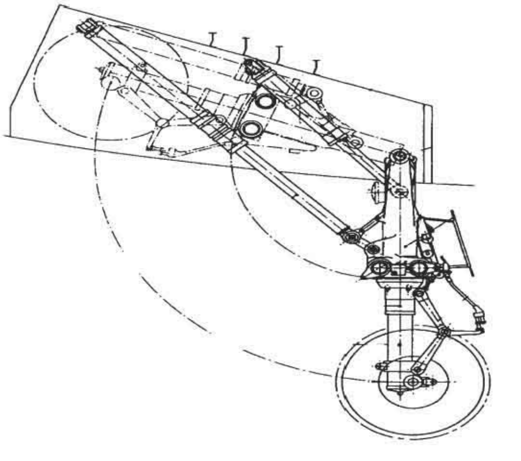


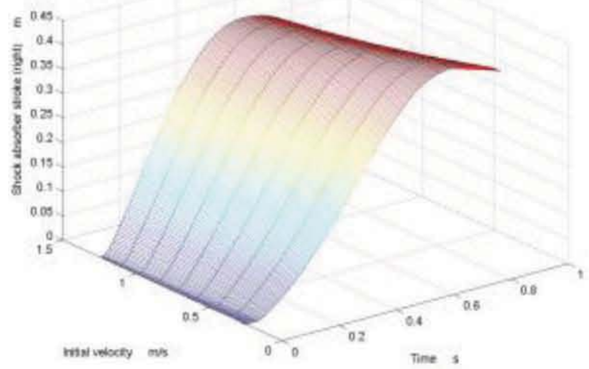
b) Mathematical Model

Since mechanical properties of the landing gear shock absorber are mainly determined by the pneumatic spring force and oleo (hydraulic) damping force, dynamical model of the absorber are presented in the overall multibody system as a force coupling element (highly non-linear!) consisting of these terms. All mechanical characteristics and geometrical data (AA, AC, AD etc.,), needed to establish the model mathematical relations, are assumed according to. The cylinder piston stick-slip friction phenomenon, the floating piston inertia effect and internal seal friction are neglected in the absorber dynamical model presented here.

c) Pneumatic spring force

Depending on the unit operation stage, the pneumatic spring force is determined by the initial inflation pressure in two nitrogen chambers and by the change of volume of the shock absorber (a unit current kinematical configuration). During modeling, it is assumed instantaneous gas compression ratio in accordance with the polytrophic law for compression. Since absorber high rate of compression is to occur during landing impact, the polytrophic exponential term is chosen as n =1.3 during modeling of all internal processes. Having considered geometrical determinations of the gas chambers (volumes *VL1, VL2*) in dependence of unit kinematical configuration and after determination of initial gas inflation pressure, the net pneumatic force is expressed as a non-linear function of shock absorber stroke.





d) Hydraulic damping force

The hydraulic damping force results from the pressure difference associated with the flow through the system of orifices. It is assumed that jet velocities and Reynolds numbers are sufficiently large that the flow is fully turbulent (the orifice area is small in relation to the absorber diameter). As a result, the net damping force is expressed as a square function of the stroke velocity. Since during the compression stroke some orifices become active/inactive (orifices *K3* change their position as the absorber closes), the net hydraulic damping force is modeled via two stage discontinuous function of the absorber stroke velocity. Orifice hydraulic resistance damping coefficients *K1, K2, K3* (Figure 2) are estimated on the basis of orifice geometry and hydraulic fluid density according to. Prior to dynamic simulations of landing aircraft, the dynamical model of shock absorber has been validated by numerical dynamical simulations of landing gear drop test.

e) Landing Impact Shock Absorber Forces

On the basis of the presented aircraft dynamical model, the landing impact dynamic simulations were performed for different initial descent velocities in the range from

$$v\,z1 = 0.25\text{ms-1 to } vz1 = 1.25\text{ms -} \qquad (1)$$

The instant of touchdown of the elastic leg that comes first to the contact with the ground (right elastic leg) is chosen as simulation initial moment. A mass of the aircraft is assumed as 64500 kg and the horizontal velocity equals $v1$ = 67.5 ms-1 . The initial aircraft pitch and roll angles are 10o and 3o respectively, while the aircraft pitching and rolling velocity at the instant of touchdown is assumed to be approximately zero. It should be noted that landing impacts with the indicated touchdown parameters should not represent demanding landing cases for a modern transport airplane.

IV. Related Work

a) Landing Gear Requirements

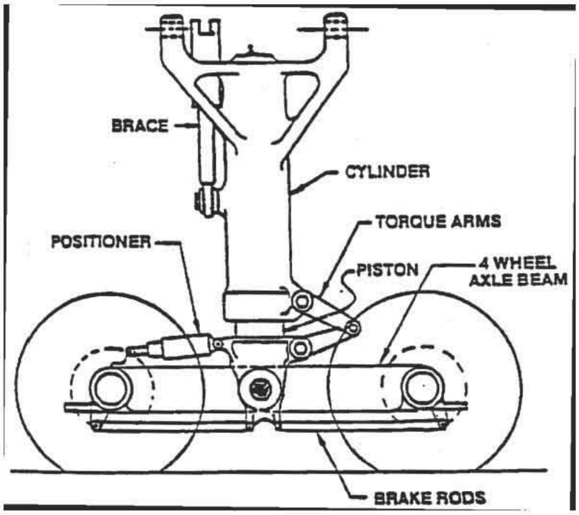
Aircraft landing gears fulfill the tasks of absorbing the vertical energy of the touch-down as well as providing a smooth ground ride before take-off and after landing. However, they perform a number of further duties which are less evident. Jenkins and Young have given a detailed presentation of these requirements which are summarized in.

The most important factors influencing the landing gear design are described in the following paragraphs. System weight is an important aspect in aircraft development. A subsequent major reduction in landing gear weight will be hard to realize because the landing gears are one of the few non-redundant load-paths in an aircraft, and any reduction in reliability from current fail-safe standards is not acceptable. Considering the progress in aircraft light-weight structural design and fuel efficiency the relative weight share of the landing gears can thus be expected to increase further. The position of the landing gears must be such that the aircraft will not tip over under static and tires depends on aircraft weight, maximum force per tire and maximum tire size, and is dictated by pavement bearing strength which may vary from airport to airport. Large civil transport aircraft as the A340, Boeing 747 and MD 11 reach loads of over 20 tons per tire on the main landing gears. During flight the landing gears of practically all modern transport aircraft are retracted. This requires restrictions on the landing gear positioning as these parts have to be stored in a limited space and must not collide with other systems. For this reason, landing gears often possess complicated kinematical layouts of the retraction mechanism for the storage in nacelles in wings and fuselage. Landing gears are usually retracted to the front so they can be released in case of a hydraulic failure and being pushed into position by the air flow, since landing gears have to carry the aircraft weight and have to absorb the energy of the landing impact, the fuselage has to be strengthened in the vicinity of the attachment points. Load alleviation is therefore also of importance for the dimensioning of the fuselage, especially at the attachment points and at the rear of the aircraft. For aircraft with a high maximum landing weight the bending moment resulting from the landing impact is often the critical design case for the rear fuselage. Therefore, comfort improvements obtained by the application of the results of this study must not result in higher attachment loads. Other load cases besides touch-down and rolling are also of great importance. On many airports aircraft are towed, either by push-rods or by special trucks. Cornering exerts high lateral loads on the landing gears.

These factors often lead to higher forces than those obtained at touch-down, especially in lateral and horizontal directions, and have to be taken into consideration as design loads. All requirements mentioned so far have to be met with a system that is one of the few aircraft parts which have no redundancies. And, as airlines look as well at acquisition costs as at DOCs (direct operational costs), the landing gear should be inexpensive and require minimum maintenance. The great number of requirements can only be fulfilled if comprehensive trade-off studies concerning space availability, weight considerations, and structural (stress-) evaluations are performed. Since a large number of engineering disciplines are involved in the suspension development, an integrated design of airframe and landing gears is essential for modern aircraft.

b) Landing Gear Configurations

Landing gears have developed from the simple skids of the first aircraft into the sophisticated and rather complex systems they are today. Originally, the spring function of the suspensions consisted only of the leg elasticity or solid springs. In the years after the First World War the oleo-pneumatic shock absorber became popular because it provided high efficiency by combining the desired spring and damping characteristics in a relatively small unit. At that time, the landing gear configuration with two main landing gears and a tail wheel was common, the most prominent. In the thirties, the retractable landing gear was introduced for reasons of reduced aerodynamic drag.



Since the generation of aircraft of the fifties the landing gear configuration of large transport aircraft has remained principally the same - a steerable nose landing gear and two, or more, main landing gears, one of the earlier aircraft with landing gears of that type being the Lock-head L-1049G Super Constellation, Other possible landing gear systems include floaters, skids, skis, track-type gears, and air cushions. They are applied in specialized aircraft but have found no wide usage. The nose wheel tricycle landing gear configuration has some important advantages when compared to the tail wheel type gear. First, the fuselage is level when the aircraft is on the ground, increasing visibility for the pilot at take-off and at ground maneuvers. Second, the center of gravity is located in front of the main landing gears which leads to a pitching moment of the aircraft at touch-down, automatically reducing lift. Furthermore, the aircraft is stabilized and the pilot can utilize the full brake power. On the other hand, aircraft with tail-wheel landing gear types have an initial angle of attack, allowing a shorter take-off distance. A major disadvantage of the conventional landing gear layout, though, is the fact that the requirements mentioned in section 2.1.1 restrict the designer's choice of landing gear location and layout. With aircraft becoming larger and the number of main landing gears increasing to three or even four, substantial limitations in the designer's freedom occur. The available envelope within which the landing gear has to be located to produce the ideal loading and stability characteristics may no longer be large enough to place the increased number of main landing gears in the fuselage and the wings. A good example is the A380 where the accommodation of four main gears with four- and six-wheel-bogies poses a demanding design challenge.

V. Conclusion

As result of performed dynamic simulations, a time evolution of the shock absorber stroke and total force in the left and right elastic leg during analyzed landing cases are presented in. Dynamic simulation results are presented for different initial descent velocities. It is evident that time diagrams of the shock absorbers' stroke and total force evolution are almost flat immediately after the touchdown. This is due to the fact that, since the shock absorber pneumatics acts as a set-up spring, it is still not active during this period and the tire dynamics affects the overall system motion dominantly. This is more emphasized for the lower initial descent velocities, since for the landing cases with larger touchdown descent velocities the set-up value is quickly reached and damping hydraulic component builds up very fast after the impact, provoking thus a big gradient of the absorber total force soon after the moment of touchdown. Of course, left shock absorber values have an additional time delay due to the fact that left elastic leg comes to the contact with the ground later on during landing process, depending on the aircraft geometry and rolling motion. The discontinuities visible at the shock absorber total force characteristics are due to the orifices different working regime (inactive/active K3 orifices) and due to the change of the absorber's pneumatic force at the point where floating piston of the second-stage pneumatic cylinder becomes active. As it can be seen, during simulated landing impacts the absorber stroke time evolution is within a range≈of 0.35 m. Since it is to be expected that the absorber maximum stroke equals 0.45 m approximately, no upper-point cylinder-piston collision occurred during analyzed landing cases.

References Références Referencias

1. P. Neittaanmäki, T. "Dynamic Simulation Of Transport Aircraft 3d Landing Elastic Leg Shock Absorber Loads" Rossi, S. Korotov, E. Oñate, J. Périaux, and D. Knörzer (eds.) Jyväskylä, 24 - 28 July 2004.
2. D. H. Chester, "Aircraft Landing Impact Parametric Study with Emphasis on Nose Gear Landing Conditions", *Journal of Aircraft*, 39, 394-403 (2002).
3. T. L. Lomax, *"Structural Loads Analysis for Commercial Transport Aircraft: Theory and Practice"*, AIAA Educational Series (1996).
4. H. Wapenhans, *"Dynamik und Regelung von Flugzeugfahrwerken"*, Institute und Lehrstuhl B für Mechanik, Technische Universität München (1989).
5. N. S. Currey, *"Aircraft Landing Gear Design: Principles and Practices"*, AIAA Education Series (1988).
6. Z. Terze et al, "Null Space Integration Method for Constrained Multibody System Simulation with no Constraint Violation", *Multibody System Dynamics*, 6, 229-243 (2001).
7. R. F. Smiley, W. B. Horne, *Mechanical Properties of Pneumatic Tires with Special Reference to Modern Aircraft Tires*, NACA Report No. 4110 (1958).
8. *Aircraft Maintenance Manual A319/A320*, Airbus Industries (2001).
9. F. Pfeifer, C. Glocker, *"Multibody Dynamics with Unilateral Contact"*, John Willey & Sons, New York (1996).
10. B. Milwitzky, F. E. Cook, *"Analysis of Landing Gear Behavior"*, NACA Report No. 1154 (1953).
11. G. Kapadoukas, A. Self, "The Simulation of Aircraft Landing Gear", *System Analysis Modeling Simulation*, 21, 237-245 (1995).
12. D. Yadav, R. P. Ramamoorthy, "Nonlinear Landing Gear Behavior at Touchdown", *Journal of Dynamic Systems, Measurement, and Control, 113, 677-683 (1991).*

This page is intentionally left blank

Verification of Storage Integraty using PDP Technique

J. Shilpa [α] & Prof. M. Madhavi [σ]

Abstract - **Cloud computing is mostly used for highly scalable applications which are very catchable now a day in the world of Internet as on primary needs. The important feature provided to the customers' data is done in unknown systems will do all different transmissions remotely. Using the transmission through remote systems of cloud computing makes users' scares of their data is that secured or not specially in some particular categories like online transmissions and health. These are the threats that create a significant barrier in the cloud computing services. To tackle this crisis, in this paper, we explored a novel highly decentralized information accountability framework. That maintains complete history of the usage of the registered user's data in the cloud. In this way, we explored an object-centered approach that creates enclosing our details of logging history combining with the users' data. We referrers couple of provably-secure PDP schemes which are most accurate when compared to old ones, not only that when compared with schemes that results less efficient than our proposed. In particular, the overhead at the server is low as opposed to linear in the size of the data. Researches using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation.**

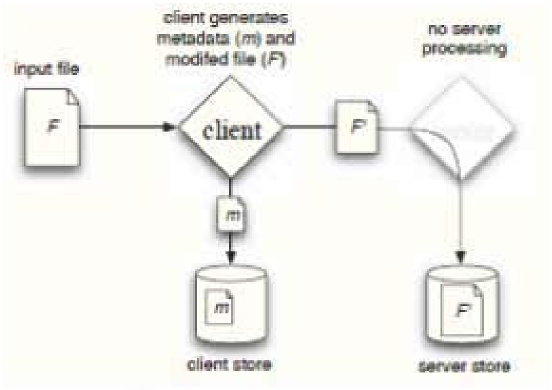
I. Introduction

However, archival storage requires guarantees about the authenticity of data on storage, namely that storage servers possess data. It is insufficient to detect that data have been modified or deleted when accessing the data, because it may be too late to recover lost or damaged data. Archival storage servers retain tremendous amounts of data, little of which are accessed. They also hold data for long periods of time during which there may be exposure to data loss from administration errors as the physical implementation of storage evolves, e.g., backup and restore, data migration to new systems, and changing memberships in peer-to-peer systems. Archival network storage presents unique performance demands.

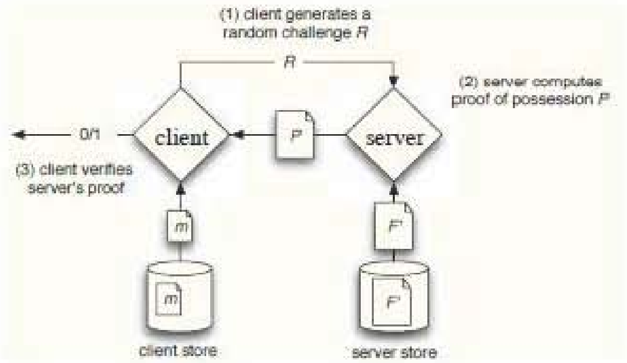
Given that file data are large and are stored at remote sites, accessing an entire file is expensive in I/O costs to the storage server and in transmitting the file across a network. Reading an entire archive, even periodically, greatly limits the scalability of network stores. (The growth in storage capacity has far outstripped the growth in storage access times and bandwidth [44]). Furthermore, I/O incurred to establish data possession interferes with on-demand bandwidth to store and retrieve data. We conclude that clients need to be able to verify that a server has retained file data without retrieving the data from the server and without having the server access the entire file. Previous solutions do not meet these requirements for proving data possession. Some schemes [20] provide a weaker guarantee by enforcing storage complexity: The server has to store an amount of data at least as large as the client's data, but not necessarily the same exact data. Moreover, all previous techniques require the server to access the entire file, which is not feasible when dealing with large amounts of data. We define a model for provable data possession (PDP) that provides probabilistic proof that a third party stores a file. The model is unique in that it allows the server to access small portions of the file in generating the proof; all other techniques must access the entire file. Within this model, we give the first provably-secure scheme for remote data checking. The client stores a small O (1) amount of metadata to verify the server's proof. Also, the scheme uses O (1) bandwidth1. The challenge and the response are each slightly more than 1 Kilobit. We also present a more efficient version of this scheme that proves data possession using a single modular exponentiation at the server, even though it provides a weaker guarantee.

Both schemes use Homomorphic verifiable tags. Because of the Homomorphic property, tags computed for multiple file blocks can be combined into a single value. The client pre-computes tags for each block of a file and then stores the file and its tags with a server. At a later time, the client can verify that the server possesses the file by generating a random challenge against a randomly selected set of file blocks. Using the queried blocks and their corresponding tags, the server generates a proof of possession. The client is thus convinced of data possession, without actually having to retrieve file blocks. The efficient PDP scheme is the fundamental construct underlying an archival introspection system that we are developing for the long-term preservation of Astronomy data.

Author α : (M.Tech), CSE Dept, ASRA Hyderabad
E-mail : javvajishilpa@gmail.com
Author σ : (M.Tech), CSE, Associate Professor, ASRA Hyderabad.
E-mail : madhavi_3101@yahoo.co.in



(a) Pre-Process and Store



(b) Verify Server Possession

We are taking possession of multi-terabyte Astronomy databases at a University library in order to preserve the information long after the research projects and instruments used to collect the data are gone. The database will be replicated at multiple sites. Sites include resource-sharing partners that exchange storage capacity to achieve reliability and scale. As such, the system is subject to freeloading in which partners attempt to use storage resources and contribute none of their own [20]. The location and physical implementation of these replicas are managed independently by each partner and will evolve over time. Partners may even out source storage to third-party storage server providers [23].

Efficient PDP schemes will ensure that the computational requirements of remote data checking do not unduly burden the remote storage sites. We implemented our more efficient scheme (E-PDP) and two other remote data checking protocols and evaluated their performance. Experiments show that probabilistic possession guarantees make it practical to verify possession of large data sets. With sampling, E-PDP verifies a 64MB file in about 0.4 seconds as compared to 1.8 seconds without sampling. Further, I/O bounds the performance of EPDP; it generates proofs as quickly as the disk produces data. Finally, E-PDP is 185 times faster than the previous secure protocol on 768 KB files.

II. Systems Overview

a) Provable Data Possession (PDP)

We describe a framework for provable data possession. This provides background for related work and for the specific description of our schemes. A PDP protocol (Fig. 1) checks that an outsourced storage site retains a file, which consists of a collection of n blocks. The client C (data owner) pre-processes the file, generating a piece of metadata that is stored locally, transmits the file to the server S, and may delete its local copy. The server stores the file and responds to challenges issued by the client. Storage at the server is in (n) and storage at the client is in O (1), conforming to our notion of an outsourced storage relationship.

i. Threat Model

The server S must answer challenges from the client C; failure to do so represents a data loss. However, the server is not trusted: Even though the file is totally or partially missing, the server may try to convince the client that it possesses the file. The server's motivation for misbehavior can that has not been or is rarely accessed (for monetary reasons), or be diverse and includes reclaiming storage by discarding data hiding a data loss incident (due to management errors, hardware failure, compromise by outside or inside attacks etc). The goal of a PDP scheme that achieves probabilistic proof of data possession is to detect server misbehavior when the server has deleted a fraction of the file.

III. Evaluation

a) Probabilistic Framework

Our PDP schemes allow the server to prove possession of select blocks of F. This "sampling" ability greatly reduces the workload on the server, while still achieving detection of server misbehavior with high probability. We now analyze the probabilistic guarantees offered by a scheme that supports block sampling. Assume S deletes t blocks out of the n-block file F. Let c be the number of different blocks for which C asks proof in a challenge. Let X be a discrete random variable that is defined to be the number of blocks chosen by C that match the blocks deleted by S. We compute PX, the probability that at least one of the blocks picked by C matches one of the blocks deleted by S. We have:

$$P_X = P\{X \geq 1\} = 1 - P\{X = 0\} =$$

$$1 - \frac{n-t}{n} \cdot \frac{n-1-t}{n-1} \cdot \frac{n-2-t}{n-2} \cdot \ldots \cdot \frac{n-c+1-t}{n-c+1}.$$

Since $\frac{n-i-t}{n-i} \geq \frac{n-i-1-t}{n-i-1}$, it follows that:

$$1-\left(\frac{n-t}{n}\right)^c \leq P_X \leq 1-\left(\frac{n-c+1-t}{n-c+1}\right)^c.$$

PX indicates the probability that, if S deletes t blocks of the file, then C will detect server misbehavior after a challenge in which it asks proof for c blocks. Fig. 3 plots PX for different values of n, t, c. interestingly, when t is a fraction of the file, C can detect server misbehavior with a certain probability by asking proof for a constant amount of blocks, independently of the total number of file blocks: e.g., if t = 1% of n, then C asks for 460 blocks and 300 blocks in order to achieve PX of at least 99% and 95%, respectively.

b) Implementation and Experimental Results

We measure the performance of E-PDP and the benefits of sampling based on our implementation of E-PDP in Linux. As a basis for comparison, we have also implemented the scheme of Deswarte et al. [17] and Filho et al. [19] (B-PDP), and the more efficient scheme in [20] (MHT-SC) suggested by David Wagner (these schemes are described in Appendix B). All experiments were conducted on an Intel 2.8 GHz Pentium IV system with a 512 KB cache, an 800 MHz EPCI bus, and 1024 MB of RAM. The system runs Red Hat Linux 9, kernel version 2.4.22. Algorithms use the crypto library of Open SSL version 0.9.8b with a modulus N of size 1024 bits and files have 4KB blocks. Experiments that measure disk I/O performance do so by storing files on an ext3 file system on a Seagate Barracuda 7200.7 (ST380011A) 80GB Ultra ATA/100 drives. All experimental results represent the mean of 20 trials. Because results varied little across trials, we do not present confidence intervals.

i. *Server Computation*

The next experiments look at the worst-case performance of generating a proof of possession, which is useful for planning purposes to allow the server to allocate enough resources. For E-PDP, this means sampling every block in the file, while for MHT-SC this means computing the entire hash tree. We compare the computation complexity of E-PDP with other algorithms, which do not support sampling. All schemes perform an equivalent number of disk and memory accesses.

In step 3 of the Gen Proof algorithm of S-PDP, S has two ways of computing ρ: Either sum the values ajmij (as integers) and then exponentiation to this sum or exponentiation gs to each value ajmij and then multiply all values. We observed that the former choice takes considerable less time, as it only involves one exponentiation to a (|mi| + ℓ + log2(c))-bit number, as opposed to c exponentiations to a (|mi| + ℓ)-bit number (typically, ℓ = 160).

ii. *Pre-Processing*

In preparing a file for outsourced storage, the client generates its local metadata. In this experiment, we measure the processor time for metadata generation only. This does not include the I/O time to load data to the client or store metadata to disk, nor does it include the time to transfer the file to the server. Fig. 5(b) shows the pre-processing time as a function of file size for BPDP, MHT-SC and E-PDP. E-PDP exhibits slower preprocessing performance. The costs grow linearly with the file size at 162 KB/s. E-PDP performs an exponentiation on every block of the file in order to create the per block tags. For MHTSC, preprocessing performance mirrors challenge performance, because both protocol steps perform the same computation. It generates data at about 433 KB/s on average.

IV. Related Work

Deswarte et al. [17] and Filho et al. [19] provide techniques to verify that a remote server stores a file using RSA-based hash functions. Unlike other hash-based approaches, it allows a client to perform multiple challenges using the same metadata. In this protocol, communication and client storage complexity are both O(1). The limitation of the algorithm lies in the computational complexity at the server, which must exponentiation the entire file, accessing the entire file's blocks. Further, RSA over the entire file is extremely slow — 20 seconds per Megabyte for 1024-bit keys on a 3.0 GHz processor [19]. In fact, these limitations led us to study algorithms that allowed for sub-file access (sampling). We implement this protocol for comparison with our PDP scheme and refer to it as B-PDP (basic PDP). A description of B-PDP is provided in Appendix B. Shah et al. [42] use a similar technique for third-party auditing of data stored at online service providers and put forth some of the challenges associated with auditing online storage services. Schwarz and Miller [40] propose a scheme that allows a client to verify the storage of m/n erasure-coded data across multiple sites even if sites collude. The data possession guarantee is achieved using a special construct, called an "algebraic signature": A function that fingerprints a block and has the property that the signature of the parity block equals the parity of the signatures of the data blocks. The parameters of the scheme limit its applicability: The file access and computation complexity at the server and the communication complexity are all linear in the number of file blocks (n) per challenge. Additionally, the security of the scheme is not proven and remains in question.

a) Command Line-Based Data Processing

The systems described in this section are implemented by monitoring a command line interpreter which allows them to passively capture and store the information necessary to assemble a retrospective view on data processing. As defined by Merriam-Webster [2001], an audit trail is a record of a sequence of events (as actions performed by a computer) from which a history can be reconstructed, and thus serves as a form of lineage. Becker and Chambers [1988] describe a system for auditing data analyses steps for a particular implementation of S, a language and interactive environment for statistical analysis and display. Their intention is to provide a tool for a user to investigate the dependencies among steps following an exploratory S analysis session. User-entered statements evaluated by S, including the associated creation and modification of data objects resulting from those statements, are dynamically recorded in an audit file. An audit facility parses the audit file into a linked list structure, which it then uses to respond to ad hoc queries and generate custom so called audit plots to display analysis step dependencies. The prototype audit facility Becker and Chambers describe has not been implemented in contemporary versions of the S system such as S-Plus [Insightful Corporation 2003].

b) Script- and Program-Based Data Processing

The systems described in this section assemble a retrospective view on processing using information encoded directly in user-supplied scripts or programs. ESSW [Frew and Bose 2001] captures lineage metadata for objects involved in scientific processing performed with application-specific scripts as well as general scripting languages such as Perl. ESSW uses custom application programming interface (API) commands within Perl wrapper scripts—code that circumscribes the functions, algorithms, or other data transformations of interest—to construct lineage. The lineage of an item is queried through a web application, and results are displayed diagrammatically using the Webdot Web service interface included with the Graphviz set of graphing tools [AT&T 2001].

c) WFMS-Based Data Processing

Extending some of the concepts in GOOSE, the Geo-Opera extension of the OPERA kernel [Alonso and Hagen 1997b; Alonso et al. 1998] provides a management system for distributed geoprocessing that incorporates elements of workflow management, transaction processing, and lineage tracking for an Earth Science example of hydrologic modeling. Data files and transformations used by hydrologic models reside outside of the system. Once transformations are registered in Geo-Opera, they are tracked as task objects internal to the system. Lineage relationships between objects are established by defining the control flow between internal task objects and data. When data is located outside the system, it is registered in the system as an external object. Each external object includes a set of system-maintained attributes supporting automated versioning, change propagation, and lineage recording.

d) Query-Based Data Processing

Brown and Stonebraker [1995] and Woodruff and Stonebraker [1997] propose a method for providing detailed or finegrained lineage for scientific processing applications. A goal of their research is delivering to scientists, through data lineage, the ability to investigate the source of faulty or anomalous data sets and the ability to determine those derived data sets affected by faulty or anomalous inputs or algorithms. Specifically, Woodruff and Stonebraker [1997] address the problem of recovering the origins of single elements in large arrays of data that have undergone a series of transformations. Creating individual metadata entries to assist with such a task would require prohibitive effort and storage size.

e) Service-Based Data Processing

The Chimera Virtual Data System (VDS) matches the scope and ambition of the Grid, targeting invocations of data transformations in a "distributed, multi-user, multi-institutional environment" [Foster et al. 2003]. Chimera features a language, the Virtual Data Language (VDL), for defining and manipulating data derivation procedures which are stored in a Virtual Data Catalog (VDC). The VDL serves as a general wrapper for program execution, capable of accommodating Grid request planning. The language is also used to query the VDC to discover or invoke the lineage or pipeline of computations that created a particular data object. Chimera is described as a virtual data prototype because it is capable of creating a directed acyclic graph (DAG) of distributed computations that can be submitted to the Grid to regenerate a given data object.

V. Conclusion

We proposed innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. Our approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge.

In the future, we plan to refine our approach to verify the integrity of the JRE and the authentication of JARs [20]. For example, we will investigate whether it is possible to leverage the notion of a secure JVM [18] being developed by IBM. This research is aimed at providing software tamper resistance to Java applications. In the long term, we plan to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of traveling content. We would like to support a variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance controls.

References Références Referencias

1. P. Ammann and S. Jajodia, "Distributed Timestamp Generation in Planar Lattice Networks," ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598- 609, 2007.
3. E. Barka and A. Lakas, "Integrating Usage Control with SIP-Based Communications," J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.
4. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.
5. R. Bose and J. Frew, "Lineage Retrieval for Scientific Data Processing: A Survey," ACM Computing Surveys, vol. 37, pp. 1- 28, Mar. 2005.
6. P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '06), pp. 539-550, 2006.
7. B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.
8. OASIS Security Services Technical Committee, "Security Assertion Markup Language (saml) 2.0," http://www.oasis-open.org/committees/tchome.php ?wg abbrev=security, 2012.
9. R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "A Logic for Auditing Accountability in Decentralized Systems," Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.
10. B. Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.
11. Y. Chen et al., "Oblivious Hashing: A Stealthy Software Integrity Verification Primitive," Proc. Int'l Workshop Information Hiding, F. Petitcolas, ed., pp. 400-414, 2003.
12. S. Etalle and W.H. Winsborough, "A Posteriori Compliance Control," SACMAT '07: Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 11-20, 2007.
13. X. Feng, Z. Ni, Z. Shao, and Y. Guo, "An Open Framework for Foundational Proof-Carrying Code," Proc. ACM SIGPLAN Int'l Workshop Types in Languages Design and Implementation, pp. 67-78, 2007.
14. Flickr, http://www.flickr.com/, 2012.
15. R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies, pp. 1-14, 2009.
16. J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing," Computer, vol. 34, no. 8, pp. 57-66, Aug. 2001.
17. J.W. Holford, W.J. Caelli, and A.W. Rhodes, "Using Self- Defending Objects to Develop Security Aware Applications in Java," Proc. 27th Australasian Conf. Computer Science, vol. 26, pp. 341-349, 2004.
18. Trusted Java Virtual Machine IBM, http://www.almaden.ibm.com/cs/projects/jvm/, 2012.
19. P.T. Jaeger, J. Lin, and J.M. Grimes, "Cloud Computing and Information Policy: Computing in a Policy Cloud?," J. Information Technology and Politics, vol. 5, no. 3, pp. 269-283, 2009.
20. R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, "Towards a Theory of Accountability and Audit," Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 152-167, 2009.

This page is intentionally left blank

Economical Efficient for High Scalable Applications

Sreedevi Pogula [α] & M. Ganesh Kumar [σ]

Abstract - **Service-oriented architecture (SOA) paradigm for the purpose of large-scale applications offers meaningful cost savings by rework existing services. However, the high oddity of client appeal and the allocated character of the access may depreciate service response time and chance. Static cloning of components in database for placing load spikes need efficient resource planning and also uses the cloud infrastructure. Moreover, no service chance gives trust is provided in situations like datacenter crashes. In this paper, we explore a cost-efficient usage for dynamic and geographically-diverse cloning of elements in a cloud computing infrastructure that perfectly adapts to load differences and provides service chance guarantees. When comes to economic level, components hire server opportunities and clones or trashes themselves based to self optimizing situations. We proved in real time applications that such an access better in response time even full cloning of the components in all servers, while providing service chance guarantees under failures.**

I. Introduction

Cloud computing is deemed to replace high capital expenses for infrastructure with lower operational ones for renting cloud resources on demand by the application providers. However, with static resource allocation, a cluster system would be likely to leave 50% of the hardware resources (i.e. CPU, memory, disk) idle, thus baring unnecessary operational expenses without any profit (i.e. negative value flows). Moreover, as clouds scale up, hardware failures of any type are unavoidable.

A efficient online application is of capable to resist traffic spikes and huge crowds efficiently. And also the service offered by the application have to be volatile to different types of failures. A perfect solution opponent to load differences would be static over-provisioning of resources, at last it result into resource underutilization for most of the time. Resource redundancy should be employed to increase service reliability and chance, yet in a cost-effective way. Most importantly, as the size of the cloud increases its administrative overhead becomes unmanageable. The cloud resources for an application should be self managed and adaptive to load variations or failures. In this paper, we propose a middleware ("Scattered Autonomic Resources", referred to as Scarce) for supple sharing to avoid stranded and underutilized computational resources that dynamically adapts to changing conditions, such as failures or load variations. Our middleware simplifies the development of online appliances composed by multiple independent components (e.g. web services) following the Service Oriented Architecture (SOA) principles. We consider a virtual economy, where components are treated as individually rational entities that rent computational resources from servers, and migrate, replicate or exit according to their economic fitness. This fitness expresses the difference between the utility offered by a specific application component and the cost for retaining it in the cloud. The server rent price is an increasing function of the utilization of server resources. Moreover, components of a certain applications are dynamically replicated to geographically-diverse servers according to the chance requirements of the application. Our access combines the following unique characteristics:

- Adaptive component replication for accommodating load variations.
- Geographically-diverse placement of clone component instances.
- Cost-effective placement of service components for supple load balancing.
- Decentralized self-management of the cloud resources for the application.

Having implemented a full prototype of our access, we experimentally prove that it effectively accommodates load spikes; it provides a dynamic geographical replica placement without thrashing and cost-effectively utilizes the cloud resources. Specifically, we found that our access offers lower response time even than full replication of the service components to all servers.

II. Motivation - Running Example

Building an application that both provides robust guarantees against failures (hardware, network, etc.) and handles dynamically load spikes is a non-trivial task. As a running example, we have developed a simple web application for selling e-tickets (print@ home) composed by 4 independent components:

- A web front-end, which is the entry point of the application and serves the HTML pages to the end user.

Author α : M.Tech, CSE Dept, HITS, Hyderabad.
E-mail : sreedevigsky.net@gmail.com
Author σ : M.Tech, Asst. Prof. MREC, Hyderabad.
E-mail : ganeshkumar.programs@gmail.com

- A user manager for managing the profiles of the customers.
- The profiles are stored in a highly scalable, eventually consistent, allocated, structured key-value store.
- A ticket manager for managing the amount of available tickets of an event. This component uses a relational database management system (MySQL).
- An e-ticket generator that produces e-tickets in PDF format (print@home).

Each component can be regarded as a stateless, standalone and self-contained web service. Figure 1 depicts the application architecture. A token (or a session ID) is assigned to each customer's browser by the web front-end and is passed to each component along with the appeal. This token is used as a key in the key-value database to store the details of the client's shopping cart, such as the number of tickets ordered. Note that even if the application uses the concept of sessions, the components themselves is stateless (i.e. they do not need to keep an internal state between two appeals).

This application is highly sensitive to traffic spikes, when, for example, tickets for a concert of a famous band are sold. If the spike is foreseeable, one wants to be able to add spare servers that will be used transparently by the application for a short period of time, without having to reconfigure the application. After this period, the servers have to be removed transparently to the end users. As this application is business-critical, it needs to be deployed on different geographical regions, hence on different datacenters.

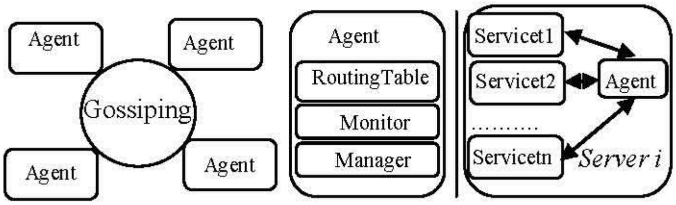
III. Scarce: The Quest of Autonomic Appliances

a) The Access

We consider appliances formed by many independent and stateless components that interact together to provide a service to the end user, as in Service Oriented Architecture (SOA). A component is self-managing, self-healing and is hosted by a server, which is in turn allowed to host many different components. A component can stop, migrate or replicate to a new server according to its load.

b) Server Agent

The server agent is a special component that resides at each server and is responsible for managing the resources of the server according to our economic-based access, as shown in Figure 2. Specifically, this agent is responsible for starting and stopping the components of the various appliances at the local server, as well as checking the "health" of the services (e.g. by verifying if the service process is still running, or by firing a test request and checking that the corresponding reply is correct). The agent knows the properties of every service that composes the application, such as the path of the service executable, its minimum and maximum replication factor. This knowledge is acquired when the agent starts, by contacting another agent (referred to as "bootstrap agent"). Any running agent participating in the application cluster can act as a bootstrap agent.



c) Routing Table

Instead of using a centralized repository for locating services, each server keeps locally a mapping between components and servers. It is maintained by a gossiping algorithm (see Figure 2), where each agent contacts a random subset (log (N) where N is the total number of servers) of remote agents and exchanges information about the services running on their respective server. Contrary to usual web services architectures, there is no central repository [such as a UDDI registry (uddi.xml.org)] for locating a service, but each agent maintains its own local registry (i.e. the routing table), as shown in Table I.

The Local Routing Table

Component	*Server*
Component1	*Server A, Server B*
Component2	*Server B, Server C*
Component3	*Server A*

A component may be hosted by several servers; therefore we consider 4 different policies that a server s may use for choosing the replica of a component:

1. A proximity-based policy: thanks to the labels attached to each server, the geographically nearest replica is chosen.
2. A rent-based policy: the least loaded server is chosen; this decision is based on the rent price of the servers.
3. A random-based policy: a random replica is chosen.
4. A net benefit-based policy: the geographically closest and least loaded replica. For every replica of the component residing at server j, we compute a weight:

d) Economic Model

Service replication should be highly adaptive to the processing load and to failures of any kind in order to maintain high service chance. To this end, each component is treated by the server agent as an individual optimizer that acts autonomously so as to ascertain the pre-specified chance guarantees and to balance its economic fitness. Time is assumed to be split into epochs. At every epoch, the server agent verifies from the local routing table that the minimum number of replicas for every component is satisfied; thus, no global or remote knowledge is required. If the required chance level is not satisfied and if the service is not already running locally, the agent starts the service. When the service has started, the server agent informs all others by using a hierarchical broadcast to update their respective routing tables. At each epoch, a service pays a virtual rent r to the servers where it is running. The virtual rent corresponds to the usage of the server resources, such as CPU, memory, network, disk (I/O, space).

To avoid oscillations of a replica among servers, the migration is only allowed if the following migration conditions apply:

1. The minimum chance is still satisfied using the new server,
2. The absolute price difference between the current and the new server is greater than a threshold,
3. The usages of the current server s are above a soft limit.
4. Replicate: if it has positive balance for the last f epochs, it may replicate. For replication, a component has also to verify that it can afford the replication by having a positive balance b0 for consecutive f epochs:

IV. Evaluation

a) Customer Registration

Customer has to enclose their details into the server. In this page several fields are mentioned name, e-mail id, phone number etc.., and also to provide card details are available and visa card, master card, one more advantage is expiry date and cvc no standard for card verification number in this cvc number is checking their card details.

The main advantage login as customer they can select their ticket details, but each ticket details are identified by one secrete key based on that secrete key it will process.

b) User Manager

The user manager for managing the profile of the customers, the profiles are stored in highly scalable, distributed, structured key value User manager login they will monitor how many number of users are requested the ticket. We consider many independent components that interact together to provide you service to the end user as SOA.

- ✓ In this page session is set for 60 Seconds. It beyond 60 seconds session will be expired.
- ✓ Distributed Optimization Algorithm is used. It maintains the all users' profile, also gossiping.
- ✓ The user manager Components are there: from, to, date, quota, type ticket, class, train number, etc…..
- ✓ The user manager including Sub modules: train details, passenger details, card details finally it will generate ticket format.

Designing : The four modules are using asp.net and coding c#.

Database : Sql Server.

c) Ticket Manager

The ticket manager for managing the amount of available tickets of an event. In this application to maintain how many members is ticket booking. Store user profile and all profiles are maintained using one of the controls is grid view control to visible in all booking details.

Grid view is store multiple records and retrieve through database in this control one more advantage is paging and modification, update, delete operation are applied.

d) E-Ticket Generator

An e-ticket generator that produces e-tickets in PDF format, it will generate automatically all details in report format. And how many members ticket sanctioned to main all ticket details in this module using grid view control.

Grid view is store multiple records and retrieve through database in this control one more advantage is paging and modification, update, delete operation are applied.

i. *Experimental Setup we employ two different test bed settings*

A single application setup consisting of 7 servers and a multi-application setup consisting of 15 servers. In the former setup, the cloud resources serve 1 application and in the latter one 3 appliances. We assume that the components of the application may require up to all servers in the cloud. We simulate the behavior of a typical user of the e-ticket application of Section II by performing the following actions:

1) Request the main page that contains the list of entertainment events;
2) Request the details of an event A;
3) Request the details of an event B;
4) Request again the details of the event A;
5) Login into the application and view user account;
6) Update some personal information;
7) Buy a ticket for the event A;
8) Download the corresponding ticket in PDF.

A client continuously performs this list of actions over a period of 1 minute. An epoch is set to 15 seconds and an agent sends gossip messages every 5 seconds. Moreover, the default routing policy is the random-based policy. We consider two different placements of the components:

- A static access where each component is assigned to a server by the system administrator.
- A dynamic access where all components are started on a single server and dynamically migrate/ replicate/stop according to the load or the hardware failures.

ii. *Results Dynamic vs static replica placement*

First, we employ the single-application experimental setup to compare our access with static placements of the components, where we consider two cases: i) each different component is hosted at a different dedicated server; ii) full replication, where every component is hosted at every server. The response time of the 95% percentile of the appeal is depicted in Figure 3. In the static placement (i), where a component runs on its own server, the response time is lower bounded by that of the slowest component (in our case, the service for generating PDF tickets). Thus, the response time increases exponentially when the server hosting this component is overloaded. In the case of full replication [static placement (ii)], the appeal are balanced among all servers, keeping the latency relatively low, even when the amount of concurrent users is meaningful. In the dynamic placement access, all components are hosted at a single server at startup: then, when the load increases, a busy component is allowed to replicate, and unpopular components may replicate to a less busy server. Our economic access achieves better performance than full replication, because the total amount of CPU available in the cloud is used in an adaptive manner by the components: processing intensive (or "heavy") components migrate to the least loaded servers and heavily used components are assigned more resources than others. Therefore, the cloud resources are shared according to the processing needs of components and no cloud resources are wasted by over-provisioning.

V. Future Enhancement

We will continue to research on security mechanisms that support: to maintain data securable and highly allocated data are the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system. Cloud computing providing unlimited infrastructure to store and execute customer data and program. As customers you do not need to own the infrastructure, they are merely accessing or renting; they can forego capital expenditure and consume resources as a service, paying instead for what they use.

a) *Security a Major Concern*

1. Security concerns arising because both customer data and program are residing Provider Premises.
2. Security is always a major concern in Open System Architectures.

b) *Data Centre Security*

1. Professional Security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means.
2. When an employee no longer has a business need to access datacenter his privileges to access datacenter should be immediately revoked.
3. All physical and electronic access to data centers by employees should be logged and audited routinely.
4. Audit tools so that users can easily determine how their data is stored, protected, used, and verify policy enforcement.

c) *Data Location*

1. When user uses the cloud, user probably won't know exactly where your data is hosted, what country it will be stored in?
2. Data should be stored and processed only in specific jurisdictions as define by user.
3. Provider should also make a contractual commitment to obey local privacy requirements on behalf of their customers,
4. Data-centered policies that are generated when a user provides personal or sensitive information that travels with that information throughout its lifetime to ensure that the information is used only in accordance with the policy.

In this application simulation of e-ticket it is used to provide service to end user and data is most securable, allocated and reduce cost, large-scale allocated appliances offers meaningful cost savings by rework existing service. Over come to centralize sever and Increase response time and no chance of server hang, Network bandwidth is increases.

VI. Related Work

There is meaningful related work in the area of economic accesses for allocated computing. In [4], an access is proposed for the utilization of idle computational resources in a heterogeneous cluster. Agents assign computational tasks to servers, given the budget constrain for each task, and compete for CPU time in sealed-bid second-price auction held by the latter. In a similar setting, Popcorn access [5] employs a first-price sealed-bid auction model. Cougaar allocated multi-agent system [6] has an adaptivity engine which monitors load by employing periodic "health-check" messages. An elected agent operates as load balancer and determines the appropriate node for each agent that must be relocated based on runtime performance metrics, e.g. message traffic and memory consumption. Also, a coordinator component determines potential failure of agents and restarts them. However, cost-effectiveness among the objectives of Cougaar, and moreover our access is more lightweight in terms of communication overhead. In [7], a virtual currency (called Egg) is used for expressing a user's willingness to pay as well as a provider's bid for a accepting the job, and finally is given to the winning provider as compensation for job execution. Providers estimate their opportunity cost for accepting a job and regularly announce a unit price table to a central entity for a specific period. The central Egg entity informs all candidate providers about the new job and acquires responses (cost estimations). However, the access in [7] is centralized and it does not provide chance guarantees. In [8], appliances trade computing capacity in a free market, which is centrally hosted, and are then automatically activated in virtual machines on the traded nodes on-call of traffic spikes. The appliances are responsible for declaring their required number of nodes at each round based on usage statistics and allocate their statically guaranteed resources or more based on their willingness to pay and the equilibrium price; this is the highest price at which the demand saturates the cluster capacity. However, [8] does not deal with chance guarantees, as opposed to our access. Also, our access accommodates traffic spikes in a prioritized way per application without requiring the determination of the equilibrium price. Pautasso et al. ropose in [9] an autonomic controller for the JOpera allocated service composition engine over a cluster. The autonomic controller starts and stops navigation (i.e. scheduler) and dispatcher (i.e. execution and composition) threads based on several load-balancing policies that depend on the size of their respective processing queues. The autonomic component also has self-healing capabilities. However, proper thread placement in the cluster and communication overhead among threads are not considered in [9]. Also, in [10], SLA agreements for a specific QoS level for web services are established. However, monitoring of SLA compliance may require the involvement of third-parties or centralized services. A bio-networking access was proposed in [11], where services are provided by autonomous agents that implement basic biological behaviors of swarms of bees and ant colonies such as replication, migration, or death. To survive in the network environment, an agent obtains "energy" by providing a service to the users. Moreover, several implementation frameworks exist to build reliable SOA-based appliances: [12] is a mechanism for specifying fault tolerant web Service compositions, [13] is a virtual communication layer for transparent service replication, and [14] is a framework for the active replication of services across sites. These frameworks do not consider dynamic adaptation to changing conditions, such as load spikes, or do not provide guarantees about geographical diversity of replicas.

VII. Conclusion

A web front-end, which is the entry point of the application and serves the HTML pages to the end user. A user manager for managing the profiles of the customers. The profiles are stored in a highly scalable, eventually consistent, allocated, structured key-value store. A ticket manager for managing the amount of available tickets of an event. This component uses a relational database management system. An e-ticket generator that produces e-tickets in PDF format (print home). The main advantage login as customer they can select their ticket details. but each ticket details are identified by one secrete key. Based on that secrete key it will process. This project is used to manage efficiently with less cost by using secretary keys. Every transaction is identified based on this key only.

The complete communication between customer, user manager, ticket manager and e-ticket generator with centralized server. Each component can be regarded as a stateless, standalone and self-contained web service. Figure 1 depicts the application architecture. A token (or a session ID) is assigned to each customer's browser by the web front-end and is passed to each component along with the appeal.

References Références Referencias

1. "The apache cassandra project," http://cassandra.apache.org/.
2. L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.
3. N. Bonvin, T. G. Papaioannou and K. Aberer, "Cost-efficient and differentiated data chance guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.
4. C. A. Waldspurger, T. Hogg, B. A. Huberman, J. O. Kephart, and W. S. Stornetta, "Spawn: A allocated computational economy," IEEE Transactions on Software Engineering, vol. 18, pp. 103–117, 1992.
5. O. Regev and N. Nisan, "The popcorn market. online markets for computational resources," Decision Support Systems, vol. 28, no. 1-2, pp. 177 – 189, 2000.

6. A. Helsinger and T. Wright, “Cougaar: A robust configurable multi agent platform,” in Proc. of the IEEE Aerospace Conference, 2005.
7. J. Brunelle, P. Hurst, J. Huth, L. Kang, C. Ng, D. C. Parkes, M. Seltzer, J. Shank, and S. Youssef, “Egg: an extensible and Economics-inspired open grid computing platform,” in Proc. of the GECON, Singapore, May 2006.
8. J. Norris, K. Coleman, A. Fox, and G. Candea, “Oncall: Defeating spikes with a free-market application cluster,” in Proc. of the International Conference on Autonomic Computing, New York, NY, USA, May 2004.
9. C. Pautasso, T. Heinis, and G. Alonso, “Autonomic resource provisioning for software business processes,” Information and Software Technology, vol. 49, pp. 65–80, 2007.
10. A. Dan, D. Davis, R. Kearney, A. Keller, R. King, D. Kuebler, H. Ludwig, M. Polan, M. Spreitzer, and A. Youssef, “Web services on demand: Wsla-driven automated management,” IBM Syst. J., vol. 43, no. 1, pp. 136–158, 2004.
11. M. Wang and T. Suda, “The bio-networking architecture: a biologically inspired access to the design of scalable, adaptive, and survivable/ available network appliances,” in Proc. of the IEEE Symposium on Appliances and the Internet, 2001.
12. N. Laranjeiro and M. Vieira, “Towards fault tolerance in web services compositions,” in Proc. of the workshop on engineering fault tolerant systems, New York, NY, USA, 2007.
13. C. Engelmann, S. L. Scott, C. Leangsuksun, and X. He, “Transparent symmetric active/active replication for service level high chance,” in Proc. of the CCGrid, 2007.
14. J. Salas, F. Perez-Sorrosal, n.-M. M. Pati and R. Jim´enez- Peris, “Ws-replication: a framework for highly available web services,” in Proc. of the WWW, New York, NY, USA, 2006, pp. 357–366.
15. M. Wang and T. Suda, “The bio-networking architecture: a biologically inspired access to the design of scalable, adaptive.

An Efficient Operations and Management Challenges of Next Generation Network (NGN)

Salavadi Ananda Kumar [α] & Dr. K. E. Sreenivasa Murthy [σ]

Abstract- **Next Generation Network (NGN) is envisioned to be an inter-working environment of heterogeneous networks of wired and wireless access networks, PSTN, satellites, broadcasting, etc., all interconnected through the service provider's IP backbone and the Internet. NGN uses multiple broadband, QoS-enabled transport technologies and service-related functions independent from underlying transport-related technologies. The operations and management of such interconnected networks are expected to be much more difficult and important than the traditional network environment. In this paper, we present an overview of the current status towards the management of NGN and discuss challenges in operating and managing NGN. We also present the operations and management requirements of NGN in accordance with the challenges and verified two routing protocols for QOS support and providing security using caesarchiper encryption/decryption in Ad-hoc networks and also provide QOS for wired networks by AQM techniques and simulated results of AQM, Routing protocols using NS-2 and Encryption/Decryption using Matlab tools.**

General terms: qos aqm, ngn, red and drop tail.

I. Introduction

NGN is envisioned to be an answer to network operators and service providers to replace existing telephone networks as well as to introduce a new converged service platform between fixed and mobile telecommunication businesses [1]. It is generally agreed that the main difference between traditional telecommunication networks and NGN is the shift from separate and vertically integrated application-specific networks to a single network capable of carrying any services. NGN is essentially about delivering new services that are available to any place, at any time, on any device, through any customer-chosen access mechanism. NGN is expected to co-exist and inter-work among wired networks (e.g., xDSL, Metro Ethernet, FTTH, leased lines, ISDN), wireless networks (e.g., 2G, 3G, WLAN, WiMAX/WiBro) as well as satellites and broadcasting networks, all interconnected through the service provider's IP backbone networks and the Internet.

In this heterogeneous networking environment, in addition to the traditional challenges such as security, QoS, and charging, new challenges such as generalized mobility, and network discovery and selection exist.

Providing effective, secure and efficient operations and management of the envisioned NGN environment is a huge challenge. In order to provide the creation, deployment, and management of all kinds of services, NGN operations are highly dependent on flexible and efficient management systems and processes [2]. When the networks are evolving towards NGN, the scenario to support various services would become more complex.

The carrying of diverse traffic such as voice, data, video or signaling would be possibly integrated onto one common platform, which would call for the corresponding network management systems.

The ITU-T Recommendation Y.2401 [5] presents the management requirements, general principles and architectural requirements for managing NGN to support business processes to plan, provision, install, maintain, operate and administer NGN resources and services [4].

Thus, we examine the challenges facing the management of NGN. The standards and research activities of NGN management are also presented.

a) NGN Overview

NGN is a packet-based network to support the transfer of mixed traffic types such as voice, video, and data [1]. It will integrate services offered by traditional networks and new innovative IP services into a single service platform. The key operation of the NGN is the separation of services and transport networks, which provides QoS-enabled transport technologies and service-related functions independent from underlying transport technologies [7]. The transport functions provide transfer of information between peer entities; the services functions are concerned with the applications and services to be operated between peer entities [8].

Fig. 1 shows typical NGN components: service network, core network, access network, and user equipment [8]. The service network is composed of various servers such as Web Server, Authentication, Authorization and Accounting (AAA), SIP Proxy Server and LDAP Server, etc. The service network is only responsible for providing services and applications for NGN users. The connection between the service network and the core network can be implemented via gateways.

Author α: Research Scholar, Jawaharlal Nehru Technological University, Hyderabad. e-mail: 1anand.80.kumar@gmail.com
Author σ: Professor, Department of ECE, Brahmas Institute of Engineering & Technology, Nellore.
e-mail: 2kesmurthy@rediffmail.com

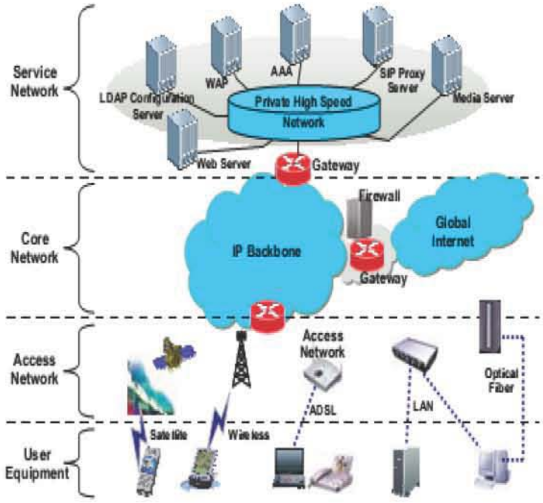


Figure 1 : NGN Network components

b) *Integrated Network Platform*

The core network in NGN represents the transportation backbone in traditional networks, which is concerned with the transfer of information between peer entities. Besides the transfer of packets, control and management functions are also implemented in the core network. The access network in NGN is derived from the existing access technologies. To accommodate various access media, the access network is separated from the core network of NGN, which serves as an intermediate between user equipment's and core network.

Integrated Network Platform refers to the integration of all IP capable wireless and wire line systems for the seamless delivery of Internet data services.

The goal is to allow mobile users to move transparently from wired to wireless networks or vice-versa without breaking their connection to the Internet. An office worker, connected to an Ethernet LAN, could transparently switch to a high-speed WLAN connection in order to maintain connectivity and provision of services. While moving around within the building, the node could switch transparently from one wireless subnet to another, and when leaving the building, could again switch transparently to a wide-area wireless data service such as GPRS or UMTS.

The increasing availability of wireless and wire line technologies with different properties will make the creation of an integrated network platform possible. Such integration should address following requirements:

- Enabling global mobility for users across different bearer types (integration of wireless & wire line technologies).
- Integration of Ad-hoc networks ñ Coverage extension in environments without networking infrastructure.
- Intelligent multiple interface handling ñ Filtering data streams to utilize the best interface which are based on different bearer technologies.

c) *Ad-Hoc Networks*

An ad-hoc network consists of a collection of mobile nodes without the required intervention of a centralized access point or existing infrastructure. The links of the network are dynamic and are based on the proximity of one node to another node. These links are likely to break and change as the nodes move across the network. Because of the temporary nature of the network links, and because of the additional constraints on mobile nodes (limited bandwidth and power), conventional routing protocols are not appropriate for ad-hoc mobile networks.

Protocols in Ad-hoc Networks

Unlike the cellular networks where base stations are essential, ad-hoc networks is backed up by communications directly between mobiles, thus the routing protocols are central and deserve our focus on their mechanisms. And in ad-hoc networks, there exists several routing protocols as listed below, which will be demonstrated in this report:

1. DSDV: Destination Sequenced Distance Vector
2. AODV: Ad-hoc On Demand Distance Vector

II. Backgrounds

AD HOC networks are networks of autonomous nodes that have wireless connections between each other. These connections can created and destroyed, changing the network topology as nodes change location, move out of range of other nodes or fail completely. Ad hoc networks pose an additional set of problems to those encountered in traditional fixed networks or wireless cellular networks. Dynamically forming the communications infrastructure from mobile devices is the source of these complications. One way of thinking about this is to imagine the problems caused by continually moving and changing the router you use to get from your local subnet to the rest of the world. How would packets get to or from you? This type of question has to be addressed along with requirements that affect traditional routing protocols such as loop free routing, completeness and stability.

As we have already seen, classical encryption techniques use scrambling of bits in order to encipher the message. In this section, we discuss three important classical cryptographic techniques namely,

1. Playfair Cipher
2. Vigenere Cipher
3. Caesar Cipher

The Playfair cipher uses a 5 by 5 table containing a key word or phrase. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping any duplicate letters), then fill the remaining spaces with the rest of the letters of the alphabet in order (put both "I" and "J" in the same space). The key can be written in the top rows of the table, from left to right, or in some other pattern, such as a spiral beginning in the upper-left-hand corner and ending in the center.

The Vigenere Cipher is the process of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. To encrypt, a Vigenere square is used. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

III. Proposed Method

NGN Functional Architecture

Fig. 2 shows an overview of the NGN functional architecture [2]. The NGN architecture needs to offer the configuration flexibility to support multiple access technologies. It also needs to support a distributed and open control mechanism, which provides a separated service provisioning from transport network operation and speeds up the provision of diversified NGN services.

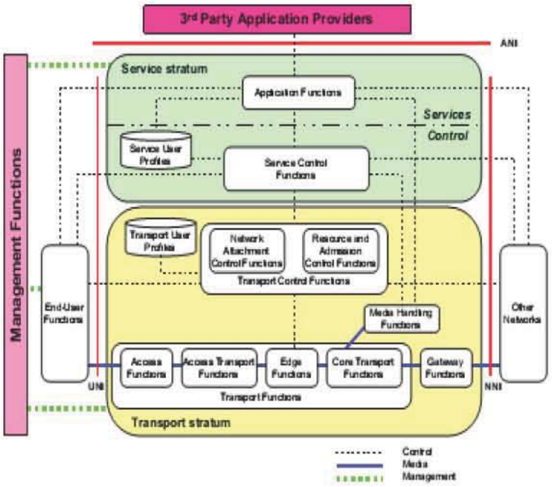


Figure 2 : NGN functional architecture

The NGN functions are divided into service and transport strata. The transport stratum functions provide connectivity for all components and physically separated functions within the NGN. The service stratum functions provide session-based and non-session-based services, including subscribe/notify for presence information and a messaging method for instant message exchange [7]. End-user functions are connected to the NGN by user-to-network interface (UNI), while other networks are interconnected through the network-to-network interface (NNI). The application-to-network interface (ANI) provides a channel for interactions and exchanges between applications and NGN elements.

a) Network Discovery And Selection

Since NGN consists of interconnected heterogeneous networks using heterogeneous user terminals, NGN should provide a seamless capability, independent of access method and network, and NGN also should address the identifying mechanisms [1]. That is, each terminal can use more than one type of network and possibly access multiple networks simultaneously for different applications (e.g., one for voice and another for receiving streaming media).

In such an environment, a terminal must be able to discover what networks are available for use. One of the proposed solutions for network discovery is to use software-defined radio devices that can scan the available networks. After scanning, they will load the required software and reconfigure themselves for the selected network. The software can be downloaded from the media such as a server, smart card, memory card or over the air.

b) Generalized Mobility

At present, mobility is used in a limited sense such as movement of user and terminal and with or without service continuity to similar public accessed networks (such as WLAN, GSM, UMTS, etc.) [6]. this means the horizontal handoff, which involves a terminal device to change cells within the same type of network to maintain service continuity. In the future, mobility will be offered in a broader sense where users may have the ability to use more access technologies, allowing movements between public wired access points and public wireless access points of various technologies. That is, in NGN environment, in addition to the horizontal handoff, the vertical handoff must also be supported. The vertical handoff mechanism allows a terminal device to change networks between different types of networks (e.g., between 3G and 4G networks) in a way that is completely transparent to end user applications. Thus, the challenge is to allow vertical handoffs between pairs of different types of networks in the presence of 2G, 3G, WLAN, WMAN, satellite, and 4G networks. The greater challenge lies when the vertical handoffs must take place with a certain set of QoS requirements still satisfied. Roaming allows a customer to automatically make and receive voice calls, send and receive data, or access other services when traveling outside the geographical coverage area of the home network. Roaming is technically supported by mobility management, authentication and billing procedures. Establishing roaming between service providers is based on roaming agreements. If the visited network is in the same country as the home network, then it is known as national roaming. If the visited network is outside the home country, then it is known as global roaming. If the visited network operates on a different technical standard than the home network, then it is known as inter-standard roaming.

In NGN, all three types of roaming should be supported to roam through different network types, operating in different cities and countries. For true global roaming, roaming agreements must be set up among service providers among countries. Today, only a few service providers in different countries provide global roaming. The challenge is to provide more roaming agreements among the service providers in different countries. The greater challenge would be to provide inter-standard roaming in different countries.

c) Qos Support

Over the past decade, much research has been conducted in the area of QoS, and many protocols and methods have been proposed. However, the predominant method to support QoS by the Internet service providers (ISPs) today is over-provisioning. That is, instead of implementing complex QoS algorithms and methods, ISPs typically provide enough bandwidth in their backbone trunks so that their networks are hardly overloaded and thus there exists very little delay and few packets are lost in transit. This is quite feasible since a lot of fiber trunks have been installed over the past decade and the bandwidth cost of wired Internet trunks is very cheap. In the ISP's views, it is much simpler and cheaper to provide over-provisioned networks than implementing and managing complex QoS mechanisms. Although NGN is supposed to provide higher bandwidth and more cost-effective channels than its predecessor networks, the bandwidth cost in NGN wireless networks will remain higher than wired networks. Thus, over-provisioning in NGN will not be feasible and QoS support mechanisms will definitely be needed. Providing QoS support in NGN will be a major challenge thus much work is needed.

Congestion is an important issue which researchers focus on in the Transmission Control Protocol(TCP) network environment. To keep the stability of the whole network, congestion control algorithms have been extensively studied. Queue management method employed by the routers is one of the important issues in the congestion control study. Active queue management (AQM) has been proposed as a router-based mechanism for early detection of congestion inside the network. In this paper we analyzed several active queue management algorithms with respect to their abilities of maintaining high resource utilization, identifying and restricting disproportionate bandwidth usage, and their deployment complexity.

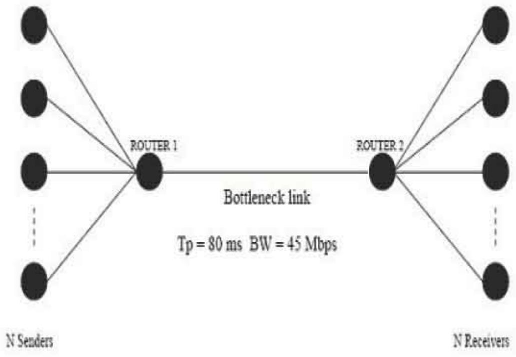


Figure 3 : Simulation topology

We compare the performance of RED, Drop tail based on simulation results, using RED and Drop Tail as the evaluation baseline. The characteristics of different algorithms are also discussed and compared. Simulation is done by using Network Simulator (NS2) and the graphs are drawn using X- graph.

Throughput: This is the main performance measure characteristic, and most widely used. In communication networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

This measure how soon the receiver is able to get a certain amount of data send by the sender. It is determined as the ratio of the total data received to the end to end delay. Throughput is an important factor which directly impacts the network performance.

Delay: Delay is the time elapsed while a packet travels from one point e.g., source premise or network ingress to destination premise or network degrees. The larger the value of delay, the more difficult it is for transport layer protocols to maintain high bandwidths. We will calculate end to end delay.

d) Routing Protocols

Efficient routing protocols can provide significant benefits to mobile ad hoc networks in terms of both performance and reliability. Mobile Ad-hoc Network (MANET) is an infrastructure less and decentralized network which need a robust dynamic routing protocol. Many routing protocols for such networks have been proposed so far. Amongst the most popular ones are Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector (AODV), and Destination-Sequenced Distance Vector (DSDV) routing protocol. To compare the performance of AODV and DSDV routing protocol, the simulation results were analyzed by graphical manner and trace file based on Quality of Service (QoS) metrics.

We will simulate an ad-hoc network using different routing protocols with the help of NS and then make a comparison based on the result.

Fig 4 shows basic topology of 3 node network in which initial location of nodes 0, 1 and 2 are respectively (5, 5), (490,285) and (150,240) (the z coordinate is assumed throughout to be 0).

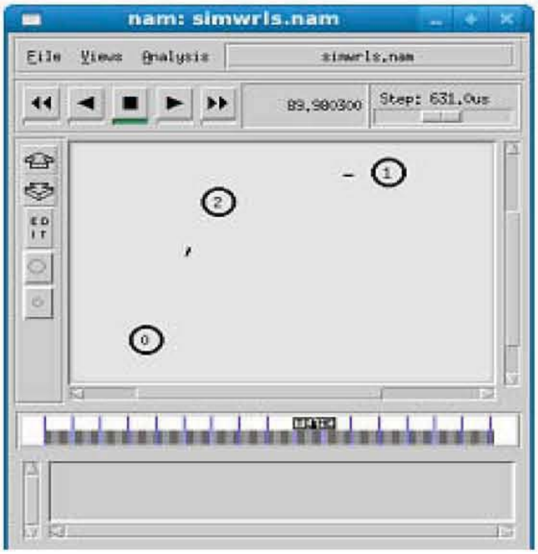


Figure 4 : Basic topology of 3-nodes network

At time 10, node 0 starts moving towards point (250,250) at a speed of 3m/sec. At time 15, node 1 starts moving towards point (45, 258) at a speed of 5m/sec. At time 110, node 0 starts moving towards point (480,300) at a speed of 5m/sec.

The simulation lasts 150 sec. At time 10, TCP connection using the DSDV ad-hoc routing protocol and the IEEE802.11 MAC protocol is initiated between node 0 and node 1.

e) Security

Over the past few years, the Internet and enterprise networks have been plagued by denial of service attacks (DoS), worms and viruses, which have caused millions of computer systems to be shutdown or infected and the stored data to be lost, ultimately causing billions of dollars in loss. The introduction of wireless LANs (e.g., IEEE 802.11) into enterprises has made network security more vulnerable since rogue base stations (i.e., unauthorized private base stations) can be easily connected to existing wired networks, potentially becoming the source of security attacks inside firewalls and intrusion detection systems. Moreover, connecting malicious PC via a base station that is not well managed is also critical.

In cryptography, a Caesar cipher, also known as the shift cipher, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on.

To pass an encrypted message from one person to another, it is first necessary that both parties have the 'key' for the cipher, so that the sender may encrypt it and the receiver may decrypt it. For the Caesar cipher, the key is the number of characters to shift the cipher alphabet. Here is a quick example of the encryption and decryption steps involved with the Caesar cipher. The text we will encrypt is 'defend the east wall of the castle', with a shift (key) of 1.

Plaintext: defend the east wall of the castle
Cipher text: efgfoe uif fbtu xbmm pg uif dbtumf

It is easy to see how each character in the plaintext is shifted up the alphabet. Decryption is just as easy, by using an offset of -1.

Plain: abcdefghijklmnopqrstuvwxyz
Cipher: bcdefghijklmnopqrstuvwxyza

Obviously, if a different key is used, the cipher alphabet will be shifted a different amount.

Mathematical Description

First we translate all of our characters to numbers, 'a'=0, 'b'=1, 'c'=2... 'z'=25. We can now represent the Caesar cipher encryption function, e(x), where x is the character we are encrypting, as:

$$e(x) = (x + k) \pmod{26}$$

Where k is the key (the shift) applied to each letter. After applying this function the result is a number which must then be translated back into a letter. The decryption function is:

$$e(x) = (x - k) \pmod{26}$$

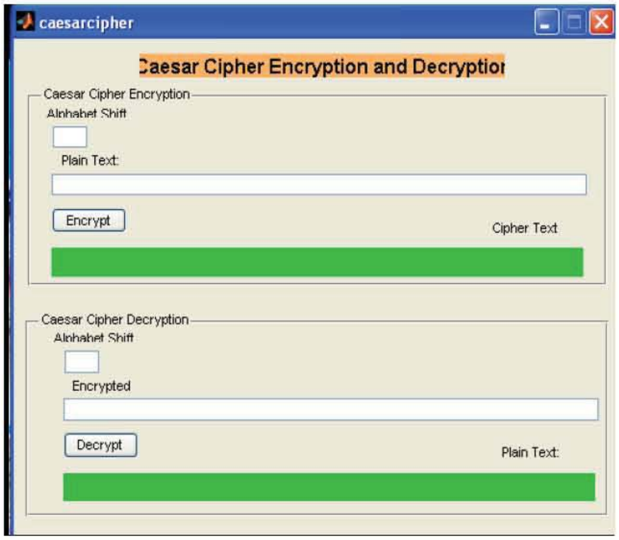
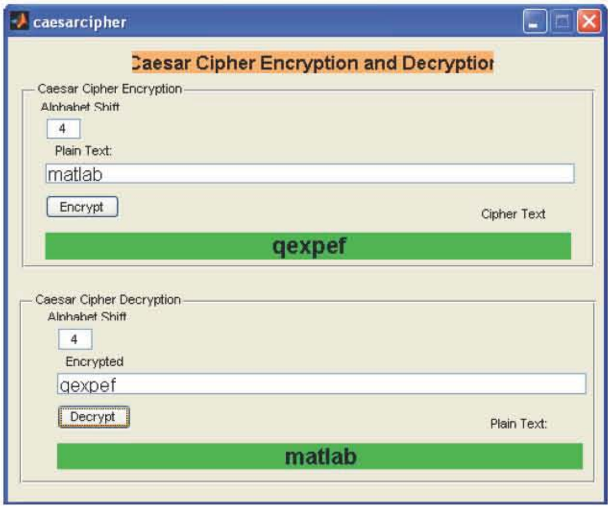


Figure 5 : Encryption process



caesarcipher

Caesar Cipher Encryption and Decryptior

Caesar Cipher Encryption

Alphabet Shift: 4

Plain Text: matlab

Encrypt

Cipher Text: qexpef

Caesar Cipher Decryption

Alphabet Shift: 4

Encrypted: qexpef

Decrypt

Plain Text: matlab

Figure 6 : Decryption process

IV. Results

a) Simulation Model

The objective of this paper is the performance evaluation of two routing protocol for mobile ad hoc networks by using an open-source network simulation tool called NS-2. Two routing protocols: DSDV and AODV have been considered for performance evaluation in this work. The simulation environment has been conducted with the LINUX operating system, because NS-2 works with Linux platform only.

Whole simulation study is divided into two part one is create the node (that may be cell phone, internet or any other devices) i.e. NS-2 output. It's called NAM (Network Animator) file, which shows the nodes movement and communication occurs between various nodes in various conditions or to allow the users to visually appreciate the movement as well as the interactions of the mobile nodes. And another one is graphical analysis of trace file (.tr).Trace files contains the traces of event that can be further processed to understand the performance of the network.

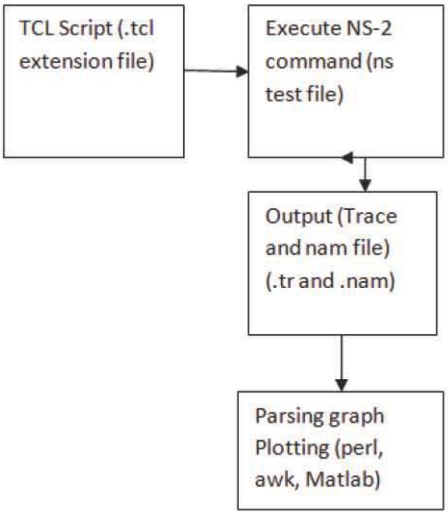

TCL Script (.tcl extension file)
Execute NS-2 command (ns test file)
Output (Trace and nam file) (.tr and .nam)
Parsing graph Plotting (perl, awk, Matlab)

Figure 7 : Simulation overview

Figure 7 depicts the overall process of how a network simulation is conducted under NS-2. Output files such as trace files have to be parsed to extract useful information. The parsing can be done using the awk command (in UNIX and LINUX, it is necessary to use gawk for the windows environment) or Perl script. The results have been analyzed using Excel or Matlab.
A software program which can shorten the process of parsing trace files (Xgraph and Trace Graph) has also been used in this paper. However, it doesn't work well when the trace file is too large.

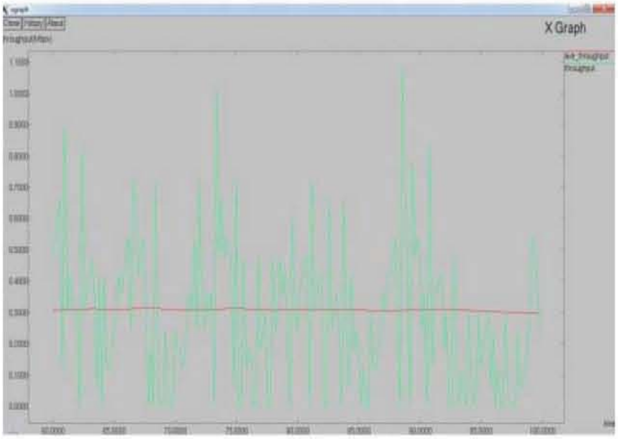


Figure 8 : Drop tail

Figure 8 shows how throughput varies w.r.t simulation time had been depicted shows unfair.

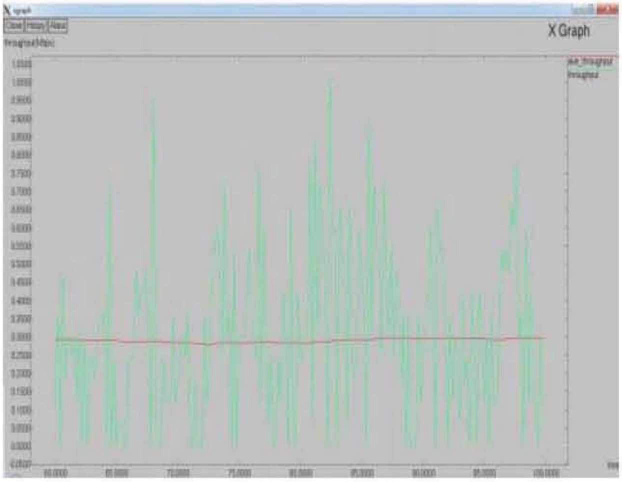


Figure 9 : RED

To generate trace file and nam file, we call tcl script in CYGWIN command shell. By varying the simulation parameter shown in table 1, we can see the graphical variation between various performance metrics like throughput, drop, delay, jitter etc.

Figure 9 shows how throughput varies w.r.t simulation time been depicted.

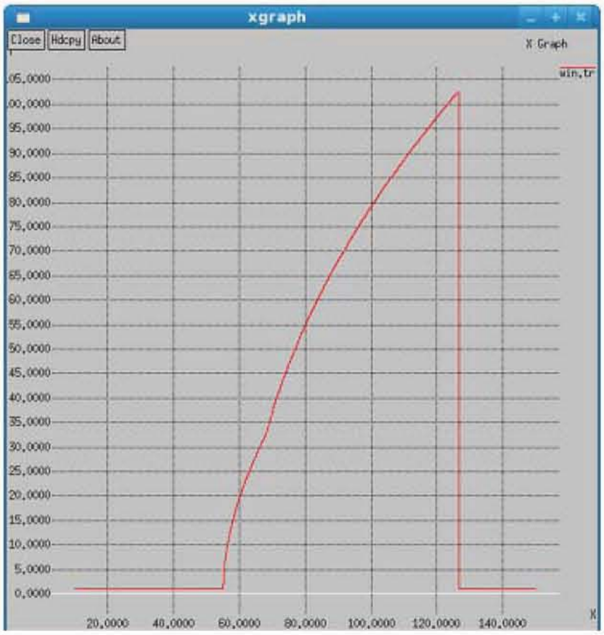


Figure 10 : window evolution before DSDV changes

At the beginning the nodes are too far away and a connection cannot be set. The first TCP signaling packet is transmitted at time 10 sec but the connection cannot be opened.

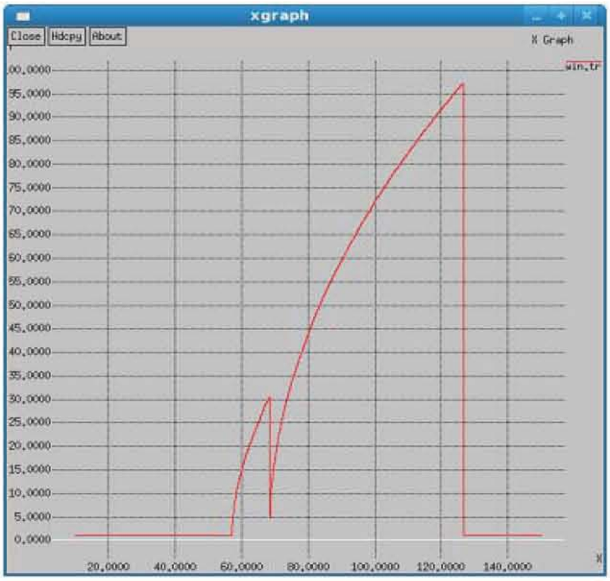


Figure 11 : window evolution after DSDV changes

Meanwhile nodes 0 and nodes 1 start moving towards node2. After 6 second (timeout) a second reatempt occurs but still the connection cannot be established and the timeout vaalue is doubled to 12sec.

At time 28 another transmission attempt occurs.While the connection still could not be established.Then at around 55 sec, both nodes 0 as well as node 1 to be within the radio of node 2 so that when tcp connection is reattempted at that time a two hop path is established between node 0 a direct connection is established.

At the moment of the path change there is a single TCP packet loss that cause the window to decrease slightly.At time 125.5 nodes 0 and 1 are too far apart for the connection to be maintained and the conncetion breaks.

From fig 12 it is seen that at 40sec connection is established and window size increases smoothly without any path change also no packet loss up to 144sec then window size decreases due to connection break.

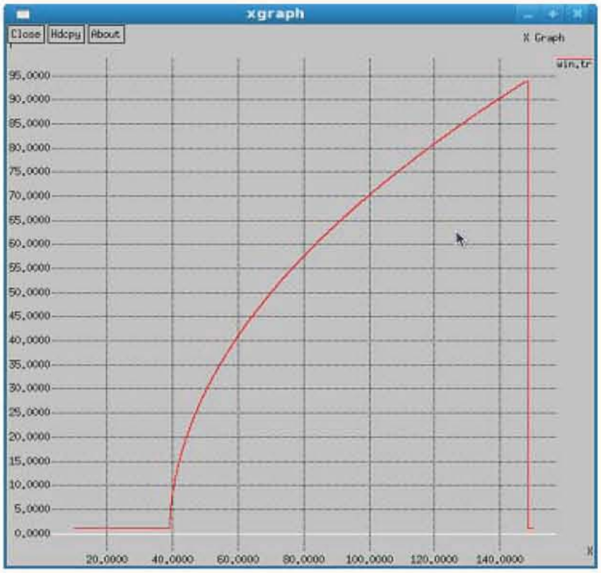


Figure 12 : window evolution over AODV changes

V. Conclusions

Simulation results show that DSDV compared with AODV, DSDV routing protocol consumes more bandwidth, because of the frequent broadcasting of routing updates. While the AODV is better than DSDV as it doesn't maintain any routing tables at nodes which results in less overhead and more bandwidth. AODV perform better under high mobility simulations than DSDV. High mobility results in frequent link failures and the overhead involved in updating all the nodes with the new routing information as in DSDV is much more than that involved AODV, where the routes are created as and when required. AODV use on -demand route discovery, but with different routing mechanics. AODV uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes.

References Références Referencias

1. ITU-T, "General overview of NGN", Recommendation Y.2001, Dec. 2004.
2. ITU-T, "General principles and general reference model for Next Generation Networks", Recommendation Y.2011, Oct. 2004.
3. ITU-T, "Functional requirements and architecture of the NGN", Recommendation Y.2012, Sep. 2006.

4. ITU-T, "Resource and admission control functions in Next Generation Networks", Recommendation Y.2111, Sep. 2006.
5. ITU-T, "Principles for the Management of the Next Generation Networks", Recommendation Y.2401, Mar. 2006.
6. ITU-T, "Mobility management requirements for NGN", Recommendation Y.2801, Nov. 2006.
7. Keith Knight, Thomas Towle, Naotaka Morita, "NGN architecture: generic principle, functional architecture, and its realization", IEEE Communications Magazine, vol. 43, no. 10, Oct. 2005, pp.49-56.
8. Mo Li and Kumbesan Sandrasegaran, "Network Management Challenges for Next Generation Networks", IEEE Conference on Local Computer Networks, Nov. 2005, pp. 593 - 598.

Global Journals Inc. (US) Guidelines Handbook 2013

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

- 'FARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'FARSC" can be added to name in the following manner. eg. **Dr. John E. Hall, Ph.D., FARSC or William Walldroff Ph. D., M.S., FARSC**
- Being FARSC is a respectful honor. It authenticates your research activities. After becoming FARSC, you can use 'FARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 60% Discount will be provided to FARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- FARSC will be given a renowned, secure, free professional email address with 100 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- FARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 15% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- Eg. If we had taken 420 USD from author, we can send 63 USD to your account.
- FARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- After you are FARSC. You can send us scanned copy of all of your documents. We will verify, grade and certify them within a month. It will be based on your academic records, quality of research papers published by you, and 50 more criteria. This is beneficial for your job interviews as recruiting organization need not just rely on you for authenticity and your unknown qualities, you would have authentic ranks of all of your documents. Our scale is unique worldwide.
- FARSC member can proceed to get benefits of free research podcasting in Global Research Radio with their research documents, slides and online movies.
- After your publication anywhere in the world, you can upload you research paper with your recorded voice or you can use our professional RJs to record your paper their voice. We can also stream your conference videos and display your slides online.
- FARSC will be eligible for free application of Standardization of their Researches by Open Scientific Standards. Standardization is next step and level after publishing in a journal. A team of research and professional will work with you to take your research to its next level, which is worldwide open standardization.

- FARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), FARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 80% of its earning by Global Journals Inc. (US) will be transferred to FARSC member's bank account after certain threshold balance. There is no time limit for collection. FARSC member can decide its price and we can help in decision.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

- 'MARSC' title will be awarded to the person after approval of Editor-in-Chief and Editorial Board. The title 'MARSC" can be added to name in the following manner. eg. Dr. John E. Hall, Ph.D., MARSC or William Walldroff Ph. D., M.S., MARSC
- Being MARSC is a respectful honor. It authenticates your research activities. After becoming MARSC, you can use 'MARSC' title as you use your degree in suffix of your name. This will definitely will enhance and add up your name. You can use it on your Career Counseling Materials/CV/Resume/Visiting Card/Name Plate etc.
- 40% Discount will be provided to MARSC members for publishing research papers in Global Journals Inc., if our Editorial Board and Peer Reviewers accept the paper. For the life time, if you are author/co-author of any paper bill sent to you will automatically be discounted one by 60%
- MARSC will be given a renowned, secure, free professional email address with 30 GB of space eg.johnhall@globaljournals.org. You will be facilitated with Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.
- MARSC member is eligible to become paid peer reviewer at Global Journals Inc. to earn up to 10% of realized author charges taken from author of respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account or to your PayPal account.
- MARSC member can apply for free approval, grading and certification of some of their Educational and Institutional Degrees from Global Journals Inc. (US) and Open Association of Research, Society U.S.A.
- MARSC is eligible to earn from their researches: While publishing his paper with Global Journals Inc. (US), MARSC can decide whether he/she would like to publish his/her research in closed manner. When readers will buy that individual research paper for reading, 40% of its earning by Global Journals Inc. (US) will be transferred to MARSC member's bank account after certain threshold balance. There is no time limit for collection. MARSC member can decide its price and we can help in decision.

Auxiliary Memberships

ANNUAL MEMBER

- Annual Member will be authorized to receive e-Journal GJCST for one year (subscription for one year).
- The member will be allotted free 1 GB Web-space along with subDomain to contribute and participate in our activities.
- A professional email address will be allotted free 500 MB email space.

PAPER PUBLICATION

- The members can publish paper once. The paper will be sent to two-peer reviewer. The paper will be published after the acceptance of peer reviewers and Editorial Board.

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, “Abstract” word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript’s Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Administration Rules Listed Before Submitting Your Research Paper to Global Journals Inc. (US)

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.
- Do not give permission to anyone else to "PROOFREAD" your manuscript.
- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation)
by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

A

Abilene · 22
Alleviated · 20
Anomalous · 32, 33, 58

B

Byzantine · 5, 8, 10, 16

C

Chimera · 58
Curtmola · 8, 16, 17, 33, 39, 59

D

Dirichlet · 25
Discritization · 44

E

Extrude · 43, 44

I

Iglesias · 30
Inevitably · 20, 24
Irretrievability · 15

K

Kinematics · 45

M

Masquerade · 31

O

Orifices · 49, 51, 53

P

Pneumatic · 48, 49, 50, 52, 53
Primitives · 3, 36
Provenance · 34, 59

R

Relinquishing · 36

S

Semielliptic · 42

T

Tampering · 5

U

Unanimous · 5

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350