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

Global Journal of Computer Science and Technology : E

Network, Web & Security

DISCOVERING THOUGHTS AND INVENTING FUTURE

HIGHLIGHTS

- Architecture and Applications
- Transmission Control Protocol
- Web Services Specifications
- Multipath Routing Approach

Computer Server Farm

Volume 12 | Issue 17 | Version 1.0 ENG

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 12 Issue 17 (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:Global Association of Research

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

Dr. Pina C. Sanelli
Associate Professor of Public Health
Weill Cornell Medical College
Associate Attending Radiologist
NewYork-Presbyterian Hospital
MRI, MRA, CT, and CTA
Neuroradiology and Diagnostic Radiology
M.D., State University of New York at Buffalo,School of Medicine and Biomedical Sciences

Dr. Roberto Sanchez
Associate Professor
Department of Structural and Chemical Biology
Mount Sinai School of Medicine
Ph.D., The Rockefeller University

Dr. Wen-Yih Sun
Professor of Earth and Atmospheric SciencesPurdue University Director
National Center for Typhoon and Flooding Research, Taiwan
University Chair Professor
Department of Atmospheric Sciences, National Central University, Chung-Li, TaiwanUniversity Chair Professor
Institute of Environmental Engineering, National Chiao Tung University, Hsin-chu, Taiwan.Ph.D., MS The University of Chicago, Geophysical Sciences
BS National Taiwan University, Atmospheric Sciences
Associate Professor of Radiology

Dr. Michael R. Rudnick
M.D., FACP
Associate Professor of Medicine
Chief, Renal Electrolyte and Hypertension Division (PMC)
Penn Medicine, University of Pennsylvania
Presbyterian Medical Center, Philadelphia
Nephrology and Internal Medicine
Certified by the American Board of Internal Medicine

Dr. Bassey Benjamin Esu
B.Sc. Marketing; MBA Marketing; Ph.D Marketing
Lecturer, Department of Marketing, University of Calabar
Tourism Consultant, Cross River State Tourism Development Department
Co-ordinator , Sustainable Tourism Initiative, Calabar, Nigeria

Dr. Aziz M. Barbar, Ph.D.
IEEE Senior Member
Chairperson, Department of Computer Science
AUST - American University of Science & Technology
Alfred Naccash Avenue – Ashrafieh

Contents of the Volume

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Web Usage Mining Architecture and Applications

By Mandeep Josan & Dr. G.N. Singh
Shri Guru Gobind Singh College, Chandigarh

Abstract - The WEBMINER is a system that implements parts of this general architecture. The first part is domain dependent application. The second part is the domain independent application. This includes pattern discovery and analysis as part of the system's data mining engine. The overall architecture for the Web mining process is depicted below:

GJCST-E Classification : *H.2.8*

Strictly as per the compliance and regulations of:

Web Usage Mining Architecture and Applications

Mandeep Josan [α] & Dr. G.N. Singh [σ]

I. Introduction

The WEBMINER is a system that implements parts of this general architecture. The first part is domain dependent application. The second part is the domain independent application. This includes pattern discovery and analysis as part of the system's data mining engine. The overall architecture for the Web mining process is depicted below:

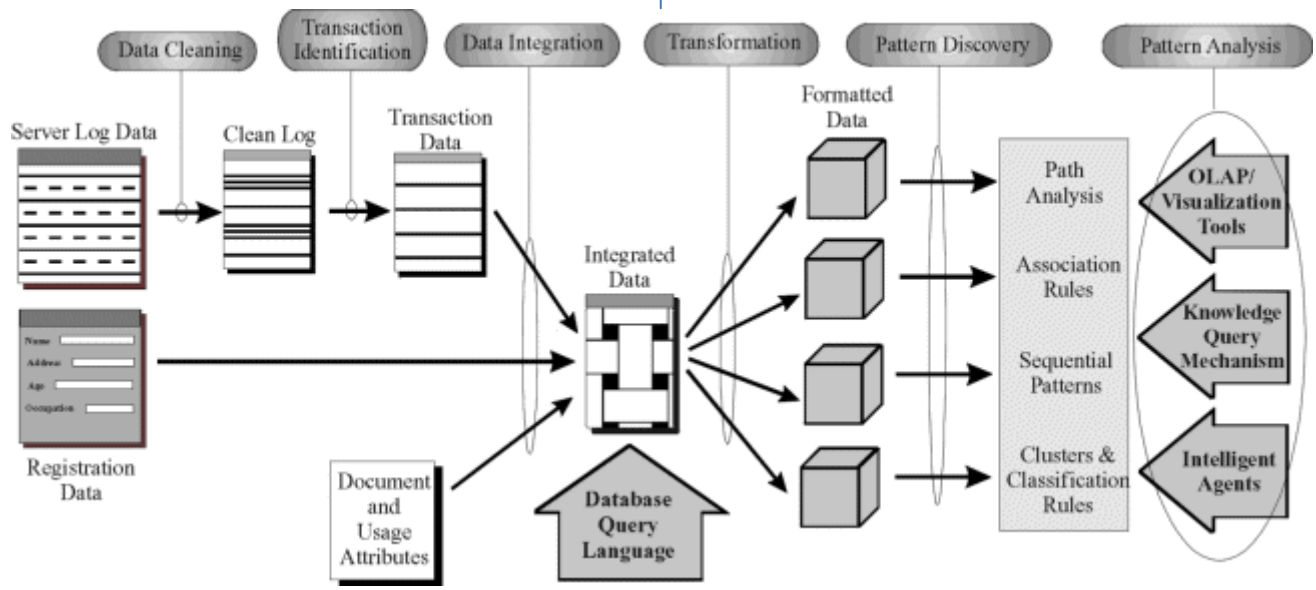


Figure : A General Architecture for Web Usage Mining

Just to briefly explain the above figure, data cleaning is the first step performed in the Web usage mining process. We have discussed some of the techniques to clean the log data. "Currently, the WEBMINER system uses the simplistic method of checking filename suffixes. Some low level data integration tasks may also be performed at this stage, such as combining multiple logs, incorporating referrer logs, etc".

After the data cleaning using one or a series of transaction identification modules into clusters. We have discussed a few techniques how to separate data into transactions. The "WEBMINER system currently has reference length, maximal forward reference, and time window divide modules, and a time window merge module".

"Access log data may not be the only source of data for the Web mining process. User registration data, for example, is playing an increasingly important role, particularly as more security and privacy conscious client-side applications restrict server access to a variety of information, such as the client user IDs". The data collected through user registration is then integrated with the access log data. There are also known or discovered attributes of references pages that could be integrated into a higher level database schema. The discovered attributes could include page types, usage frequency and link structures. "While WEBMINER currently does not incorporate user registration data, various data integration issues are being explored in the context of Web usage mining".

"In WEBMINER, a simple Query mechanism has been implemented by adding some primitives to an SQL-like language". This allows the user to specify his patterns of interest to the mining engine.

This information from the query is used to reduce the scope, and thus the cost of the mining process. The development of a more general query mechanism along with appropriate Web-based user

Author α : Shri Guru Gobind Singh College, Chandigarh.
E-mail : mandeep.jgill@gmail.com
Author σ : Department of Physics and Computer Science, Sudarshan Degree College, Lalgaon Distt. Rewa (M.P.) India.

interfaces and visualization techniques, are still in research.

a) BENEFITS

Let's have a look at some of the benefits you get from Web mining:

II. Match Your Available Resources to Visitor Interests

Resources can be products you "sell, information fragments you distribute online, banner ads from your client advertisers, e-mail fragments from a mailing list, or anything else" which is distributed online. "Metadata of these resources are then stored in a database. WebAnalyst helps learn visitor interests by collecting and analyzing information generated by interactions with your website, such as clickstream data, search requests, and cookies. WebAnalyst can use the gleaned knowledge to rank your resources by their relevance to the user's interests. Servicing a user request for information, with the best matching resources, results in a higher visitor-to-customer conversion rate for your e-business".

III. Increase the Value of Each Visitor

Upon carrying out collaborative filtering, we can predict what kind if information a visitor may be interested in, and the products she might consider purchasing. "These predictions used to present the visitor with related products and resources", and hence chances of them purchasing it. "This knowledge significantly increases the value of a customer for an e-business when used in individualized cross-selling and up-selling promotions, and thus increasing revenue."

IV. Improve the Visitor's Experience at the Website

"A sound combination of data and text mining techniques can help determine user interests - early in the process of the visitor's interaction with the website. This allows the website to act interactively and proactively and deliver the most relevant customized resources to the visitor". In the world of Internet, easy access to relevant information might make a difference between a profitable customer and lost opportunity. "By increasing the customer's satisfaction, you reduce attrition and build brand loyalty".

V. Perform Targeted Resource Management

Since, all visitors are different in buying behavior you may notice that some of them are your best potential customers, ready to click and buy, while others are prospecting for information, simultaneously familiarizing themselves with your brand. These prospecting customers may become "very important and profitable customers" in the future. Also not to forget there is another group of visitors who enjoy only free rides. "These folks will use promotional resources that you offer to the fullest extent, but will never purchase anything. All these visitors come through a single pipe to your website and are in a common queue for your website resources". It's best to your advantage if you can tell each type of visitor apart from the other. "Your website performance is limited and you might want to prioritize requests coming from your best prospects. If you are distributing promotional resources of high value, you might want to spend your promotional budget wisely by offering and delivering your promotional materials only to your best prospects - not to every Web surfer on the planet. WebAnalyst can work with load-balancing products to provide the best quality of service to your best customers".

VI. Collect Information in New Ways

"While for the majority of e-vendors the task of collecting data is just an intermediate step necessary for better targeting their marketing, for others this task might be the main motivation for creating a website itself". Traditional data collection methods like promotions, surveys, focus groups, etc. have many well known problems, including high cost, poor response rates and low accuracy. "Now imagine that you can offer your promotional items online through a content-rich website, where visitors can find useful information in addition to submitting their contact information and requesting the promotion. WebAnalyst can learn the visitor's preferences (at virtually no cost) based on the content that the user was browsing. Of course, WebAnalyst is designed to work hand-in-hand with your privacy management system, allowing you to collect valuable data while respecting the privacy of your visitors".

VII. Test the Relevance of Content and Web Site Architecture

Perhaps you would like to increase usability, or optimize your website for the eyes of your best prospects by taking close look at the website's content and architecture. "Log analyzers can help you visualize the most navigated paths through your website, averaged over all visitors. When optimizing your website structure, your main concern should be to improve experience of your most promising prospects, and not just everybody. Roughly 15% of your website visitors comprise really valuable prospects. The remaining 85% have little value to you other than sustaining the brand recognition traffic. Thus you have to segregate your least important prospects and subtract their contribution from the overall picture of the site navigation. What is left represents the real quality of your website. This is the

picture that can help you really improve your bottom line".

VIII. Web Mining Applications

Web mining extends analysis much further by combining other corporate information with Web traffic data. This allows accounting, customer profile, inventory, and demographic information to be correlated with Web browsing, which answers complex questions such as:

- Of the people who hit our Web site, how many purchased something?
- Which advertising campaigns resulted in the most purchases, not just hits?
- Do my Web visitors fit a certain profile? Can I use this for segmenting my market?

Practical applications of Web mining technology are abundant, and are by no means the limit to this technology. Web mining tools can be extended and programmed to answer almost any question.

Web mining can provide companies managerial insight into visitor profiles, which help top management take strategic actions accordingly. Also, the company can obtain some subjective measurements through Web Mining on the effectiveness of their marketing campaign or marketing research, which will help the business to improve and align their marketing strategies timely.

For example, the company may have a list of goals as following:

- Increase average page views per session;
- Increase average profit per checkout;
- Decrease products returned;
- Increase number of referred customers;
- Increase brand awareness;
- Increase retention rate (such as number of visitors that have returned within 30 days);
- Reduce clicks-to-close(average page views to accomplish a purchase or obtain desired information);
- Increase conversion rate (checkouts per visit).

The company can identify the strength and weakness of its web marketing campaign through Web Mining, and then make strategic adjustments, obtain the feedback from Web Mining again to see the improvement. This procedure is an on-going continuous process.

References Références Referencias

1. Allan, J. and H. Raghavan. "Using part-of-speech patterns to reduce query ambi- guity." In *Proceedings of the 25th annual international ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 307–314, Tampere, Finland, 2002. ACM Press. http://doi.acm.org/10.1145/564376.564430.
2. Aslam, J. A. and M. Montague. "Models for metasearch." In *Proceedings of the 24th annual international ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 276–284, New Orleans, LA, 2001.
3. Beitzel, S. M., E. C. Jensen, A. Chowdhury, O. Frieder, and D. Grossman. "Temporal analysis of a very large topically categorized web query log." *Journal of the American Society for Information Science and Technology*, 2008
4. Beitzel, S. M., E. C. Jensen, A. Chowdhury, and D. Grossman. "Using titles and category names from editor-driven taxonomies for automatic evaluation." In *Proceedings of the 12th ACM International Conference on Information and Knowledge Management (CIKM)*, pages 17–23, New Orleans, LA, 2003. ACM Press. http://doi.acm.org/10.1145/ 956863. 956868.
5. Chakrabarti, K., S. Chaudhuri, and S.-w. Hwang. "Automatic categorization of query results." In *Proceedings of the 2004 ACM SIGMOD International Confer- ence on Management of Data*, pages 755–766, Paris, France, 2004. ACM Press. http://doi.acm.org/10.1145/1007568. 1007653.
6. Chien, S. and N. Immorlica. "Semantic similarity between search engine queries using temporal correlation." In *Proceedings of the 14th International Conference on the World Wide Web (WWW)*, pages 2–11, Chiba, Japan, 2005. ACM Press. http://doi.acm.org/10.1145/1060745. 1060752.
7. Saraiva, P. C., E. S. de Moura, N. Ziviani, W. Meira, R. Fonseca, and B. Riberio- Neto. "Rank-preserving two-level caching for scalable search engines." In *Pro- ceedings of the 24th annual international ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 51–58, New Orleans, LA, 2001. ACM Press. http://doi.acm.org/10.1145/383952. 383959.
8. Sebastiani, F. "Machine learning in automated text categorization." *ACM Computing Surveys*, 34(1):1–47, 2002 http://doi.acm.org. ezproxy.gl. iit.edu/ 10.1145/505282.505283.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Transmission Control Protocol over Wireless LAN

By Dr. Gagandeep Singh Barar & Dr. G.N. Singh

Panjab University, Chandigarh

Abstract - 802.11 standards based WLAN is one very successful technology in commerce. Huge number of WLAN has been deployed across the world. It's very worthwhile to investigate link characteristics of WLAN and its effects to upper layers, especially TCP protocol which is used by numerous network applications. The 802.11 standard is firstly introduced in this section.

GJCST-E Classification : C.2.1

Strictly as per the compliance and regulations of:

Transmission Control Protocol over Wireless LAN

Dr. Gagandeep Singh Barar [α] & Dr. G.N. Singh [σ]

I. Introduction

802.11 standards based WLAN is one very successful technology in commerce. Huge number of WLAN has been deployed across the world. It's very worthwhile to investigate link characteristics of WLAN and its effects to upper layers, especially TCP protocol which is used by numerous network applications. The 802.11 standard is firstly introduced in this section.

II. 802.11 Standard Overview

The 802.11 standard is approved by **LAN MAN Standards Committee of the IEEE Computer Society** for LAN over wireless medium. This standard is part of a family of standards for local and metropolitan area networks. Figure 1 depicts the whole standards family.

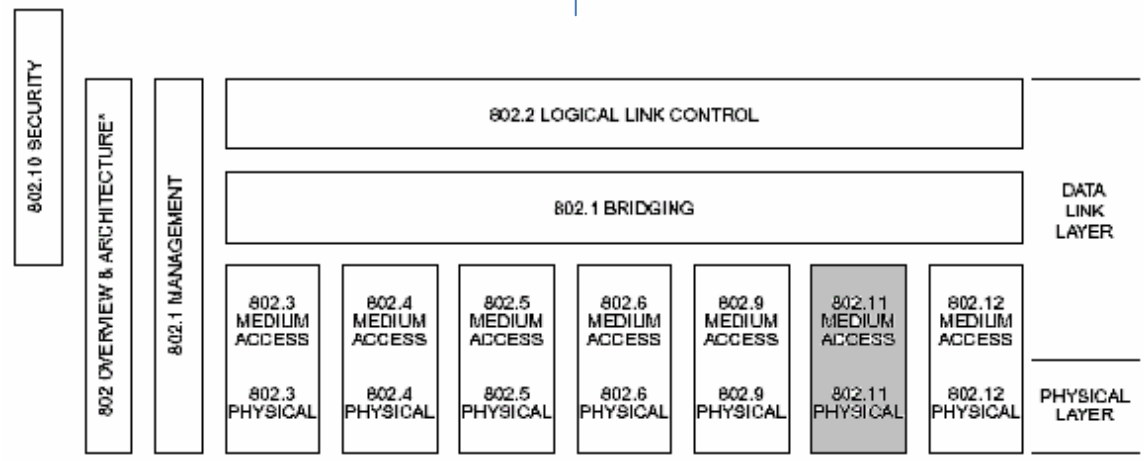


Figure 1 : Protocol Architecture of 802 Standard Family

The 802.11 standard includes a series of specifications which standardize MAC and Physical Layer of WLAN. This standard includes several different Physical Layers (802.11, 802.11b, 802.11a, 802.11g); but these Physical Layers use the same MAC layer. The following figure gives one overview of specifications of the 802.11 standard.

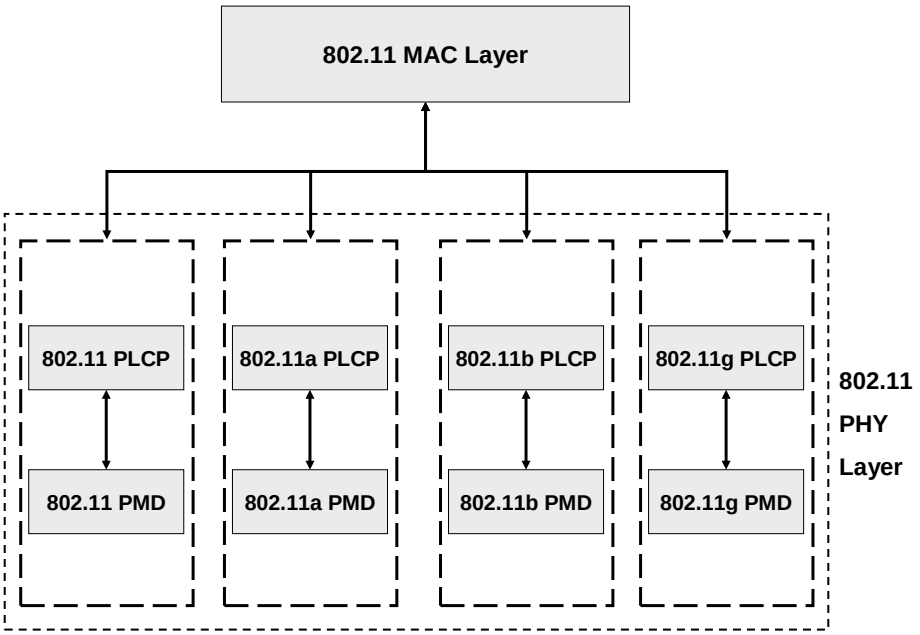


Figure 2 : The 802.11 Standard

Each physical layer includes two sub-layers, PLCP and PMD. PLCP is one convergence procedure to map MAC PDU into a frame format designed for radio transceiver of corresponding PMD layer. PMD layer interacts with PLCP layer and provides the actual means to transmit data on medium. The following table summarizes the technical details of different PMD sub-layers of 802.11.

Table 1 : PMD details of 802.11

	802.11	802.11b	802.11a	802.11g
Frequency	2.4G	2.4G	5G	2.4G
PHY	FHSS, DSSS,IR	DSSS	OFDM	OFDM
Data Rate (Mbps)	DSSS: 1, 2 FHSS: 0.5-4.5 IR: 1, 2	1, 2, 5.5, 11	**6**, 9, **12**, 18, **24**, 36, 48, 54	**…20**,…, 54
Channel	4	4	8	4

*IR physical layer is seldom used in practice. The deployment based on original 802.11 is being substituted by 802.11b, 802.11a, 802.11g. WLAN based on 802.11b dominates the currently WLAN deployment.

The factors of the 802.11 standard which affects link characteristics will be described in the following sub-sections, such as network architecture, medium access method, etc.

III. Network Architecture

BSS (Basic Service Set) is the basic building block of 802.11 LAN. It includes two or more mobile stations which can directly communicate with each other through wireless medium.

One DS (Distribute System) can be used to interconnect multiple BSSs. In this situation, Each BSS has one special station---AP (Access Point). In addition to act as one station, AP also provides access to DS for other stations in this BSS.

The DS and BSSs allow IEEE 802.11 to create a wireless network of arbitrary size and complexity. IEEE 802.11 refers to this type of network as the ESS (Extended Service Set) network. It is usually called as Infrastructure Network. The following figure illustrates the simplest ESS network.

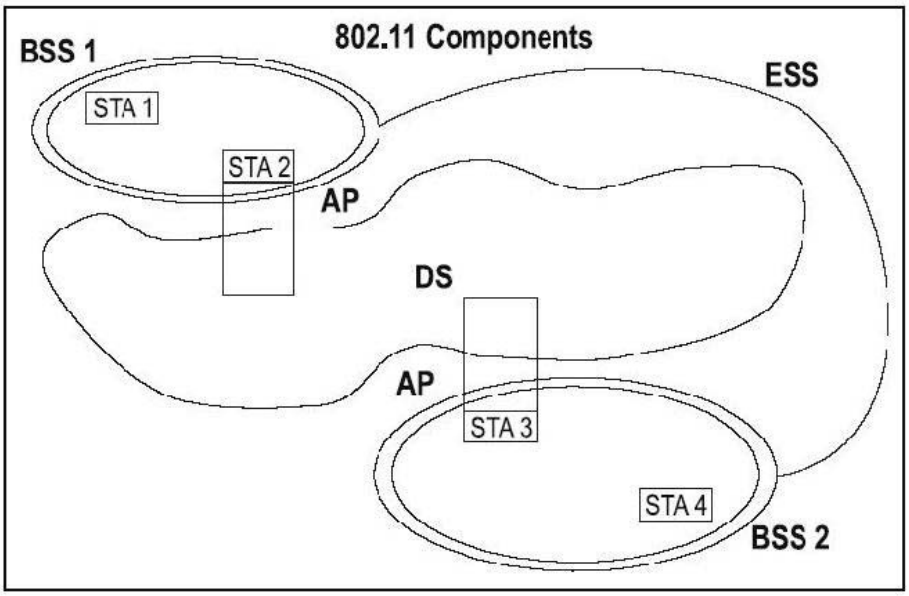


Figure 3 : 802.11 Infrastructure Network (ESS)

DS in ESS normally connects with Internet or other wired networks. In this way, mobile station can access Internet or other network by WLAN.

There is another network type in 802.11, Ad hoc Network. In ad hoc network, there is no DS. There is just one independent BSS and there is no station act as AP. Stations in ad hoc network communicate with each other directly or relaying by intermediate stations.

WLANs with different network architectures own very different link characteristics. The next section will describe how the two network types affect link characteristics in detail.

IV. DCF and PCF

The different physical layers of 802.11 use the same MAC layer. MAC layer of 802.11 uses one CSMA/CA protocol. It does not use Collision Detection of 802.2 because the transmitter cannot detect collision in wireless medium.

The basic medium access method of 802.11 MAC is a DCF (Distributed Coordination Function). Its simple operation mode uses two-way handshaking (DATA-ACK). The following figure gives one simple example.

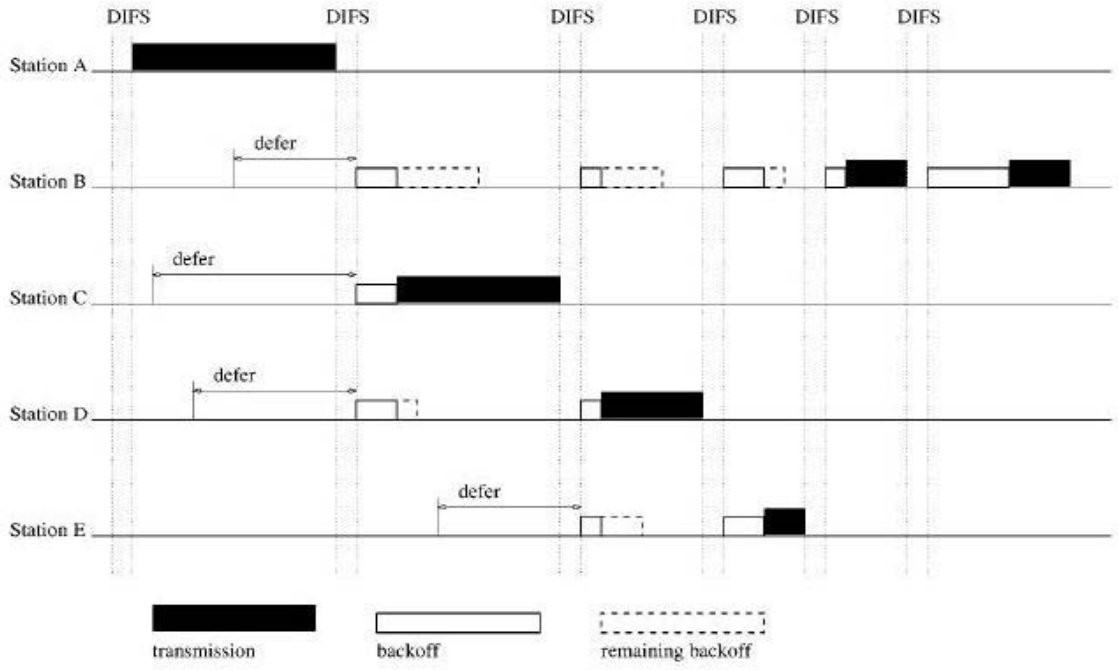


Figure 4 : Basic Access of MAC protocol

To send a packet, a station X first listens to the channel for time T_{DIFS}. If there is silence for T_{DIFS}, X proceeds with the transmission (e.g., station A in figure 4); otherwise, X waits for the first TDIFS of silence after the current busy period, then backs off for a random interval (e.g., station C in figure 4). For each packet, X initializes a contention window size W to be W_{min}. X sets a timer to a random integer uniformly distributed over 0, 1 … W, and decrements it after every T_{slot} period of silence, but suspends it if another station Y begins transmission – this suspension spans the acknowledgment as well (see below); when the timer reaches 0, X begins transmission of its packet (e.g., stations B, D and E in figure 4). Time is thus discretized by T_{slot} to support back-off timers, and a transmission typically occupies multiple slots. The packet is transmitted in its entirety, even if there is a collision, since X does not do collision detection.

The receiver uses the CRC bits in each packet to check for collisions and, if no error is detected, sends an ACK (acknowledgment) after time T_{SIFS} (SIFS is short inter-frame space; $T_{SIFS} < T_{DIFS}$). If the sender does not detect an ACK within an ACK-timeout, it enters a **retransmit back-off**: if W is smaller than the maximum window size W_{max}($W=2^{m}*W_{min}$, m is the number of retransmission attempts), then W is doubled; X sets a timer to a value uniformly chosen from less than the new W, and retransmitted when this timer expires just as before. If retransmission time exceeds d, the packet is thrown away and new packet will be transmitted. Finally, a station must separate two consecutive packets by a random back-off, even if the channel is idle for DIFS after the first transmission (e.g., station B in figure 4.)

In the basic mode of DCF, back off is designed to avoid contention. The contention window size affects MAC layer's throughput. If it's too small, too many collisions happen; otherwise, stations idle for too much time and bandwidth is wasted. The contention window size also affects RTT of wireless link seen by upper layer.

In DCF, RTS/CTS is adopted to solve hidden station problem and to alleviate effects of possible collisions. RTS and CTS is short control message. They are used to acquire the channel for a period time by one station; other stations update their NAV (Network allocation Vector) according to received RTS/CTS and do not transmit frames in these periods. Thus only RTS/CTS may collide with each other; the adverse effect is much less than collisions among long data packets.

AP can also use PCF based on DCF as the medium access method. The PCF provides contention-free frame transmission. The AP use Beacon frame which contains one DTIM element to begin one CFP (Contention-Free Period) and other stations update their NAV according information in beacon frame. In this period, AP polls other stations and other stations can not initiate data transmission. AP can send frame to other stations and if the station which is polled has packets to transmit, the station will transfer frame. The following figure is one example for frame transmission in PCF.

References Références Referencias

1. IEEE Standard, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE P802.11, 1999
2. IEEE Standard, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications---high-speed physical layer in the 5 GHz band, IEEE P802.11, 1999
3. IEEE Standard, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications---higher-speed physical layer extension in the 2.4GHz band, IEEE P802.11, 1999
4. N. Golmie, R.E. Van Dyck, A. Soltanian, A. Tonnerre and O. Rebala, "Interference Evaluation of Bluetooth and IEEE 802.11b Systems", Wireless Networks, V9, pp201-211, 2003
5. Arunesh Mishra, Minho Shin, William Arbaugh, "An Empirical analysis of the IEEE 802.11 MAC Layer Handoff Process", citeseer.nj.nec.com/541775.html
6. Y. Tian, K. Xu, N. Ansari, "TCP in Wireless Environment: Problems and Solution," *IEEE Communications*, vol 43. no.3, 2005.

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Security in Database Systems

By Abdulrahman Hamed Almutairi & Abdulrahman Helal Alruwaili

King Saud University

Abstract - The paper focuses on security issues that are associated with the database system that are often used by many firms in their operations. The rapid development and proliferation of Information technology has offered many opportunities for integrated business operations. It has enabled business enhances their efficiency and effectiveness in operations such as customer care, sales, human resources and production. However, these developments have served to bring issues of security. Many firms are falling victims of cyber crimes. These are malicious people who target their data and compromise its integrity. This is occasioned by unauthorized access, which makes data lose its integrity and lastly operations of the business are affected negatively. This paper will tackle various issues in database security such as the goals of the security measures, threats to database security and the process of database security maintenance.

Keywords : *database security, security techniques, database threats, integrity.*

GJCST-E Classification : *C.2.0*

Strictly as per the compliance and regulations of:

Security in Database Systems

Abdulrahman Hamed Almutairi [α] & Abdulrahman Helal Alruwaili [α]

Abstract - The paper focuses on security issues that are associated with the database system that are often used by many firms in their operations. The rapid development and proliferation of Information technology has offered many opportunities for integrated business operations. It has enabled business enhances their efficiency and effectiveness in operations such as customer care, sales, human resources and production. However, these developments have served to bring issues of security. Many firms are falling victims of cyber crimes. These are malicious people who target their data and compromise its integrity. This is occasioned by unauthorized access, which makes data lose its integrity and lastly operations of the business are affected negatively. This paper will tackle various issues in database security such as the goals of the security measures, threats to database security and the process of database security maintenance.

Keywords : database security, security techniques, database threats, integrity.

I. Introduction

Sorting Database security is a crucial operation that a firm should enhance in order to run its activities smoothly. It is a deliberate effort to protect an organization data against threats such as accidental or intentional loss destruction or misuse. The threats pose a challenge to the organization in terms of integrity of the data and access. The threat can result from intangible loss such as hardware theft or intangible loss such as loss of confidence in the organization activities. All these activities have been rampant due to electronic commerce as opposed to convectional trade involving physical goods. There has seen consumers been sensitive to any cases of security violations. It is also very hard to apprehend culprits who commit the violations because of the remoteness of transactions. Also, most database store sensitive information for consumers which can be vulnerable to hacking and misuse. Therefore, firms have embraced greater controls and checks on their database to maintain the integrity of the information and ensure that their system are monitored closely to avoid deliberate violations by intruders.

II. Threats of Database Security

Database security issues have been more complex due to widespread use and use of distributed client/server architecture as opposed to mainframes system. Databases are a firm main resource and therefore, policies and procedure must be put into place to safeguard its security and the integrity of the data it contains. Besides, access to the database has been become more rampant due to the internet and intranets therefore, increasing the risks of unauthorized access (Singh, 2009).

The objective of database security is to protect database from accidental or intentional los. These threats pose a risk on the integrity of the data and its reliability. Besides, database security allows or refuses users from performing actions on the database. Database managers in an organization identify threats and make policies that take action to mitigate any risks. Such actions include controls using passwords and username to control users who access the databases. The system created is called database management security system which keeps user details and allows access when provided with passwords and usernames (Singh, 2009).

There are different threats to the database systems. Loss of availability means that data or systems cannot be accessed by any user. This most often arise from sabotage of the hardware, applications or networks system. This may halt the activities of the organization as well impede on the operation in the day to day activities of the organization (Singh, 2009). For example, in case of a bank where customers can looses their confidence in the security of their deposits and eventually the bank lose customer and performance decline. Excessive privilege abuse is another method through which data can loss its integrity. When users are given too much privilege in the system database they abuse them for malicious purposes. For example, in the accounting department, the user may change other issue not concerned with the function of his job. All privileges should match the job requirements for each user (Singh, 2010).

Another threat to database security is that of privileges elevation. This is when some user can convert extra privileges from ordinary user to administrator through taking database platform software vulnerability. For example, in a firm accounting department, a user may convert excess rights to that of administrator and use them to create illegal transactions and accounts. This is done by exploiting the software weaknesses in the database system (Singh, 2009).

Another threat is having a weal audit trial. This is when an organization exposes itself to risk of various types due to weaknesses in its internal system. This is due to weak deterrence mechanism. Denial of service is another problem in database security. This is a kind of

Author α : King Saud University, College of computer and information sciences.

an attack where data or network applications are targeted to avoid access to users. Often, the intention is to extort money. For example, attackers can crash servers from remote areas and then extort money. Other techniques that can be used in denial of service include data corruption, network flooding and resource overload.

Another threat to the problem of database insecurity is weak system and procedures for performing authentication. Weak authentication can result to attackers getting legitimate rights of user and then steal or change credentials. Some of the ways in which an attacker can hack in include use of social engineering, where passwords are requested through phone calls for maintenance purposes. Other include brute force where the attacker does guess the passwords. Strong authentication is therefore required to address these challenges. Besides that, there is backup data exposure, where the storage media is left exposed leading to attacks. For example, tape and hard disks need to be secured well (Singh, 2009).

Loss of data integrity can cause the data to be corrupted and invalid. This can results to delay in operations of the company as well as making wrong decisions which can affect the performance of the company (Singh, 2009). This can only be restored through backup and recovery procedures. Another issue at player is the loss of confidentiality. This is where the secrecy of crucial data in an organization is breached resulting to loss of confidentiality and eventual loss of competitiveness (Singh, 2009). Another threat to database system is the loss of privacy. This can lead to the firm being subjected to blackmail, bribery and shame.

Theft or fraud is also common in firms such as banks. This occurs when personnel enter protected areas where databases are hosted and interfere with the systems. To prevent this threat, the firms should have controls on restricted areas as well install firewall to prevent people gaining unauthorized access to the database systems (Singh, 2009). Other threats that can be detected are accidental losses which could result from malfunctioning systems and operating procedures. Other forms of threats to databases could include inference theft. This is the process of sending queries deducing unauthorized information from legitimate sources. Identity theft is another form of threat to database. This is the situation where a person poses as another person and uses social security number to wipe out the details of the holders (Kumar, 2005).

There are several goals that are often targeted for database security issues. The first one is confidentiality. This relates to secrecy or privacy in terms of access by authorized subjects or processes.

The second goal is to ensure that integrity is maintained and that means that data can only be changed by authorized subjects. Another goal is the availability of data. This is the need to maintain access to only authorized persons.

III. Security Threat Classification

Several Human errors can be said to be accidental in that incorrect input and wrong use of applications can be seen as a factor that can lead to such threats. Errors in software include those of incorrect applications of security protocol and denial of access to authorized users. Natural or accidental disasters can also be cited as one of the factors of security concerns. This includes damage of software and hardware (Kumar, 2005).

IV. Classification of Database Security

Security of databases involves restoring the database to a safe mode after failure. There are various types of security issues that are related to database. Physically security can be said to be security of the hardware associated with the system and where the database is hosted or located. Some cause such as floods and earthquakes can be a threat to that and the only solution is to store databases back up. The other types of measure are the system issues or logical security. These are measures that resides in the operating systems and usually far more difficult to achieve (Sumathi, 2007).

V. Guidelines for Database Security

For some steps need to be taken in order to build a robust system. This is a system which has got Simplicity in design and very easy to use and that make it less vulnerable to attacks. Normalization of the database should be done at early stages before use to enhance its functioning and avoid hitches after updates. Allocation of privileges to different users is another guide in that each user should be allocated some privileges to avoid chances of hacking. It is also important for users to create view for each group of users. After the designing stage, the database needs to be maintained and several issues needs to be taken care of. There are some procedures that need to be taken care of in maintenance. The first one is operating systems issues and availability.

Operating system should be capable of ensuring verification of users and applications programs which attempts to access the system and authorizes them. This work is handled by the database administrator who also keeps accounts and passwords (Sumathi, 2007).Besides that there is confidentiality and accountability. By accountability, the system should not allow any user without its permission to avoid illegal access. Therefore, there is need to monitor authentication and authorization of users. Authorization is usually handled by controls which are found on the database management system that controls access by

users and actions done when accessing the database. Authentication is usually carried out operating system. The database administrator creates passwords for every user (Sumathi, 2007). The next step is through encryption. This is defined as coding of data so that it is not read and understood easily by the users. Database management system have system to encode data which is extremely sensitive for transmission over channels. It also provides a channel for decoding data which is also secured enough (Sumathi, 2007). Database system have also a mechanism to verify whether what the user claims to be is actually true. Such measure include passwords and usernames that enable the authentication of users. It is hosted at the operating system or at the database system management system. Passwords are legitimate user access methods.

VI. Process of Creating Database Architecture

We Security in database can be enhanced through a process of developing architecture system. There is a process of maintaining and establishing security architecture. The first phrase according to Basta and Zgola 2010 is carrying out assessment and analysis. This involves identifying the security threats, vulnerability and resources that exist in the devices and vendor partnership. A through and exhaustive audit of the database environment should be done. This is to identify any social engineering gaps as well firewall faults. Experts are normally called in to identify risks, define the likelihood of a threat of an asset and determine the cost of any such threat to the assets. Once this is done, the next step is to come up measure to counteract these threats.

The next phrase is to design and model the system. This is usually done through creating policies and prototype security that satisfies the business needs. AT this stage, policies and procedures are created and the software is defined. Once this is done, the next step is to identify tools and applications for reducing risks (Basta and Zgola 2010).

The third stage is usually deployment. This is the phase where the tools firewall and applications are put into place. The exercise involves making simulation in terms of deployment tests. These are simulation tests that helps to test the robustness and any case of unforeseen variable do affect overall security objectives (Basta and Zgola, 2010).

The fourth stage is the management and support. This is where the ongoing support and assessment of the security architecture was deployed as seen in the previous phase Monitoring is done to ensure that changes can be rectified as soon as possible. Need for reassessment and initiating the start of security life cycle (Basta and Zgola 2011).

VII. Illustration of Maintaining and Creating Database Security Architecture

Figure 1 : Database Security Architecture

VIII. Techniques for Database Security

Authorization can be one of the techniques that can be used for granting rights of access of a subject into a system. Another method that is effective is the view. This is a virtual table that can be produced at the time of request of data access. What happens is that view has to have access in the tables other than the base tables in such a way those restrictions are made on the user. This provides appropriate security to crucial data.

Back up is the process of taking to an offline storage facility, data and log file. To keep track of transaction involving the database, it is necessary for one to have journal file on all updates of the database. In event of failure of the database system, the log file and the database are then used to restore the database to normal functioning position. Integrity constraint is used to contribute to avoid cases of data becoming invalid and hence giving misleading information. The ultimate goal of the constraints is to maintain integrity of the data and hence its consistency. Database can be secured through encryption. This is encoding of the system using special algorithm that is only accessible when decryption key is provided. This is especial useful when sending sensitive information over communication lines (Bertino et al (2005).

Audit trial is another method that can help in the database security. Audit trial need to be carried to found the history of operations on the database. It is necessary to restore information lost as well as discover abuse of privileges by any users (Singh, 2009).

Another technique that can be used to secure database is the use of access control. This is the where the access to the system is only given after verifying the credentials of the user and only after such verification is done, the access is given. Use of steganography is rampant in the era of information technology. This technique is used to hide information from unauthorized access. What happens is the data is embedded in the LSB's of the pixel value. Certain number bits are used to hide sensitive information (Basta and Zgola, 2011).

IX. Various Techniques for Database Security

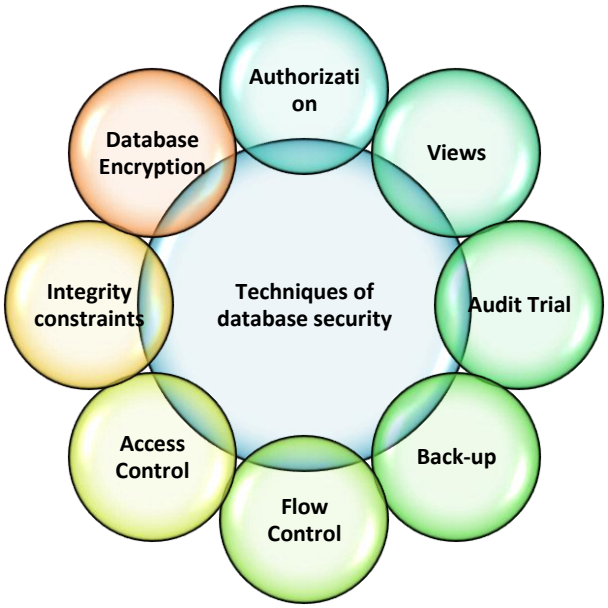


Figure 2 : Various techniques for database security

X. Advantages of Database Management System

What A database management system is used is a group of programs that manages the database structure and controls the access to the data stored in the database. It is thus an intermediary of between the users and the database. It has several advantages. It improves data sharing in a way that enables the end users have better access to data that is correctly managed. There is improved data security in that the security is guaranteed and the data privacy is maintained. Database management has an effect of ensuring that there is promotion of data integration in a whole organization and one can see a bigger picture of all activities (Coronel et al, 2012). There is also minimized data inconsistency such that the anomalies such as storing different data in different places is reduced. It is also probable that data access is facilitated and could be used to provide quick answers to queries giving out. There is better decision making is achieved due to accuracy, timelessness and validity of the information generated. The final result is increased end user productivity because it empowers one to make rational decisions for the success of the business (Coronel et al, 2012).

XI. Requirements for Database Security

User authentication and identification is normally required before the user can access the database. Authentification methods are passwords, biometric readers or signature analysis devices. These are required for better management of users. The second requirements involves authorization and access controls. These are the rules that govern what access to what information. These policies govern how information is disclosed and then modified. When you look at the access controls, these are the polices that govern the authorizations. There has to be integrity and consistency in the database operations. There has to be a correct set of rules in operation which protects the database from malicious destructions. Auditing is another requirement in database. This demands that a record of actions pertaining to operations. This is necessary in order to review and exams the efficiency of the controls system and recommend for better actions (Coronel et al, 2012).

XII. Integrity Principles in Database Security

Answers Data integrity refers to reliability and accuracy of the data that is stored and used in business. Data should assist a firm to make the right decision and avoid inconsistencies. Therefore, there are several guidelines that normally should be adhered to. The first one is well-formed transactions. This means that data should not be liable to manipulation easily and arbitrarily by users. This promotes its integrity. This reduces chances of compromising on the data accuracy. It is paramount the privileges are given at minimum basics to restrict any unauthorized access. There must be a separation of duties in that, individual should be exposed to misuse assets on their own. In database security, there must be ability to reconstruct events such that it is possible to hold individual accountable for their actions. Every organization has a structure and this structure has people who are charged with the responsibility to delegate authority. Another principle is that there must be continuity of operations. This means that, in face of calamity such as disaster, the operations of the firm must continue at some degree (Coronel etal, 2012).

Figure 3 : Database security

XIII. Conclusion

Which the paper has generally discussed the database security concerns and research into various issues surrounding the sector. Organizations now are relying on data to make decisions on various businesses operations that enhance their operations. Therefore, it is prudent to keep sensitive information away from unauthorized access. Database security research paper has attempted to explore the issues of threats that may be poised to database system. These include loss of confidentiality plus loss of integrity. Besides, it has detailed on loss of privacy leading to blackmail and embarrassment in the business. The paper has also discussed areas concerning techniques to counter any issue of threat. These could be use of views and authentication. Another method is through back-up method which ensures that the information is stored elsewhere and recovered in case of failure or attacks. The paper has also discussed the requirements that are set for a robust database management system. Some of the requirements are audit trial. Lastly, the paper has looked at the process for managing a database system and has discussed all the steps that need to be taken.

References Références Referencias

1. Kumar et al Managing Cyber threats: Issues, Approaches and Challenges Springer Publishers, 2005.
2. S. Singh, Database systems: Concepts, Design and applications New Delhi: Pearson Education India, 2009.
3. S. Sumanthi, Fundamentals of relational database management systems Berlin: Springer, 2007.
4. P, Singh Database management system concept V.K (India) Enterprises, 2009
5. A. Basta, and M. Zgola, Database security Cengage Learning, 2011.
6. Coronel et al Database System Design, implementation and management Cengage Learning, 2012.
7. Bertino et al Database security-Concepts, Approaches and challenges IEEE Transactions on dependable and secure computing, 2005.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Secured Web Services Specifications

By Sudeep Mukherjee & Dr. Rizwan Beg

Integral University Lucknow, India

Abstract - The proliferation of XML based web services in the IT industry not only gives rise to opportunities but challenges too. Namely the challenges of security and a standard way of maintaining it across domains and organisational boundaries. OASIS, W3C and other organisations have done some great work in bringing about this synergy. What I look in this paper are some of the more popular standards in vogue today and clubbed under WS-* specification. I will try to give an overview of various frameworks and protocols being used to keep web-services secure. Some of the major protocols looked into are WS-Security, SAML, WS-Federation, WS-Trust, XML-Encryption and Signature. This paper will give you a brief introduction to impact of using WS-* on time complexity due to the extra load of encrypting and certificates. Windows communication foundation (WCF) is one of the best designed toolset for this though WCF is not the topic of discussion in this paper.

Keywords : *soa; web-service; ws-security; ws-trust; ws-federation; xml; soap.*

GJCST-E Classification : *D.4.6*

Strictly as per the compliance and regulations of:

Secured Web Services Specifications

Sudeep Mukherjee [α] & Dr. Rizwan Beg [σ]

Abstract - The proliferation of XML based web services in the IT industry not only gives rise to opportunities but challenges too. Namely the challenges of security and a standard way of maintaining it across domains and organisational boundaries. OASIS, W3C and other organisations have done some great work in bringing about this synergy. What I look in this paper are some of the more popular standards in vogue today and clubbed under WS-* specification. I will try to give an overview of various frameworks and protocols being used to keep web-services secure. Some of the major protocols looked into are WS-Security, SAML, WS-Federation, WS-Trust, XML-Encryption and Signature. This paper will give you a brief introduction to impact of using WS-* on time complexity due to the extra load of encrypting and certificates. Windows communication foundation (WCF) is one of the best designed toolset for this though WCF is not the topic of discussion in this paper.

Keywords : soa; web-service; ws-security; ws-trust; ws-federation; xml; soap.

I. Introduction

Dependable and secure computing intends to provide services with a high degree of availability(A), reliability, safety, integrity (I), maintainability, and confidentiality (C)[1]. Old fashioned Human-to-Machine interaction is a forgotten story on World Wide Web. Increasingly we see that application-to-application interaction is running our internet. Therefore it is not surprising when we humans interact with the web majority of work is done by these software agents communicating with other computer systems requesting service and getting the desired result in response.

This has radically changed the efficiency as well as customer satisfaction for online business houses, so much so that many business models have no to minimal human intervention. As such new technologies, protocols and frameworks have flooded the market. Yet this great leap has a very dark side to it too. The expansion of application-application messaging infrastructure has attracted old and new attackers who are bent upon destroying or breaking this system for financial gains.

E-commerce application are the favourite hunting ground for attackers who would like nothing more than to get their hands on the sensitive back end data like, customer profile, cards, addresses etc. In the years gone by most of the companies had an easy option just install a firewall or intrusion detection software this kept their domain and data safe but as mentioned earlier with the new concept of application-to-application cross domain communication firewalls have become defunct to a large extent. Firewalls isolate an organization's network system but allow two TCP ports remain open - port 80 for HTTP and port 447 for HTTPS[2].

These ports are used for communication to send and receive Web pages. This deadly combination of easy access and human readable data is a goldmine for attackers. Irrespective of the level of SOA integration security should be one of the top priorities of any organisation. Every computer based organization must revisit their security strategy for facing new security challenges posed by Web Services. Some of these issues are

- Legacy applications work on the concept that authentication alone can filter out the unwanted attackers unfortunately this assumption in new internet infrastructure is grossly mistaken. These applications do not have the where withals to face the new age attackers.
- Most organisations to save cost have used the strategy to keep their core application the same and expose them to the World Wide Web through a layer of web-services, this causes an immediate security hole and more often than not the business logic is compromised.
- Validation checks are kept on the client-side UI, this is not the approved way of doing business in a SOA based architecture
- As mentioned earlier firewalls or packet-filters at the network level are incapable of detecting malicious behaviour of XML/SOAP based attackers.

Transport Layer Security (TLS), is the most popular tool used to secure web-based data through authentication and encryption. Unfortunately in the case of SOA because TLS works between two endpoints it has no way of protecting multiple points or intermediaries. SOAP requires protection of its messages as it is passed through a chain of intermediaries, this is the inherent nature that makes Web-Services most vulnerable.

As security solution on a transport layer, the TLS couldn't provide flexibility for message transmitting, such as encrypted different elements of the message by different key, in which recipients could only read parts of the message about him.[3]

Author α : Department of Computer Science & Engineering, Integral University Lucknow, India. E-mail : sudeep.integral@gmail.com
Author σ : HOD Department of Computer Science & Engineering, Integral University Lucknow, India. E-mail : rizwanbeg@gmail.com

Because of their nature (loosely coupled connections) and their use of open access (mainly HTTP), SOA infrastructures implemented by web services add a new set of requirements to the security landscape. Web services security requirements also involve credential mediation (exchanging security tokens in a trusted environment), and service capabilities and constraints (defining what a web service can do, under what circumstances).[4]

Let's look at some of the ways to keep Web-Services secure. This paper tries to enumerate few of the security tools that have been introduced by the industry which make Web Services more secure. The first major aspect that I will look into is Authentication.

II. Authentication

Authentication is needed to protect resources and control the access to these resources. If SOA concepts are to be implemented then the authentication procedure should be seamless between different entities and the user should not be asked to login more than once.

Service-to-service authentication is possible using variety of methods like HTTP-based to SSL certificate based. If we look into the SOAP message then the new protocols gives us an added option of passing tokens along with the SOAP request. Mostly the HTTP and SSL based authentication is transparent to the Web service while SOAP-based token protocols require interaction between Web services.

Web services that use tokens for authentication are best served by the OASIS WS-Security standard. Currently five token types are defined. These are the Username Token, X.509 token, the SAML token, Kerberos token, and the Rights Expression Language (REL) token. When a service provider attempts to access a remote Web service, it has the option to send an authentication token, impersonating the user within a WS-Security message.

1) *Username Token*
2) *X.509 Certificate Token*

An X.509 certificate specifies a binding between a public key and a set of attributes that includes (at least) a subject name, issuer name, serial number and validity interval. This binding may be subject to subsequent revocation advertised by mechanisms that include issuance of CRLs, OCSP tokens or mechanisms that are outside the X.509 framework, such as XKMS. An X.509 certificate may be used to validate a public key that may be used to authenticate a SOAP message or to identify the public key with a SOAP message that has been encrypted.[5]

3) *The Rights Expression Language (REL) Token*
4) *SAML Token*

Security Assertion Markup Language (SAML) is an XML standard for exchanging authentication and authorization data between entities SAML is a product of the *OASIS* Security Services Technical Committee.[6]
A SAML specification defines

- **Assertions**: It basically defines the three A's i.e. Attribute, Authentication and Authorization data.
- **Protocol**: This defines the main elements taking place in the Web-Service Request/Response standard and they help in packaging assertions.
- **Bindings**: Clearly lays out the way to map SAML Protocols on all the other messaging and communication protocols.
- **Profiles**: Defines the combination of bindings, assertions and protocols to support a particular use case.

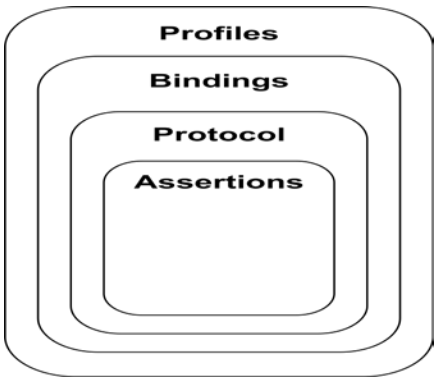


Figure 1 : SAML Structure

An assertion contains a packet of security information

<saml:Assertion…>
…
</saml:Assertion>

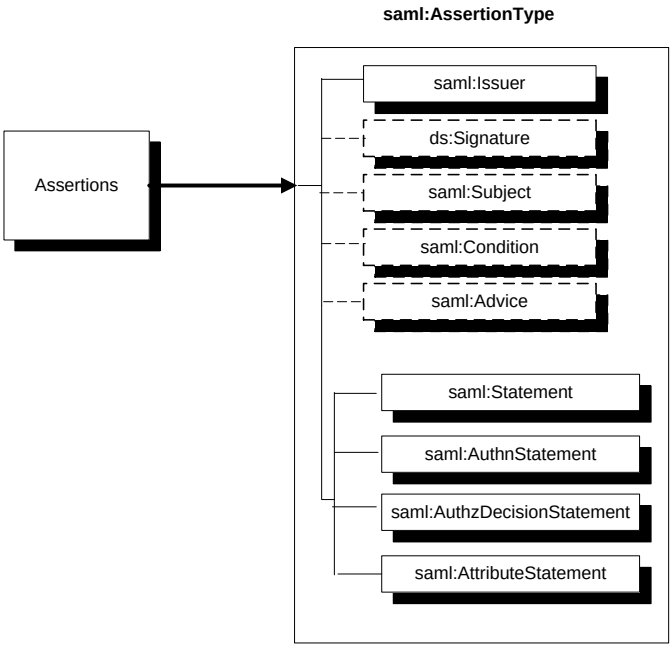


Figure 2 : SAML Assertion Element

For authentication between different organisations and their web services the best method is to use Identity and Trust based federated authentication mechanism. This sort of large scale model is well supported by WS-Trust and WS-Federation specifications developed to support WS-Security.

III. Direct Authentication

If a web-client needs to use a web-service, then the web-service will require the client to authenticate itself so as to enforce further authorization and auditing controls. Following are some of the ways this can be achieved

- A client may present either a shared secret or a password to the web-service for authentication.
- An identity server helps the web-service to validate credentials of the client.
- If the Web-service is a simple one then it may not need any authentication.
- Both the Web-service and the consumer trust one another and do not need any other kind credential management.

In all of the above cases we can use direct authentication scheme under which the Web service acts as an authentication service and the client presents its credentials for validation directly to the web-service. This credential will include some kind of shared secret and will be checked against an identity store.

IV. Brokered Authentication

Let's look at the following few scenarios which will explain the need for Brokered Authentication

The client may be using different services, i.e. more than one service.
No Trust between the service and client.
The Identity server and Web-Service have no trust.

Brokered authentication is used by the Web service to validate the credentials presented by the client. It does not need a direct relationship between client and service. This process has the following players

Client. The principal agent who initiates a request to the Web-service.

Web-Service. Web service that provides a response based on proper authentication.

Trusted Broker. By issuing a token to the client it issues a promise that the client is safe and authorized to use the Web-Service

Identity store. The server which holds the credentials for every authorized client on the domain.

Figure 4, describes these steps which will make things clearer

1) The client requests authentication from authentication broker.
2) The broker communicates with the identity store and validates the client.
3) The Broker on successful authentication responds with a security token. This token has a predefined time to live and during its lifetime it can be used by the client to authenticate itself and request any service from the server.
4) A request is submitted to the service in this request security token from the previous step is attached.
5) The service validates the security token and authenticates the incoming request as genuine and authorized.
6) If the token is validated successfully then the server responds to the client as requested in the 4th step.

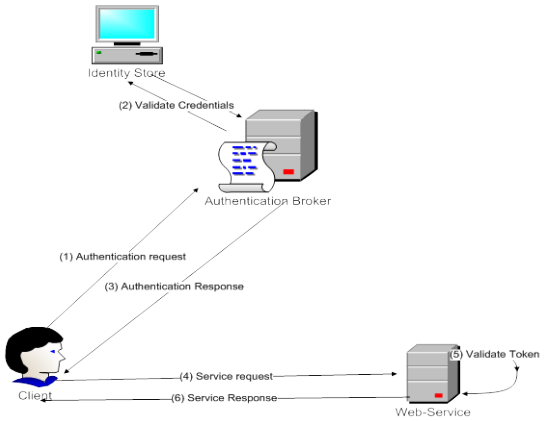


Figure 3 : Brokered authentication

Authentication brokers can be of different kind but essentially all perform the same task. Three popular authentication brokers are:

1. X.509 PKI
2. Kerberos protocol
3. Web Service Security Token Service (STS)

V. X.509 PKI

In this process we use X.509 certificates given by a certificate authority using in a public key infrastructure for verification of the credentials presented by client application.

When a Web-service receives the message, it uses the public key, to validate the signature.

Following players are involved in this method of authentication

Certificate authority. It is an authentication broker that is delegated with the task of generating and forwarding X.509 certificates.

Client. The principal agent who initiates a request to the Web-service and needs to authenticate itself with the token provided by the broker.

Web-Service. Web service that provides a response based on proper authentication.

In order to ensure a consistent processing model across all the token types supported by WSS: SOAP Message Security, the <wsse: Security Token Reference> element SHALL be used to specify all

references to X.509 token types in signature or encryption elements that comply with this profile.[5]

VI. Brokered Authentication: Kerberos

Kerberos protocol can be used for authentication. It will work like a broker between the client and the server. The client sends a request to the broker for a ticket. The broker returns a service ticket and session key used to create a Kerberos security token. The security token carries the service ticket and a special piece of data called *authenticator.* This is encrypted by using the session key. The client can now send the Kerberos security token with its request to the Web service.

On receipt of this token, web-service extracts encrypted ticket. Then it uses its own service key to decrypt the service ticket. This session key from the service ticket is used to decrypt the authenticator and authenticate the client.

Figure 5 summarizes the following steps

1. Client in its request attaches a Ticket Granting Ticket and forwards it to the KDC.
2. In response to the above request KDC generates a session key and service ticket. It contains data for client authorisation and the new session key. To protect the ticket KDC uses the Public Key of Web-service to encrypt it. On arrival of the response Client decrypts the session key and the authenticator is encrypted with this session key. The new Security Token in this case includes the authenticator and the ticket sent by the KDC.
3. The client is sends a request with this security token attached to the Web-service.
4. On receipt of such a message the Web-service uses its private key to decrypt the Service Ticket. This ticket contains the session key which is used to decrypt the authenticator. After the security token is validated, the Web-service is now ready to respond to the client.

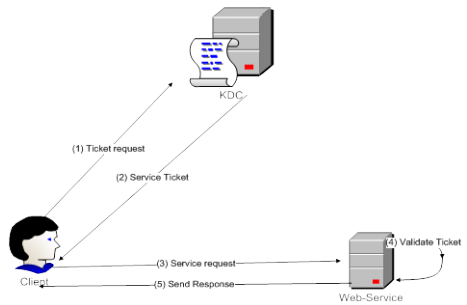


Figure 4 : Kerberos Brokered Authentication

VII. Brokered Authentication: WS-Trust & WS-Federation

Let's assume that many different clients have their authentication implemented on different platforms. We are required to bring seamless interoperability among these different clients. Only way to implement this is through the concept of Identity management and trust implementation.

Another use-case which ways in favour of these two is that sometimes organisations need security tokens which can be extended to support extra security. Thus we require a way that broker can be flexible enough to adjust to the needs of the user. This too can be achieved by Identity management.

Most of the commercial domains are protected by well entrenched firewalls thus one of the requirements for security can be that the security tokens must easily traverse or pass through these firewalls using the ports that re standard. As discussed earlier single sign on facility can be a by-product of this kind of security structure.

a) Identity Management

With SOA security stack Identity management has a very broad spectrum and it covers everything from documents, information, identity-related events etc. All of these can be used to confirm the identity of the client and authenticate him at the entry point of our SOA implementation. Under the security architecture of SOA an entity's identity is the basis for trust as well as authorisation.

b) Identity Management Architectures

There are three major identity architectures available for use in Web services:
Isolated identity management.
Federated identity management.
Centralized identity management.

c) Usage of Identity Management with Web Services

According to Axel Buecker and Heather Hinton, successful cross-organizational Web services require a way for providers to securely identify and provide services to authorized requesters and a way for requesters to securely invoke Web services with the necessary credentials.[7]

Without a proper identity framework things can become complicated in the Web-services environment. Let's say an organization Sudeep Inc. uses X.509 certificates to identify Web services and clients, while another company XYZ Ltd. has Kerberos tickets for identification. If a client from XYZ Ltd sends a request to a web-service under the domain of Sudeep Inc we will have a big issue as the client will have Kerberos ticket attached with the message while the web-service requires a X509 certificate. Even though both client and web-service are genuine yet the communication will fail. To make life easier for cross-domain and organisation communication we use Identity management frameworks. This enables the Web servers to safely identify each other. Irrespective of what kind of security apparatus is being used individually. According to

Buecker and Hinton, organizations need only develop a single set of Web services to facilitate Web service identity management across organizational boundaries:

Trust services.
Authentication and validation services.
Identity and attribute mapping services.
User lifecycle management services.
Authorization services.

d) Federated identity management

If you need to establish a business in a distributed environment then the first requirement is to manage identities in a federated way.

A federation is a set of organizations that establish trust relationships with respect to the identity information the federated identity information that is considered valid. A federated identity management system (IdM) provides a group of organizations that collaborate with mechanisms for managing and gaining access to user identity information and other resources across organizational boundaries[8].

This simplifies identity and credential management for the SOA as a whole, but requires individual services to be aware of and trust assertions from one another. In a single enterprise- wide SOA, it may not be difficult for providers to trust one another, but they may be less willing to trust assertions when the SOA includes providers from different organizations. A requester in the SOA may make a request to a provider and supply an arbitrary assertion to gain access. In identity federation, it is important to develop organizational policies appropriate for the types of data that traverse the SOA.

This benefits the user as well because they don't have to remember different credentials for different services of the same organisation. A single credential authenticates them for every service. This in turn increases the user experience. Many IdM systems use cookies to make user information available to servers. State information is stored at the client, which sends the cookie to the server the next time the user accesses that server. Like session and trust tickets, cookies can be valid only for the session during which they were issued or can persist beyond the session's end. A persistent cookie is typically written to a file on the browser's hard drive if its lifetime hasn't elapsed when the browser is shut down and therefore can be used for a longer period of time.[8]

Different Roles in Federated Identity Management Framework.

The two major roles are the identity provider and service provider or the Web-Service.

1) Identity provider
2) Service provider

e) Trust management

Trust is contract between two parties which entails them to believe the claims made by each other. Trust management is the process of or model for creating relationships amongst the different entities in an organisation, domains or systems. This infrastructure is created by cryptographic methods

Creating Trust amongst Web-Services

If a signed SAML or WS-Security message cannot be guaranteed to be trustworthy during communication between remote clients, then neither is of any use to anybody. Originally SAML had direct trust relationship but now it has brokered trust and community trust model too.

Direct trust relationships are the simplest of all because each entity has a copy of others public key and uses it to authenticate the communicating partner. It may be simple but not at all scalable.

Direct trust relationship has been enhanced and named as Brokered trust model. Under this scheme when two pairs are communicating with each other it is not necessary for them to share their public keys instead they exchange each other keys with the usage of Trusted Third Party. This model scales better as compared to the Direct Pairwise model.

Public Key Infrastructure is central to the third model called community trust model. Under this scheme trust is established through an external PK I. This model is as simple as direct Pairwise model yet more scalable than the brokered trust model.

Trust Federation Frameworks

Let's look at some of the frameworks now being used to provide trust framework for web-services. It is up to the company to decide which framework is best suited for its unique needs.

SAML

SAML, developed by the Security Services Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS), is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application.[9]

WS-Trust

This protocol was developed and proposed by IBM, Microsoft, RSA, Verisign, BEA, and several other vendors. Stated goal of all these vendors was to create a federation system which has its root in SOAP and WSDL but uses the WS-Security extensions too.

WS-Trust addresses these issues by:

- Defining a request/response protocol
  - Client sends RequestSecurityToken
  - Client receives Request Security Token Response
- Introducing a Security Token Service (STS)

Brokered authentication with STS involves the following participants:

- **Client**. The client accesses the Web service.
- **STS**. The STS is the Web service that authenticates clients by validating credentials that are presented by a client.
- **Service**. The service is the Web service that requires authentication of a client prior to authorizing the client.[10]

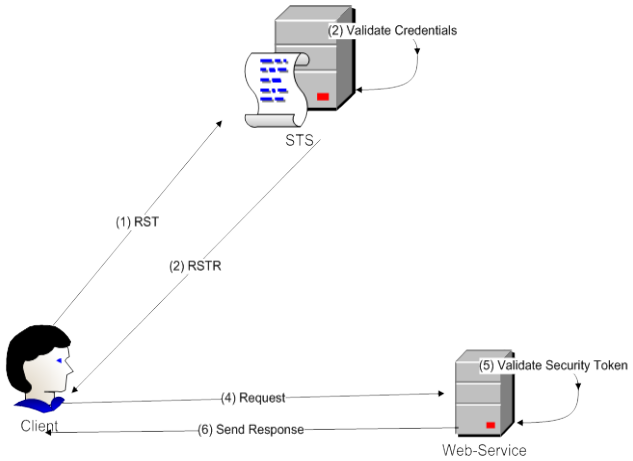


Figure 5 : STS token issuance and request/response

WS-Federation

The goal of federation is to allow security principal identities and attributes to be shared across trust boundaries according to established policies. The policies dictate, among other things, formats and options, as well as trusts and privacy/sharing requirements. In the context of web services the goal is to allow these identities and attributes to be brokered from identity and security token issuers to services and other relying parties without requiring user intervention (unless specified by the underlying policies). This process involves the sharing of federation metadata which describes information about federated services, policies describing common communication requirements, and brokering of trust and tokens via security token exchange (issuances, validation, etc.).

Federations must support a wide variety of configurations and environments. This framework leverages the WS-* specifications to create an evolutionary federation path allowing services to use only what they need and leverage existing infrastructures and investments. Federations can exist within organizations and companies as well as across organizations and companies. They can also be ad-hoc collections of principals that choose to participate in a community. [11]

Requestor: A programmatic agent for obtaining information or service

Subject: The entity on whose behalf a Request or operates

Claims: Statements made about a subject.

Security Token: A data structure for expressing collections of claims

Security Token Service (STS): A Web service that provides issuance and management of security tokens.

Identity Provider (IP): An entity, typically a trusted third party authority that provides claims about a set of Subjects

IP/STS: STS operated by an IP to issue claims using tokens

Relying Party (RP): An entity that provides information or services to Requestors based on claims they present

Target Service: A web service (or application) operated by an RP

RP/STS: STS operated by a RP to issue claims using tokens[12]

WS-Federation expands on WS-Trust by providing various protocols by which STSs (interchangeably called Identity Providers in WS-Federation), requesters, and providers can interact with one another to allow Web services to trust each other across organizational boundaries. Each organization is a separate *trust realm*. WS-Federation allows Web services to communicate between multiple trust realms. Additionally, WS-Federation provides two profiles for how requesters interact with providers and STSs: the active requester profile and the passive requester profile. The passive requester profile details how messages should be passed between a requester Web browser, the provider, the Identity Providers (IPs) and STSs of both organizations so that WS-Federation can be used within the context of Web applications, providing users with a single sign-on experience. The active requester profile details how requesters should interact with the provider and the IP/STSs to access a provider in another trust realm. [13]

VIII. SOAP Message Security -XML Security

SOAP is the base on which communication through message interchange structure is built. SOAP itself is a XML based protocol. Unfortunately the data in the SOAP message are vulnerable to confidentiality and integrity threats. We all know that TLS provides end-to end security, unfortunately SOAP headers can be modified by intermediary nodes leaving a big security hole. To further make matter worse are the different protocols of different networks which may be the intermediary node. If we implement security on the XML level it helps in improving source integrity and confidentiality.

As used in computer security, cryptography provides the following processes:[14]

- ✓ Encrypting converts plaintext (that is, data in normal, readable form) into cipher text, which conceals the

meaning of the data to any unauthorized recipient. Encrypting is also called enciphering. Most cryptographic systems combine two elements:

- An algorithm that specifies the mathematical steps needed to encrypt the data.
- A cryptographic key (a string of numbers or characters), or keys. The algorithm uses the key to select one relationship between plaintext and cipher text out of the many possible relationships the algorithm provides. The selected relationship determines the composition of the algorithm's result.
- ✓ Decrypting converts cipher text back into plaintext. Decrypting is also called deciphering.
- ✓ Hashing uses a one-way (irreversible) calculation to condense a long message into a compact bit string called a message digest.
- ✓ Generating a digital signature involves encrypting a message digest with a private key to create the electronic equivalent of a handwritten signature. You can use a digital signature to verify the identity of the signer and to ensure that nothing has altered the signed document since it was signed.

WS-Security provides much flexibility, marrying SOAP messaging with multiple security standards and technologies: The standard extends the SOAP Header to provide security information for secure messaging, it leverages lower-level standards such as XML Signature and XML Encryption, it is extensible to support multiple token formats for identity and authorization, and it supports multiple trust models for sharing security contexts.[15]

WS-Security gives us the added benefit of using multiple encryptions within the same SOAP message, thus various parts of the same SOAP message can be encrypted for different receivers (SOAP intermediaries). In the same way an intermediary can add its own additional signature to the message. This has the effect of providing integrity protection for newly added header. XML Signature and XML Encryption are the first line of defence in XML and Web services security. Therefore both are well supported in available products and development API's.

WS-Security has the added advantage of providing a mechanism for avoiding replay attacks (i.e., timestamps) and a way to add security tokens to the message being communicated. A drawback of WS-Security is that it has no concept of session, and it is focused on securing a single SOAP message or a single SOAP request/response exchange. Where we require security for multiple message exchanges, WS-Secure Conversation is the protocol that can be used to maintain a security context.

IX. XML-Signature

Signatures are used to verify message origin and integrity. Signatures are also used by message producers to demonstrate knowledge of the key, typically from a third party, used to confirm the claims in a security token and thus to bind their identity (and any other claims occurring in the security token) to the messages they create.[16]

XML Signature is the specification that defines a standard interoperable format for representing digital signatures in XML. It lays out a method that shows us a way to efficiently apply signature to primarily XML messages. It can be used on binary files too but that is not the focus of this paper

XML Signature gives us a practical and flexible signature mechanism. Yet coders must think about the threat perception of their application and should keep in mind few of these points

A. What is Signed is Secure
B. Only data item should be signed
C. Signature for external references too

X. XML Encryption

XML Encryption has been designed to provide SOAP/XML documents confidentiality by encrypting them completely or partially. Both XML Encryption and XML Signature are similar standards. Even encryption is not only limited to XML but it can be used for binary data too. This standard demands support for both Triple-DES and AES-128/256.

XI. Impact Of Security on Time Complexity

Though security is now an inevitable part of modern communication yet we must be prepared to sacrifice a bit on time complexity. In this section I have tried to bring out some differences between secured and unsecured web-service. The web-service used are technically very simple, they have separate functions for primitive data types and a simple class. We will be calling the web-service from a client application in three scenarios.

1. First scenario will be when client and server applications are on the same machine
2. Second scenario will be when client and server are on different machines but in the same domain.
3. Third scenario will be with the server application on a shared host and will be accessed by the client over the internet.

The factors which I have taken into account are as follows.

- Reliable Messaging
- Security
- Concurrent Clients

The result variable has been kept simple. I will measure the output by comparing the Response Time

which is the total time elapsed from the point client makes a request to the time client receives a response. The experiment uses simple data types as messages and to even out any kind of noise or disturbance each experiment has been replicated 100 times. The need for replication arose due to the variance in Response Time between two identical requests. The reason for such a variance is manifold, it could be due to network latency, client machine lag or server load. To summarize the data I have calculated Average Response Time, which tends to reduce the effect of noise on the data. It may be argued that the output variable should have been more complex or dependent on other factors but this paper doesn't deal with it. Following table summarizes the data.

Firstly we find that when web-services do not use 'Reliable Messaging' and 'Security' the average response time is always lower. Unfortunately in many scenarios not using security is not an option.

Secondly looking at time complexity I would say that using only Reliable Messaging is much better than using security. If we are forced to use both types of security then performance is surely to take a severe hit as represented in the data table.

Third point which becomes apparent is that if number of concurrent user increases the performance decreases. This is true for most software's but in web-services we must understand that this becomes more critical as web-services are meant for an environment where number of users are not fixed and more often than not internet will be the communication medium.

The experiment quite clearly brings out the problem with using security on web services. Unfortunately there are no other alternatives at present. Therefore if we require security then we must be ready to sacrifice response time. My experiment is not definitive due to the fact I have ignored all error mechanisms and 'data noise'. Noise tends to pollute the result. Plus I have used simple messages instead of complex messages.

XII. Conclusion

The standards I have looked into are not the only one in existence there are many more and depending on your needs you might have to look at few of them.

Web services have this great ability to produce extremely inter-operable systems and loosely coupled architecture. It is and will give every organisation a high degree of flexibility in their solution architecture. If we are to use this inherent flexible nature to its full, it is essential to understand the security threats lurking in the shadows and devise methods to minimize or eradicate these threats. Fortunately most of the vendors have jumped on this bandwagon thus we see so many security standards are being designed. Many of these vendors like IBM, Microsoft, Google etc are churning out API's and tools to support these security standards. We as developers are fortunate to be spoilt for choices.

If we look at the most widely used languages of web like C#, VB.NET and each one of them already have API's in place to tackle security issues. Unfortunately the specifications are standard but the API's are not. Thus there are quite a few differences in all these competing vendor specific implementation.

Next problem is the user apathy toward implementation of these new standards. Robust security for Web Services is mandatory and most of the technology, standards protocols etc are already in place. The problem lies in mapping this existing security technology to XML and SOAP, and it is neither easy nor short. This mapping is of non-trivial nature and you need a deep understanding of the specifications as well as the language. If either of the knowledge is missing you will end up implementing faulty security for your services.

Once the user and the vendor are on the same wave length we will see the world of secured and completely seamless interoperable world of web services that we all want become reality. Use of a defined set of interfaces, along with centralized identity and access control policies, will reduce the risk of user access to unrelated resources. Running computing services in isolated domains, providing default encryption of data in motion and at rest, and controlling data through virtual storage have all become activities that can improve accountability and reduce the loss of data. In addition, automated provisioning and reclamation of hardened run-time images can reduce the attack surface and improve forensics.[17]

References Références Referencias

1. R. A. Lutz Lowis, "Vulnerability Analysis in SOA-Based Business Processes," presented at the IEEE TRANSACTIONS ON SERVICES COMPUTING, 2011.
2. "The XML Security Gap: It's Bigger than you think," White Paper2003.
3. K. Hongzhao, "A Study on the Security Mechanism for Web Services," presented at the World Congress on Engineering and Computer Science, San Francisco, USA, 2010.
4. V. Jain. (2009 20/09/2012). Securing Web Services and Service- Oriented Architectures with Oracle Web Services Manager 11g [White Paper].
5. OASIS, "Web Services Security X.509 Certificate Token Profile 1.1," in *Introduction*, ed: OASIS Open, 2006.
6. T. H. Nathan Klingenstein, Hal Lockhart,Scott Cantor, Anil Saldhana. (2012 08/09/2012). *OASIS Security Services (SAML) TC*. Available: https://

www.oasis-open.org/committees/tc_home. php?wg_abbrev=security
7. P. A. Axel Buecker, Neil Readshaw, "Federated Identity and Trust Management," ed. USA: IBM, 2008.
8. S. ABHILASHA BHARGAV, ANNA C.SQUICCIARINI, ELISA BERTINO, "Trust Negotiation in Identity Management," presented at the IEEE SECURITY & PRIVACY, 2007.
9. OASIS, "SAML V2.0 Executive Overview," in *Committee Draft*, ed: OASIS, 2005.
10. Microsoft. (2005, 29/10/2012). *Brokered Authentication: Security Token Service (STS)*. Available: http://msdn.microsoft.com/en-us/ library/ff650503.aspx
11. OASIS, "Proposed Charter: OASIS Web Services Federation (WSFED) Technical Committee," in *WS-Federation Specification Overview*, ed, 2007.
12. OASIS, "WS-Federation 1.1 Overview," ed. OASIS WSFED: OASIS, 2007.
13. T. W. Anoop Singhal, Karen Scarfone, "Guide to Secure Web Services," vol. 800-95, ed. USA: National Institute of Standards and Technology, 2007.
14. C. A. Nigel Williams, Arnaud Desprets,Tommy Joergensen,James O'Grady, "Securing CICS Web Services," in *Securing CICS Web Services* vol. First Edition, 1 ed: IBM, 2008, p. 70.
15. B. L. Mike Rosen, Kevin T. Smith,Marc J. Balcer, *Service-Oriented Architecture and Design Strategies*. Indianapolis: Wiley Publishing, Inc., 2008.
16. OASIS, "Web Services Security:SOAP Message Security 1.1," in *Message Security Model*, ed: OASIS, 2006, p. 13.
17. IBM. (2009, IBM Point of View: Security and Cloud Computing. *Cloud computing White paper,* 19. Available: ibm.com/cloudcomputing

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Wireless Sensor Network Security Model for D2P Attacks Using Zero Knowledge Protocol

By Mukesh Kansari & Mrs.Shikha Pandey

Rungta College of Engineering and Technology, Bhilai (C.G.), India

Abstract - Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, low-power, small-size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network. These small devices used in wireless sensor nodes are called sensor nodes. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring in the near future. In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the operational conditions are most often harsh or even hostile. Since these networks are usually deployed in remote places and left unattended, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes.

Keywords : *sensor nodes, threats, wsn, attacks, security.*

GJCST-E Classification : *C.2.1*

Strictly as per the compliance and regulations of:

Wireless Sensor Network Security Model for D2P Attacks Using Zero Knowledge Protocol

Mukesh Kansari [α] & Mrs.Shikha Pandey [σ]

Abstract - Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, low-power, small-size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network. These small devices used in wireless sensor nodes are called sensor nodes. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring in the near future. In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the operational conditions are most often harsh or even hostile. Since these networks are usually deployed in remote places and left unattended, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes.

Keywords : sensor nodes, threats, wsn, attacks, security.

I. Introduction

A Wireless Sensor Network is a special type of network that consist of distributed, low-power, small-size devices using sensors to cooperatively collect information through infrastructure less ad-hoc wireless network [1]. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to building security monitoring in the near future [2]. It shares some commonalities with a typical computer network, but also exhibits many characteristics which are unique to it. The security services in a Wireless Sensor Network should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most important security requirements in Wireless Sensor Network are listed below:

Data confidentiality: The security mechanism should ensure that no message in the network is understood by anyone except intended recipient. A sensor node should not allow its readings to be accessed by its neighbors unless they are authorized to do so.

Author α : M.Tech (SE) Dept. of Computer Science and Engg. Rungta College of Engineering and Technology, Bhilai (C.G.), India.
E-mail : kansari256@gmail.com
Author σ : Assitt. Professor Dept. of Computer Science and Engg Rungta College of Engineering and Technology, Bhilai (C.G.), India.
E-mail : shikhamtech2008@gmail.com

Data integrity: The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.

Data freshness: It implies that the data is recent and ensures that no adversary can replay old messages. This requirement is especially important when the WSN nodes use shared keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN.

Self-organization: Each node in a WSN should be self organizing and self-healing. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [3].

Secure localization: In many situations, it becomes necessary to accurately and automatically locate each sensor node in a WSN. For example, a WSN designed to locate faults would require accurate locations of sensor nodes identifying the faults. A potential adversary can easily manipulate and provide false location information by reporting false signal strength, replaying messages etc. if the location information is not secured properly. Authentication: It ensures that the communicating node is the one that it claims to be. An adversary can not only modify data packets but also can change a packet stream by injecting fabricated packets. It is, therefore, essential for a receiver to have a mechanism to verify that the received packets have indeed come from the actual sender node.

II. Charesterstics & Applications of Wsns

There is following characteristics of WSN which are-

Power consumption constrains for nodes using batteries or energy harvesting, Communication failures, Ability to cope with node failures, Mobility of nodes, Dynamic network topology, Heterogeneity of nodes, Scalability to large scale of deployment, Ability to withstand harsh environmental conditions, Easy of use Unattended operation.

Applications of WSN are-

Area monitoring,
Environmental monitoring Greenhouse monitoring Landslide detection,
Industrial monitoring Machine

health monitoring,
Water/Wastewater Monitoring Landfill ground well level monitoring and pump counter agriculture, Fleet monitoring, Health Monitoring Security.

III. Security Attacks in Wsn

Wireless Sensor Networks are vulnerable to various types of attacks. These attacks are mainly of three types (denial of service attack, distributed attack and phishing attack.), Attacks on secrecy and authentication: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks. Attacks on network availability: attacks on availability of WSN are often referred to as denial-of-service (DoS) attacks. Stealthy attack against service integrity: in a stealthy attack, the goal of the attacker is to make the network accept a false data value. In these attacks, keeping the sensor network available for its intended use is essential. The DoS attack usually refers to an adversary's attempt to disrupt, subvert, or destroy a network. However, a DoS attack can be any event that diminishes or eliminates a network's capacity to perform its expected functions.

IV. DoS Attacks

Wood and Stankovic have defined a DoS attack as an event that diminishes or attempts to reduce a network's capacity to perform its expected function. Some of the important types of DoS attacks in Wireless Sensor Networks are discussed below.

a) Physical Layer Attacks

The physical layer is responsible for frequency selection, modulation, and data encryption [4]. As with any radio-based medium, the possibility of jamming is there. In addition, nodes in Wireless Sensor Networks may be deployed in hostile or insecure environments where an attacker has the physical access. Two types of attacks in physical layer are (i) jamming and (ii) tampering.

b) Link Layer Attacks

The link layer is responsible for multiplexing of data streams, data frame detection, medium access control, and error control [4]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation.

c) Network Layer Attacks

The network layer of Wireless Sensor Networks is vulnerable to the different types of attacks such as: spoofed routing information, selective packet forwarding, sinkhole, Sybil, wormhole, hello flood etc.

i. *Spoofed routing information*

The most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network [5].

ii. *Selective forwarding*

Thn a multi-hop network like a Wireless Sensor Network, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others [5].

iii. *Sinkhole*

In this attack, a malicious node acts as a blackhole [6] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. Fig 1 shows the conceptual view of a sinkhole attack.

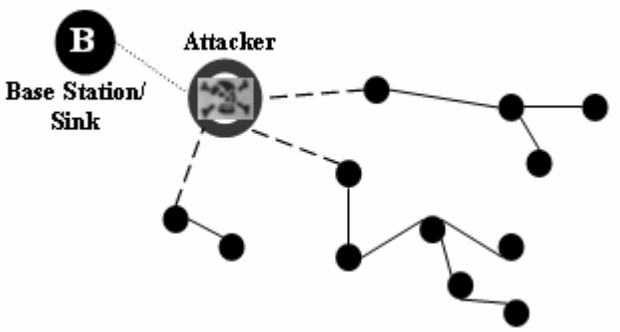


Figure 1 : Sinkhole Attack

iv. *Sybil attack*

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack [7]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [7]. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to Sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Douceur [8] showed that, without a logically centralized authority, Sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity

and coordination among entities. However, detection of Sybil nodes in a network is not so easy.

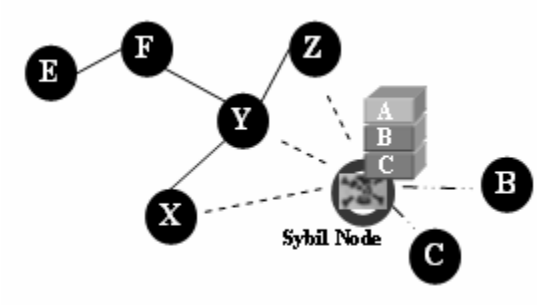


Figure 2 : Sybil Attack

v. *Wormhole*

Wormhole attack [9] is a critical attack in which the attacker records the packets at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information.

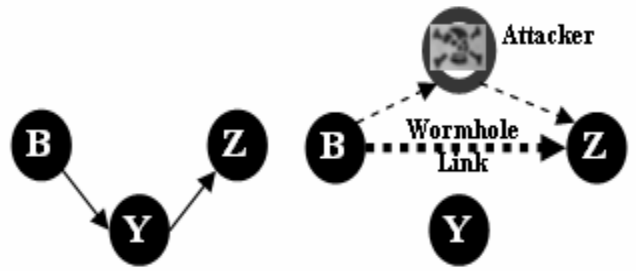


Figure 3 : Wormhole Attack

Fig 3 shows a situation where a wormhole attack takes place. When a node B broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multi-hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

vi. *Hello flood*

Most of the protocols that use Hello packets make the naive assumption that receiving such a packet implies that the sender is within the radio range of the receiver. An that receiving such a packet implies that the sender is within the radio range of the receiver. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighborhood [5]. Subsequently, the attacker node falsely broadcasts a shorter route to the base station, and all the nodes which received the Hello packets, attempt to transmit to the attacker node.

vii. *Acknowledgment spoofing*

Some routing algorithms for Wireless Sensor Networks require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighboring nodes and spoof the acknowledgments thereby providing false information to the nodes [5].

d) Transport layer attacks

The attacks that can be launched on the transport layer in a Wireless Sensor Network are flooding attack and de-synchronization attack.

i. *Flooding*

Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

ii. *De-synchronization*

De-synchronization refers to the disruption of an existing connection. An attacker may, for example, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist.

e) Attacks on secrecy and authentication

There are different types of attacks under this category as discussed below:

i. *Node replication attack*

In a node replication attack, an attacker attempts to add a node to an existing WSN by replication the node identifier of an already existing node in the network. A node replicated and joined in the network in this manner can potentially cause severe disruption in message communication in the Wireless Sensor Network by corrupting and forwarding the packets in wrong routes.

ii. *Attacks on privacy*

Since Wireless Sensor Networks are capable of automatic data collection through efficient and strategic deployment of sensors, these networks are also vulnerable to potential abuse of these vast data sources. Privacy preservation of sensitive data in a Wireless Sensor Network is particularly difficult challenge [10]. Moreover, an adversary may gather seemingly innocuous data to derive sensitive information if he knows how to aggregate data collected from multiple

sensor nodes. Following are some of the common attacks on sensor data privacy [10].

iii. *Eavesdropping and passive monitoring*

This is most common and easiest form of attack on data privacy. If the messages are not protected by cryptographic mechanisms, the adversary could easily understand the contents. Packets containing control information in a WSN convey more information than accessible through the location server, Eavesdropping on these messages prove more effective for an adversary.

iv. *Traffic analysis*

In order to make an effective attack on privacy, eavesdropping should be combined with a traffic analysis. Through an effective analysis of traffic, an adversary can identify some sensor nodes with special roles and activities in a WSN.

v. *Camouflage*

An adversary may compromise a sensor node in a WSN and later on use that node to masquerade a normal node in the network. This camouflaged node then may advertise false routing information and attract packets from other nodes for further forwarding. After the packets start arriving at the compromised node, it starts forwarding them to strategic nodes where privacy analysis on the packets may be carried out systematically.

V. Distributed Attack

A distributed attacks occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Distributed attacks are traditionally viewed to be fundamentally more difficult to detect than single-source attacks. One reason why distributed attacks are difficult to contain is because defenses against these attacks are typically deployed at edge networks, near the victim. Deploying defenses at the edge makesdetecting attacks easier,

VI. Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

VII. Challenges

There are following challenges occurring in the wireless technology which are given in the following two categories- Challenges Vs Internet:

1. Bandwidth is very expensive in WSNs
2. Ad-hoc
3. Energy
4. Wireless and Collaborative use
5. Collect and

Decimate Research Challenges:

1. Medium Access Control (MAC)
2. Routing
3. Localization
4. Operating Systems
5. Security
6. Programming Abstractions and Query Processing

VIII. Conclusion

Wireless Sensor networks have become promising future to many applications. In the absence of enough security, deployment of sensor networks is vulnerable to variety of attacks. Overall security for wireless sensor networks is very hard to develop due to the limited resources of the sensors. Sensor network security will always be a field in which much work needs to be done. Current research in sensor network security is mostly built on a trusted environment [11]; however there are several research challenges remain unanswered before we can trust on sensor networks. In this paper we have discussed threat models and unique security issues faced by wireless sensor networks. In WSNs, there are still some challenges that are to be addressed.

References Références Referencias

1. Tan f Akylidiz, Weliain S U, yogesh sankarasubramaniam and eradal caryici. "A survey on Sensor Networks" IEEE Communication Magazine, august 2002.
2. Yuanzhu Peter Chen Arthur L. Liestman Jiangchuan Liu. "Energy-Efficient Data Aggregation Hierarchy for Wireless Sensor Networks" Proceedings of the 2nd Int'l Conf. on Quality of Service in Heterogeneous Wired/Wireless Networks August 2005.
3. L. Eschenauer and V.D. Gligor, "A key- management scheme for distributed sensor networks", In Proceedings of the 9th ACM Conference on Computer and Networking, pp. 41- 47, Nov 2002.
4. D. Braginsky and D. Estrin, "Rumor routing algorithm for sensor networks", In Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications", pp. 22-31, New York, NY, USA, 2002, ACM Press.
5. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

6. Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.
7. Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international Symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.
8. Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).
9. Hu, Y.-C., Perrig, A., and Johnson, D.B. "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986.
10. M Gruteser, G. Schelle, A. Jain, R. Han, and D. Grunwald, "Privacy-aware location sensor networks", In Proceedings of the 9th USENIX Workshop on Hot Topics in Operating Systems, (HotOSIX), 2003.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Improvement in Congestion Control Using Multipath Routing in Manet

By Mr. Abhishek Bande & Mr. Gaurav Deshmukh

University of Pune, Maharashtra India

Abstract - The ad hoc connections, which opens many opportunities for MANET applications. In ad hoc network nodes are movable and there is no centralised management. Routing is an important factor in mobile ad hoc network which not only works well with a small network, but also it can also work well if network get expanded dynamically. Routing in Manets is a main factor considered among all the issues. Mobile nodes in Manet have limited transmission capacity, they intercommunicate by multi hop relay. Multi hop routing have many challenges such as limited wireless bandwidth, low device power, dynamically changing network topology, and high vulnerability to Failure. To answer those challenges, many routing algorithms in Manets were proposed. But one of the problems in routing algorithm is congestion which decreases the overall performance of the network so in this paper we are trying to identify the best routing algorithm which will improve the congestion control mechanism among all the Multipath routing protocols.

Keywords : *disjoint multipath, multi hop, reliability, congestion control, optimization.*

GJCST-E Classification : *C.2.2*

Strictly as per the compliance and regulations of:

An Improvement in Congestion Control Using Multipath Routing in Manet

Mr. Abhishek Bande[α] & Mr. Gaurav Deshmukh[σ]

Abstract - The ad hoc connections, which opens many opportunities for MANET applications. In ad hoc network nodes are movable and there is no centralised management. Routing is an important factor in mobile ad hoc network which not only works well with a small network, but also it can also work well if network get expanded dynamically. Routing in Manets is a main factor considered among all the issues. Mobile nodes in Manet have limited transmission capacity, they intercommunicate by multi hop relay. Multi hop routing have many challenges such as limited wireless bandwidth, low device power, dynamically changing network topology, and high vulnerability to Failure. To answer those challenges, many routing algorithms in Manets were proposed. But one of the problems in routing algorithm is congestion which decreases the overall performance of the network so in this paper we are trying to identify the best routing algorithm which will improve the congestion control mechanism among all the Multipath routing protocols.

Keywords : disjoint multipath, multi hop, reliability, congestion control, optimization.

I. Introduction

Mobile Ad hoc network is a self configuring, self organizing and self maintaining dynamic network. A mobile ad hoc network (MANET) is a network consisting of a set of mobile nodes with no centralized administration [1,2]. In mobile ad hoc network nodes are in movable format means they can form any topology as they change their position so by considering nodes are movable we are currently having many protocols for routing in multipath. The main objective of multipath routing protocols is to provide reliable communication and to ensure load balancing ad to improve quality of service of MANETs. These multipath protocols are broadly classified into five categories to improve delay, provide reliability, reduce overhead, maximize network life and hybrid routing. In multipath routing protocols have issues for multiple paths discovery and maintaining these paths. Issues, objectives, performances, advantages and disadvantages of these protocols are summarized. In MANETs each mobile node has limited resources such as battery, processing power, and on-board memory (i.e., RAM). In MANETs, mobile nodes communicate with each other in a multi-hop fashion. That means a mobile node sends a packet to a destination via intermediate nodes. Hence, the availability of each node is equally important in MANETs. Otherwise, overall performance of the network may be affected by single intermediate node. In order to meet these characteristics and design constraints, an efficient routing protocol is essential for MANET. Designing an efficient routing protocol for MANETs is a very challenging task to achieve. Many routing protocols have been proposed and these protocols can be classified as proactive and reactive. In proactive routing protocols like destination sequence distance vector (DSDV) mobile nodes update their routing tables by periodically exchanging routing information among themselves. Proactive routing protocol generates large number of control messages in the network due to periodic information exchanges. Hence, proactive routing protocols are not considered suitable for MANET. To overcome the limitations of proactive routing protocols [3], reactive routing protocols like dynamic source routing (DSR) and ad hoc on-demand distance vector routing (AODV) protocols have been proposed for MANET. In reactive routing protocol, a route is discovered when it is required. Reactive routing protocol consists of two main mechanisms: (a) route discovery and (b) route maintenance. A source node discovers a route to a destination by using the route discovery mechanism. On the other hand, a source node detects any topology change in the network by using the route maintenance mechanism. In route discover procedure Once all paths have been discovered [4], a source node chooses a path, which is the shortest and stores remaining paths in database. When the shortest path algorithm is used, nodes which is located around the center of a network may carry more traffic compared to other nodes that are located at the other or boundary of the same network. When multiple connections are setup in a network, the wireless links located at the center of the network carry more traffic and can, therefore network gets congested. This type of congestion problem may affect the performance of a network in terms of delay, throughput and reliability. If source node chooses shortest path then it may break due to node movement as nodes are movable. Moreover, communication through a wireless medium is inherently unreliable and is also subjected to link errors like UDP.

Multipath routing protocols proposed for MANET can be broadly classified as [5] (a) delay aware multipath routing protocols, (b) reliable multipath routing

Author α σ : Department of Computer Engineering, University of Pune, Maharashtra India. E-mails : abhishek.bande2008@gmail.com, deshmukhgaurav9@gmail.com

protocols, (c) minimum overhead multipath routing protocols,(d) energy efficient multipath routing protocols and(e) hybrid multipath routing protocols. In this paper we are covering all the protocols which are for multipath based on congestion control.

II. Literacher Servey

a) Computer Network

A Network is defined as the group of people or systems or organizations who want to share their information collectively for their business purpose. In Computer terminology the definition for networks is similar as a group of computers logically connected for the sharing of information or services (like print services, multi-tasking etc.). These networks may be fixed (cabled, permanent) or temporary.

Types of Computer Network: There are mainly two types of computer networks a) Wired Network b) Wireless Network

i. *Wired Network*

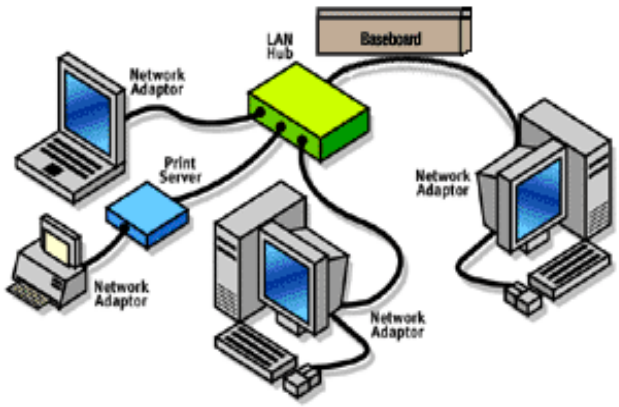


Fig. (a) : Wired Network

The wired networks are generally connected with the help of wires and cables means there exist a physical connection between two computers. Generally the cables being used in this type of networks are CAT5 or CAT6 cables. The connection is usually established with the help of physical devices like Switches and Hubs in between to increase the strength of the connection. In wired network there is a reliability of data to be reached at destination. Following are some advantages of wired network.

Advantages:

A wired network offer connection speeds of 100Mbps to 1000Mbps. Physical, fixed wired connections are not prone to interference and fluctuations in available bandwidth, which can affect some wireless networking connections.

Disadvantages:

Wired networks are expensive to maintain the network due to many cables between computer systems and even if a failure in the cables occur then it will be very hard to replace that particular cable as it involved more and more costs.

When using a laptop which is required to be connected to the network, a wired network will limit the logical reason of purchasing a laptop in the first place.

ii. *Wireless Network*

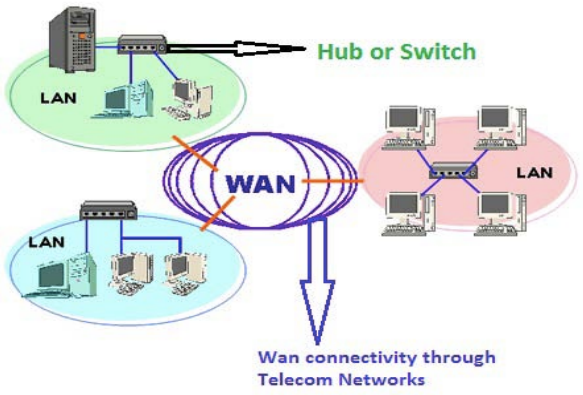


Fig. (b) : Wireless Network

In Wireless networks there is no physical existence of cable between two computers. It use some sort of radio frequencies in air to transmit and receive data instead of using some physical cables. The Wireless network eliminates the disadvantage of wired networks and it also eliminates cable cost.

Advantages:

Mobile users are provided with access to real-time information even when they are away from their home or office. Network can be extended to places which cannot be wired. Wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.

Disadvantages:

Interference due to weather, other radio frequency devices, or obstructions like walls. The total Throughput is affected when multiple connections exists.

In Wireless network there is no guarantee of data to reach at destination.

b) Routing

Routing is the process of selecting paths in a network along which to send network traffic. It is an act of moving information across an inter-network from a source to destination.

Routing is mainly classified into

a) Static Routing b) Dynamic Routing

i. *Static Routing*

Static routing refers to the routing strategy being stated manually or statically, in the router. Static routing maintains a routing table usually written by a networks administrator.

The routing table doesn't depend on the state of the network status, i.e. whether the destination is active or not. Static routing doesn't depend on availability of destination node.

ii. *Dynamic Routing*

Dynamic routing refers to the routing strategy that is being learnt by an interior or exterior routing protocol. This routing mainly depends on the state of the network i.e. the routing table is affected by the activeness of the destination.

c) Mobile Ad-Hoc Network

A wireless mobile ad hoc network [6] is usually defined as a set of wireless mobile nodes dynamically self-organizing a temporary network without any central administration or existing network infrastructure. Since the nodes in wireless ad hoc networks can serve as routers, they are movable so they can form any type of topology. They forward packets for other nodes if they are on the route from source to the destination (like intermediate node. Besides other issues, routing is an important problem in need of a solution that not only works well with a small network, but also sustains scalability as the network gets expanded and the application data gets transmitted in larger volume. Since mobile nodes have limited transmission capacity, they mostly intercommunicate by multi hop relay. Multi hop routing is challenged by limited wireless bandwidth, low device power, dynamically changing network topology, and high vulnerability to failure, to name just a few. To answer those challenges, many routing algorithms in MANETs [6] were proposed. There are different dimensions to categorize them: proactive routing versus on-demand routing, or single-path routing versus multipath routing. In proactive protocols, routes between every two nodes are established in advance even though no transmission is in Demand and in reactive routing routes between every two nodes are established when needed.

Our motivation is that congestion is a cause for packet loss in MANETs [6]; mostly packets will loss cause of congestion only. Our aim is to control congestion in MANETs [6]. Typically, reducing packet loss involves congestion control. Congestion in routing in MANETs [6] may lead to the following problems:

1. *Long delay:* It takes time for a congestion to be detected by the congestion control mechanism. In severe congestion situations, it may be better to use a new route. The problem with an on-demand routing protocol is the delay it takes to search for the new route.
2. *High overhead:* In case a new route is needed, it takes processing and communication effort to discover it. If multipath routing is used, though an alternate route is readily found, it takes effort to maintain multiple paths.
3. *Many Packet Losses:* Many packets may have already been lost by the time congestion is occurred or detected. A typical congestion control solution will try to reduce the traffic load, either by decreasing the sending rate at the sender or dropping packets at the intermediate nodes or doing both. The result is a high packet loss rate or a small throughput at the receiver.

III. Classification of the Routing Protocols in ad Hoc Network

a) Delay Aware

i. FZR (Fresnel Zone Routing)

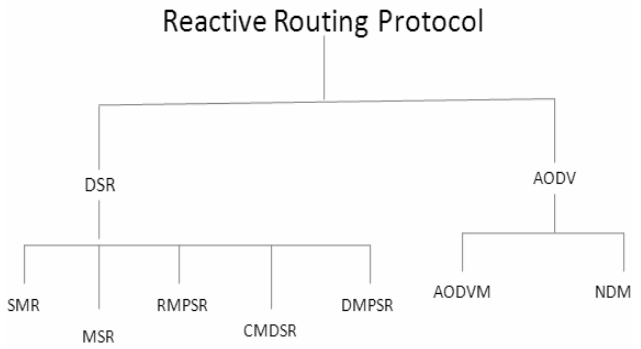


Fig. (c) : Reactive Routing Protocol Taxonomy

ii. AODVM-PSP (Multipath Ad-Hoc on Demand Distance Vector Protocol with Path Selection Probability)

iii. BGR (Biased Geographical Routing Protocol)

b) Reliable

a) Multipath Routing Protocol for Changing Topology
b) End-to-End Estimation Based Fault Tolerant
c) NTBR (Neighbor Table Based Multipath Routing)
d) CHAMP (Caching And Multipath Routing)

c) Minimum Overhead

a) SMR (Split Multipath Routing)
b) MDSR (Multipath Dynamic Source Routing)
c) ADOVM (Multipath AODV)

d) Energy Efficient

a) MDR (Multipath on Demand Routing)
b) EM-GMR (Energy and Mobility Aware Geographical Multipath Routing)

e) Hybrid

a) MSR (Multipath Source Routing)
b) RMPSR (Robust Multipath Source Routing)

f) Congestion

Congestion is a problem that occurs on shared networks, when multiple users access to the same

resources (bandwidth, buffers, and queues). When number of packets are present in a network is greater than capacity of network then this situation is called as congestion. Congestion in a network may occur when the load on the network i.e. the number of packets sent to the network is greater than the capacity of network.

Congestion Control Mechanisms:

i. *End-system flow control:* This is not a congestion control mechanism scheme, but it is a way to prevent the sender in network from overflow the buffers of the receiver.
ii. *Network congestion control:* In this scheme, end systems choke back in order to avoid congesting the network. The mechanism is similar to end-to-end flow controls, but the main intention is to reduce congestion in the network, not the receiver.
iii. *Network-based congestion avoidance:* In this scheme, a router detects that congestion may occur and attempts to slow down senders before queues become full.
iv. *Resource allocation:* This technique involves scheduling the use of physical circuits or other resources, for a specific time period. A virtual circuit, built across a series switches with a guaranteed bandwidth is a form of resource allocation. This technique is difficult, but can eliminate network congestion by blocking traffic that is in excess of the network capacity.

g) Multipath Routing Protocols

Taxonomy of multipath routing protocol based on congestion control

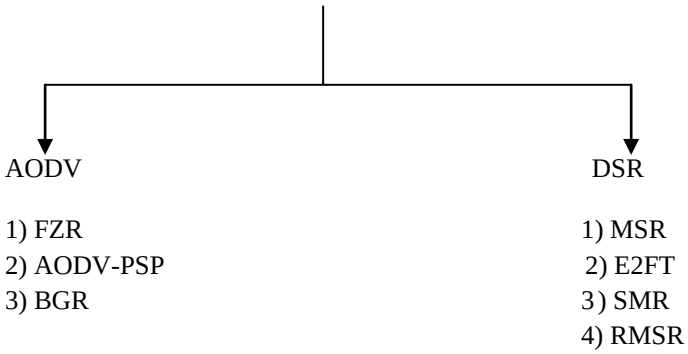


Fig. (d) : Taxonomy of MRP based on congestion control

1) FZR: (Fresnel Zone Routing.)
2) AODV-PSP: (Multipath Ad-Hoc On Demand Distance Vector Protocol With Path Selection Probability)
3) BGR: (Biased Geographical Routing Protocol.)
4) MSR: (Multipath Source Routing)
5) E2FT: (End 2 End Estimation based fault tolerant)
6) SMR: (Split Multipath Routing)
7) RMSR: (Robust Multipath Source Routing)

i. *AODV (Ad hoc On-Demand Distance Vector)*

a. *AODV description*

The AODV protocol [1] is a reactive routing protocol it is also called as a pure on-demand routing protocol because a mobile node does not have to maintain any routing information if it is not located in an active path. Like DSR, the AODV protocol also consists of two main mechanisms a route discovery and a route maintenance mechanism. But the route request packet (RREQ) structure of the AODV protocol is different from that of the DSR protocol. To detect a fresh or new route from an old route, each node maintains two counters such as node sequence ID and broadcast ID. Each route request (RREQ) packet contains information about the destination sequence number which is used for distinguish from remaining node and the source sequence number in addition to source address and destination address. The sequence numbers are used to indicate the freshness and newness of a route in network. Each neighbor node either sends a reply message called as RREP to a source or it rebroadcasts a request message RREQ to its neighbors depending on whether it is the destination or not. If a node is not the destination, it needs to keep track of a request packet to set up a reverse path as well as a forward path. When a destination replies back to a source, it uses the reverse path. Mobile nodes can determine whether a route is a current one or an old one by comparing the destination sequence number in the RREQ packet with that of the sequence number stored in the route cache. If the route request sequence number is greater than the recorded one, it does not send a reply to the source. Instead, it re-broadcasts that request message. An intermediate node only replies from its route cache if the route request sequence number is less than or equal to the sequence number stored in the route cache. If a node does have a current route, it sends a reply using a unicast route reply packet (RREP). The reply packet travels along the reverse path, which was set up previously. When a reply packet travels back through the reverse path, each intermediate node sets up a forward path to the node from which it receives this reply. When a route reply packet reaches the source, the source starts sending data packets to the destination using the discovered path. If that source learns more routes later on, it updates its route cache accordingly.

b. *AODV Properties*

- Floods RREQs with unique IDs so duplicates can be discarded.
- Each node maintains backup route(s) in alternative route table.
- Distance-vector protocol so only destination, next hop and number of hops known.
- Alternative route (backup) route(s) or other routes which are discovered while route discovery used when primary fails.

- No multiple complete routes available.
- Alternative route(s) determined in RREP phase.
- Alternative route(s) by overhearing RREPs to other nodes.
- No complete route(s) information known at source.

ii. *Fresnel zone routing (FZR)*

FZR is a multipath routing protocol which supports congestion control. It classifies intermediate nodes according to their capacity and efficiency in forwarding packets. FZR protocol is a combination of both proactive and reactive routing protocols. FZR [10] can lighten congestion at an intermediate node and achieve better transport layer throughput. In FZR path hop count which is nothing but the shorter distance traveled by the packet so the hop count is used for zone construction. In FZR [10], each node maintains a distance table; the table consists of the fields: destination address, sequence number and hop distance. To construct and maintain these tables, a mobile node broadcasts Hello messages. Upon receiving a Hello message, a node updates its own table. When a distance table is propagated throughout the network, each node updates its distance table and the first order paths are discovered. FZR [10] discovers alternate second order path with an on-demand approach. A source node or an intermediate node located in the first zone initiates the route discovery process. When a neighbor located in the second zone receives a request packet, it sends a reply message to the originating node via the upstream neighbors. The upstream nodes then record the forward path in the table and forward the reply messages to the originator. Upon receiving a reply massage, the originator records the path in the forward path table and this procedure repeats itself until message packet received at destination. Then data is transferred on this path.

iii. *Ad hoc On-demand Multipath Distance Vector routing (AOMDV)*

a. *AOMDV description*

The AOMDV uses the basic AODV route construction process. In this case, some extensions are made to create multiple link-disjoint paths. The main idea in AOMDV is to compute multiple paths during route discovery. It consists of two components:

- A route update rule to establish and maintain multiple loop-free paths at each node.
- A distributed protocol to find link-disjoint paths.

Before describing AOMDV [8], we first discuss AODV, from which it is derived. In AODV, when a source needs a route to a destination, it initiates a route discovery process by flooding a RREQ for destination throughout the network. RREQs should be uniquely identified by a sequence number so that duplicates can be recognized and discarded. Upon receiving a non-duplicate RREQ, an intermediate node records previous hop and checks whether there is a valid and fresh route entry to the destination in routing table. If such entry is found, the node sends back a RREP to the source; if not it rebroadcasts the RREQ message. A node updates its routing information and propagates the RREP upon receiving further RREPs only if a RREP contains either a larger destination sequence number or a shorter route found.

In AOMDV [8] each RREQ, respectively RREP arriving at a node defines an alternate path to the source or destination. Just accepting all such copies will lead to the formation of routing loops. In order to eliminate any possibility of loops, the "advertised hop count" is introduced. The *advertised hopcount* of a node *i* for a destination node *d* represents the maximum hopcount of the multiple paths for node *d* available at *i*. The protocol only accepts alternate routes with hopcount lower than the advertised hop count, alternate routes with higher or the same hopcount are discarded. The advertised hop count mechanism establishes multiple loop-free paths at every node. These paths still need to be disjoint. For this we use the following:

When a node *S* floods a RREQ packet in the network, each RREQ arriving at node *I* via a different neighbor of *S,* or *S* itself, defines a node-disjoint path from *I* to *S*.

In AOMDV this is used at the intermediate nodes. Duplicate copies of a RREQ are not immediately discarded. Each packet is examined to see if it provides a node-disjoint path to the source. For node-disjoint paths all RREQs need to arrive via different neighbors of the source. This is verified with the *first hop* field in the RREQ packet and the *firsthop_list* for the RREQ packets at the node.

At the destination a slightly different approach is used, the paths determined there are link-disjoint, not node-disjoint. In order to do this, the destination replies up to k copies of the RREQ, regardless of the firsthops. The RREQs only need to arrive via unique neighbors.

AOMDV properties

- Extension of AODV.
- RREQs from different neighbors of the source are accepted at intermediate nodes.
- Multiple link-disjoint routes are created (with modification at the destination they can be node-disjoint).
- Maximum hop count to each destination ("advertised hop count") is used to avoid loops.
- Multiple routes are established in single route discovery process.
- Nodes maintain next-hop info for destinations (multiple next-hops possible).

iv. *Multipath AODV with Path Selection Probability (AODV-PSP)*

a. *AODV-PSP description*

The AODVM-PSP protocol is an extension of AODVM protocol discussed earlier. The route discovery mechanism of AODVM-PSP [11] is similar to that of the AODV protocol. The multiple paths are set up in a similar manner as that of the AODVM protocol.

The main difference between AODVM-PSP and AODVM [11] is that AODV-PSP considers delays along a path while making a routing decision. When a node sends a packet to a destination, the packet includes information as to what time (concept of timestamp) it was transmitted. An intermediate node or a destination node can estimate the delay based on the information included in the packet. The AODVM-PSP does not especially find link- disjointed paths unlike the AODVM [11] protocol. The AODVM-PSP [11] does not use keep alive packet like the AODVM protocol to avoid the congestion. The RSR protocol is based on a disparity routing scheme. In a disparity routing scheme, a message is partitioned or divided in small parts and sent over different paths. The idea is that if a path fails, there is still a chance for other paths to send a packet successfully to a destination. Disparity routing can be broadly classified into two types:

Non-redundant and redundant. In non-redundant disparity routing, a message is divided into sub-messages and these sub-messages are routed through different paths. In redundant disparity routing, a message is also divided into sub-messages, but the number of sub-messages is less than the number of discovered paths that the routing protocol uses. The traffic dispersion on different paths is done in a round-robin fashion where each path has a constant weight of one packet. If no other alternate path is available, RSR performs similarly as DSR. In the destination node, RSR has an agent named duplicate packet filter (DPF) at the destination r. The function of DPF is to filter out the duplicate packets. Moreover, when there is no intermediate node between a source and a destination, PDA does not duplicate a message. PDA also does not duplicate a packet if there is only one route available between a source and a destination.

v. *Biased geographical routing (BGR) protocol*

The BGR [11] protocol improves the delay performance of a network by using the congestion in formation of a network. The main idea behind the BGR protocol is to insert a bias angle in each packet. This bias angle determines the route of a path towards a destination. The BGR protocol uses two congestion control algorithms, namely in-network packet splitter (IPS) and end-to-end packet scatter (EPS). The IPS splits traffic flows to avoid congestion. Congestion arises when too many connections are set up through a certain section of a network (i.e. hot-spot). In order to avoid a hot-spot, the IPS splits the traffic flow just before the hot-spot. The IPS requires periodic information (congestion information) exchanges among neighbors. If IPS fails to reduce congestion, the EPS algorithm is activated. In the case of EPS algorithm, a source splits traffic flows among multiple paths, therefore, reduces congestion.

IV. Conclusion

Multipath routing can improve network performance in terms of delay, throughput and reliability. Multi path routing protocols also improve load distribution, reliability, delay and energy efficiency. AODVM-PSP (Ad hoc on demand distance vector routing with path selection probability) considers delays along the path while making routing decision. The ability to forward traffic on multiple paths would be useful for customizing paths for different applications, improving reliability, and balancing load. Due to scalability and economic.

References Références Referencias

1. H.Lei, C.E. Perkins, 'Ad Hoc Networking with Mobile IP," Proceedings ofthe (EMC '9), Bonn, September. 1997
2. U.Jonsson, et al, G'MIPMANET-Mobile IP for Mobile Ad Hoc Networks," IEE4EAC annual Workshop on Moblle Ad Hoc Aetworking and Compiuting (MobiHOC '02), Boston, Mossachusetts, USA, August 2000/
3. Kwan-Wu Chin, John Judge, AidenVWilliams and Roger Kermenode, "Implementation Experience with MANET Rouitng Protocols", AM SIGCOMM communication review, \ olume 32, Issue 5, November 2002.
4. David B. Johnson, David A. Maltz, Josh Broch. "Dynamic Source Routing for Multihop wireless ad hoc networks", In Ad Hoc Networking, edited by Charles E. Perkins, chapter 5, pp 139-172. Addison-Wesley, 2001.
5. C.E Perkins and P.Hhagwat, "Highly Dynamic Destination Sequence Vector Rouiting (DSDV) for mobile computers". Cnomputer Communication. 1994, pp.234-244.
6. S. Corson and J. Macker, "*Mobile Ad hoc Networking(MANET): Routing Protocol Performance Issues and Evaluation Considerations*", IETF WG Charter, http://www. ietf. org/html.charters/manet-charter.html, January 1999.
7. S. Lee and M. Gerla, "*AODV-BR: Backup routing in ad hoc networks*." Proceedings of IEEE WCNC 2000, Chicago, pages 1311-1316, September 2000.
8. M. Marina and S. Das, "*On-demand Multipath Distance Vector Routing in Ad Hoc Networks*", in Proceedings of the International Conference for Network Procotols (ICNP), Riverside, Nov. 2001.

9. S. Das, C. Perkins and E. Royer, "*Ad Hoc on Demand Distance Vector (AODV) Routing*", IETF RFC3561, July 2003.
10. Multipath "Fresnel Zone" Routing For wireless ad hoc networks by Yibin Liang
11. "Survey of multipath routing protocols for mobile adhoc networks" by Mohammed Tarique a KemalE.Tepe b, SasanAdibi c, ShervinErfani b.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Node Disjoint Multipath Routing Approach for Controlling Congestion in Manets

By Mr. Abhishek Bande & Mr. Gaurav Deshmukh

University of Pune, Maharashtra India

Abstract - Mobile Ad hoc Networks are highly dynamic networks. Quality of Service (QoS) routing in such networks is usually limited by the network breakage due to either node mobility or energy depletion of the mobile nodes. Node-disjoint routing becomes inessential technique in communication of packets among various nodes in networks. Meanwhile AODV (Ad Hoc On-demand Multipath Distance Vector) creates single-path route between a pair of source and destination nodes. Some researches has done so far to make multipath node-disjoint routing based on AODV protocol. But however their overhead and end-to-end delay are relatively high, while the detail of their code is not available too. In an ad hoc network, identification of all node-disjoint paths between a given pair of nodes is a challenging task. The phenomena that a protocol is not able to identify all node-disjoint paths that exist between a given pair of nodes is called path diminution. In this paper, we discuss that path diminution is unavoidable when a protocol discovers multiple node-disjoint paths in a single route discovery and working of node disjoint multipath protocol.

Keywords : *routing; ad hoc networks; path diminution; node-disjoint multipath routing; single route discovery, node disjoint routing.*

GJCST-E Classification : *C.2.2*

Strictly as per the compliance and regulations of:

Node Disjoint Multipath Routing Approach for Controlling Congestion in Manets

Mr. Abhishek Bande [α] & Mr. Gaurav Deshmukh [σ]

Abstract - Mobile Ad hoc Networks are highly dynamic networks. Quality of Service (QoS) routing in such networks is usually limited by the network breakage due to either node mobility or energy depletion of the mobile nodes. Node-disjoint routing becomes inessential technique in communication of packets among various nodes in networks. Meanwhile AODV (Ad Hoc On-demand Multipath Distance Vector) creates single-path route between a pair of source and destination nodes. Some researches has done so far to make multipath node-disjoint routing based on AODV protocol. But however their overhead and end-to-end delay are relatively high, while the detail of their code is not available too. In an ad hoc network, identification of all node-disjoint paths between a given pair of nodes is a challenging task. The phenomena that a protocol is not able to identify all node-disjoint paths that exist between a given pair of nodes is called path diminution. In this paper, we discuss that path diminution is unavoidable when a protocol discovers multiple node-disjoint paths in a single route discovery and working of node disjoint multipath protocol.

Keywords : routing; ad hoc networks; path diminution; node-disjoint multipath routing; single route discovery, node disjoint routing.

I. Introduction

Mobile ad hoc network is a type of wireless that is composed of wireless mobile nodes. Each mobile node dynamically changes the network topology without relying on a wired backbone network or a fixed base station. Mobile nodes in MANETs are constrained by their limited power, processing, memory resources and high degree of mobility. In such networks, the wireless mobile nodes may dynamically join or leave the network topology. In MANETs, many routing protocols have been suggested to communicate between mobile nodes. And pertinent routing protocols are used in various network environment and application.

Multipath routing protocols search node-disjoint, link disjoint or non-disjoint routes during the rout discovery Process. Node-disjoint routes have completely disjoint routes where there are no nodes or links in common. Link-disjoint routes have no links in common but may have nodes in common. Non-disjoint routes may use nodes or links in common. Following are the figures which explains the what are the node disjoint paths and link disjoint paths.

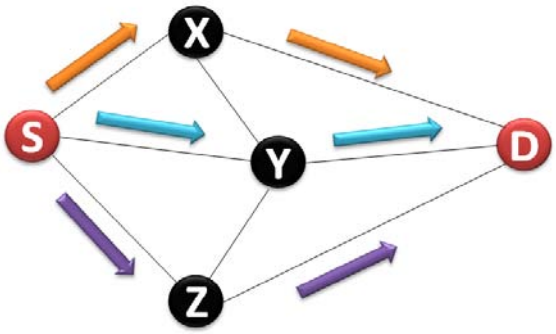


Fig (a) : Node Disjoint

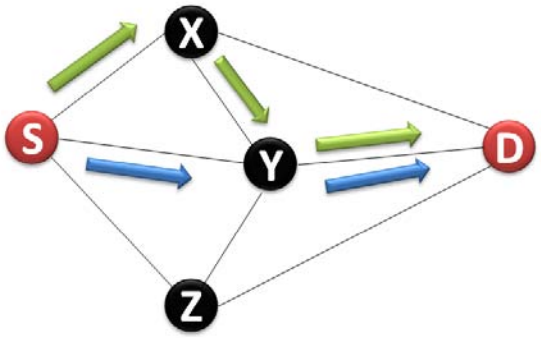


Fig (b) : Link Disjoint

If a node or link fails (and it is used by the main and backup route) in non-disjoint and link-disjoint routes, then main and backup routes will be disconnected at the same time. However in node-disjoint routes, main routes and backup routes use completely different nodes or links. Therefore, even though main route will be disconnected, data transmission may be available through the backup route.

In single-path routing protocols, route maintenance may be Performed after route fail. Therefore, data transmission will be stopped while the new route is established, causing data transmission delay. On the other hand, multipath routing protocols perform the route maintenance process even if only one route fails among the multiple routes. To perform the route maintenance process before all routes fail, the network must always maintain multiple routes. This can reduce data transmission delays caused by link failure.

Other than the source and the destination, node-disjoint paths have no node in common, while link-

Author α σ : Department of Computer Engineering, University of Pune, Maharashtra India. E-mails : abhishek.bande2008@gmail.com, deshmukhgaurav9@gmail.com

disjoint paths do not share any link. Clearly, node-disjoint paths are also link-disjoint paths. Node-disjoint paths are desirable where node resources are Scarce or when nodes are susceptible to failure. On the other hand, link-disjoint paths are preferred where link resources are scarce or when only links are susceptible to failure. Using link-disjoint paths, one can address the issue of fault-tolerance. However, link-disjoint paths cannot be used for simultaneous data transfer because doing so will overload the nodes that are common in more than one path. Using node-disjoint paths, one can address fault-tolerance as well as load sharing.

II. Related Work

Multipath routing establishes multiple routes between source and destination nodes. For fault tolerance, even if one route failure occurs, source nodes can maintain connections by using other routes. So multiple routing protocols can reduce data transmission failures and delay times that are caused by route disconnection. Multipath routing protocols search node-disjoint, link disjoint or non-disjoint routes during the route discovery process. Node-disjoint routes have completely disjoint routes where there are no nodes or links in common. Link-disjoint routes have no links in common but may have nodes in common. Non-disjoint routes may use nodes or links in common. If a node or link fails (and it is used by the main and backup route) in non-disjoint and link-disjoint routes, then main and backup routes will be disconnected at the same time. However in node-disjoint routes, main routes and backup routes use completely different nodes or links. Therefore, even though main route will be disconnected, data transmission may be available through the backup route. In single-path routing protocols, route maintenance may be performed after route fail. Therefore, data transmission will be stopped while the new route is established, causing data transmission delay. On the other hand, multipath routing protocols perform the route maintenance process even if only one route fails among the multiple routes. To perform the route maintenance process before all routes fail, the network must always maintain multiple routes. This can reduce data transmission delays caused by link failure.

Several implementation of multipath routing are based on AODV; typical examples are AOMDV, AODVM, AODV-BR and MP-AODV protocols. The AOMDV [2] protocol establishes loop-free link-disjoint paths in the network. When intermediate nodes receive the RREQ packet from the source node, AOMDV stores all RREQ packets, unlike conventional AODV, which discards duplicates. So, each node maintains a firsthop-list where information from additional field called firsthop in RREQ packet to indicate the neighbor node of the source nodes. If firsthop of received RREQ packet is duplicated from its own firsthop-list, the RREQ packet is discarded. On the other hand, the RREQ packet is not duplicated from previous RREQ packets. Then the node updates the nexthop, hopcount and advertised-hopcount in routing table. At the destination, RREP packets are sent from each received RREQ packet. The multiple routes are made by RREP packets that are follow the reverse routes that have been setup already in intermediate nodes [6].

For the AODVM protocol, intermediate nodes are not allowed to send a RREP packet directly to the source node. Also, intermediate nodes do not discard the duplicate RREQ packets. But the intermediate nodes record all received RREQ packets in routing table. The destination node sends an RREP for all the received RREQ packets. An intermediate node forwards a received RREP packet to the neighbor in the routing table. Whenever a node overhears one of its neighbors broadcasting RREP packet and it removes that neighbor from its routing table, because nodes cannot participate in more than one route.

For the AODV-BR protocol, neighbor nodes overhear the RREP packets for establishing and maintaining the backup routes during the route initiation process. If part of the main route is broken, nodes broadcast error packets to neighbor nodes. When neighbor nodes receive the error packet, they establish an alternate route using information about the overheard RREP packets previously. AOMDV has the overhead of storing multiple next hops and hop counts and the first hop list for each destination. By overhearing the neighbor's packets, AODVM may not establish alternate routes depending on the path along which the RREP packets are sent. Moreover, to speak strictly, AODV-BR is not a multipath routing protocol, because it only maintains bypass routes when the main route is broken by using the neighbor nodes around the main routes. MP-AODV protocol uses the modified RREQ and RREP packet that has additional 1bit flag 'F'. This flag distinguishes the packet into the main route (RREQ, RREP) or backup route (RREQ_2, RREP_2) route discovery processes. Unlike a conventional AODV, intermediate nodes that receive the RREP packet increment the RREQ ID value in the seen table. By incrementing the RREQ ID value, the protocol ensures that a backup route will not use any nodes that belong to the main route. When a source node receives the RREP packet, the main route is established, and the source node starts data transmission and broadcasts the RREQ_2 packet (a packet with a RREQ ID value of two) for simultaneously searching a backup route. RREQ_2 is a packet for establishing a backup route, and its flag bit F is set to one. When the RREQ_2 packets are delivered to the intermediate nodes, the RREQ ID values in the seen table are compared with the RREQ ID values in the RREQ_2 packets. If they are identical, the nodes discard the RREQ_2 packet. If not, the nodes forward the RREQ_2 packet continuously.

When nodes belonging to the main route receive the RREP packet, the RREQ ID value in the RREQ_2 packet and the RREQ ID value in the seen table are identical because the protocol has already increased the RREQ ID value in the seen table during the previous route discovery process. After this process, the intermediate nodes belonging to the main route do not join in the backup routes.

MP-AODV has high control overhead and end-to-end delay, because it uses at last five control packets to establish two node-disjoint route.

III. Multipath Routing Protocol

We call the proposed protocol Vertex Disjoint Multipath Routing (VDMR). Like other on-demand protocols, VDMR is also based on the request–reply paradigm. We describe the protocol in two phases: *route discovery* and *route maintenance*.

a) Route discovery

If a source node, *S*, wishes to communicate with a destination node, *D*, and it does not have a route to the destination, it initiates a route discovery. To initiate a route discovery, node S broadcasts a route request (RREQ). The transmitted RREQ is heard by all nodes which are in the transmission range of the source. The RREQ carries the following information in its header: *Source Address, Destination Address, Source Seq No, Path Traversed*. A node that is neither the source nor the destination of an RREQ is called an intermediate node. The processing of an RREQ at a node will differ depending upon whether the node is the source/destination of the RREQ, or an intermediate node. An intermediate node maintains an *RREQ Cache* where it stores information about the RREQs forwarded earlier. Note that two or more RREQs are said to copies of one another if they have the same *Source Address, Destination Address, Source Seq No*.

If node *i* has already forwarded a copy of the RREQ or if the address of node itself is present on the *Path Traversed* of the RREQ, then it discards the RREQ. When an RREQ reaches node *D*, it stores the RREQ in *RREQ Cache*. Node *D* collects all copies of an RREQ received and saved in *RREQ Cache* before the expiry of a timeout. Upon expiry of the timeout, destination *D* reads all RREQs cached in its *RREQ Cache* and computes there from a maximal set of node-disjoint paths (using the heuristics described in Appendix B) by inspecting the *Path Traversed* in each of the RREQs. Node *D* then sends multiple route replies3 (RREP), one for each node-disjoint path. It also stores the RREPs in its *RREP Cache*. An RREP contains the following information in its header: *Source Address, Destination Address, Source Seq No, Reverse Path*, where, *Reverse Path* of the RREP is *Path Traversed* of the RREQ in reverse direction. Note that the multiple RREPs differ in *Reverse Path*. Upon receiving an RREP, an intermediate node updates its routing table and unicasts the RREP to the next node along the path. When node *S* receives an RREP, it stores the path to node *D* in its *Route Cache*.

b) Route maintenance

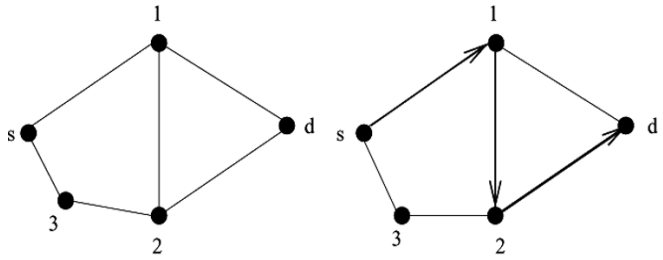
If a link failure occurs while transmitting data packets, then a node sensing link failure generates a route error (RERR) message. An RERR contains the route to node *S*. The RERR message informs upstream nodes about the link failure. All the nodes update their routing tables by deleting the entry of the path along which a link failure occurred. When an RERR reaches node *S*, it also updates its routing table by deleting the entry of the path that has failed. Then, it looks up its routing table for a path. If it finds a path, it starts sending data packets along the path. Otherwise node *S* initiates a new route discovery. In what follows, we discuss that a protocol may or may not be able to discover all node-disjoint paths that exist in the network between a given pair of nodes.

c) Path diminution

By 'path diminution'4 we mean that the number of node-disjoint paths discovered by a protocol is less than the number of node-disjoint paths that exist in the network between a given pair of nodes. There are two reasons of path diminution: RREQ forwarding policy and computation of disjointness at the destination. We are, here, concerned with the occurrence of path diminution due to an RREQ forwarding policy A policy which is generally adopted in single path routing protocols such as Dynamic Source Routing (DSR) (Johnson and Maltz, 1996) and Ad hoc On-demand Distance Vector Routing (AODV) (Perkins and Royer, 1999) is that only the first copy of an RREQ is forwarded at an intermediate node, while other copies are discarded. This policy works well for finding *a* path from a given source to a destination. However, if one wishes to use it in a protocol to discover multiple node-disjoint paths, the protocol may or may not be able to discover all node-disjoint paths that exist between a given pair of nodes.

d) Example

Consider a network shown in Figure (c). There are two node-disjoint paths between *s* and *d*. If node 2 receives a copy of an RREQ from node 3 before it receives a copy from node 1, then it broadcasts this copy of the RREQ to its neighbors. The destination receives two copies of the RREQ with *Traversed Path* <3, 2> and <1>. When the destination computes disjointness, it finds two node-disjoint paths.



(a) (b)

Fig (c) : A network with 2 node-disjoint paths from *s* to *d*

However, if node 2 receives a copy of an RREQ from node 1 before it receives a copy from node 3, node 2 broadcasts the copy of the RREQ to its neighbors. It discards the copy of RREQ received from node 3. Two copies of the RREQ with *Traversed Path* <1, 2> and <1> reach the destination. When the destination computes the disjointness, it finds only one path. Although, there exist two node-disjoint paths between *s* and *d*, the protocol is not able to find them.

e) An expensive solution

One method for mitigating path diminution can be described as follows. An intermediate node discards only those copies of an RREQ that cause loops. The node forwards all other copies of an RREQ after appending its own address to the *Path Traversed* of the copy of the RREQ. The destination collects all copies of the RREQ before computing disjointness. Assuming that an algorithm for computing the maximum set of node-disjoint paths is available, one will be able to discover all node-disjoint paths. The number of RREQs that an intermediate node has to transmit can be as large as $(n - 3)!$ 5 Further, the number of copies of an RREQ that may reach the destination can be as large as $(n - 2)!$ 6 As a result, this scheme requires an exponential amount of computational and communication overheads. Clearly, this solution is not acceptable in an ad hoc network where resources of nodes are limited.

f) Mitigating path diminution

We propose three schemes to mitigate path diminution. In a fundamental sense, these schemes play upon the number of RREQs that each intermediate node forwards and the manner in which it selects the RREQs that are forwarded. However, the features that are common among all proposed schemes are as follows.

- To prevent loops, an intermediate node checks whether its own address is already present in *Path Traversed* of the RREQ. If that is so, it discards the RREQ. Otherwise, it forwards the RREQ according to a stated policy.
- Before forwarding a copy of an RREQ, an intermediate node appends its own address to *Path Traversed* of the RREQ.
- To keep a record of the RREQs forwarded, a node maintains a *RREQ Cache*. Before forwarding a copy of the RREQ, a node stores the RREQ in its *RREQ Cache*.

We now discuss the features of the proposed schemes that are different.

i. *Path diminution in node-disjoint multipath routing*

1. *All Disjoint Copies (ADC).* An intermediate node forwards all node-disjoint copies of an RREQ and discards the copies which are not node-disjoint. Upon receiving a copy of an RREQ, an intermediate node checks whether *Path Traversed* of the copy of the RREQ is disjoint with those already forwarded. If that is so, it forwards the copy of the RREQ. Otherwise, it discards the copy of the RREQ.
2. *Two Disjoint Copies (2DC).* An intermediate node forwards the first copy of an RREQ. It also forwards another copy of the RREQ, if any, provided its *Path Traversed* is node-disjoint with that already forwarded. Other copies of the RREQ are discarded. To keep a record of *number of copies* forwarded with disjoint *Path Traversed*, an intermediate node maintains a counter *rreq Count*. The variable *rreq Count* is initially set to 0 and is incremented each time when the node forwards a copy of the RREQ. If *rreq Count* reaches 2, the node discards subsequent RREQs (if any).
3. *At most one Copy per Neighbour (OCN).* An intermediate node forwards at most one copy from each neighbour. It discards the duplicate copy from a neighbour. Upon receiving a copy of an RREQ, an intermediate node checks the previous hopID in *Path Traversed* of the RREQ. An intermediate node forwards the copy of the RREQ if and only if the previous hopID does not match with the previous hopID of any of the copy of the RREQ stored in its *RREQ Cache*. Let us return to the example shown in Figure 1(a). Suppose each intermediate node forwards 2 disjoint copies of an RREQ. Node *D* will receive 3 copies of the RREQ with *Path Traversed* <1>, <1, 2> and <3, 2>, respectively.7 Upon computing disjointness, the destination identifies two node-disjoint paths with *Path Traversed* <1> and <3, 2>. The destination sends two RREPs one along each node disjoint paths. In other words, if 2DC is used as RREQ forwarding policy, the protocol will be able to find both node-disjoint paths in the example network. There is no guarantee that any of these schemes will always discover all node-disjoint paths between a given pair of nodes. However, these schemes are adopted to introduce a diversity in the *Path Traversed* of the copies of an RREQ that reach the destination. In other words, adoption of the policies discussed above can enhance the chances of forwarding those copies of

an RREQ which have the potential of obtaining disjoint *PathTraversed* at the destination node.

ii. *Node Disjoint Multipath Routing Considering Link and Node Stability*

The main aim of the proposed work is to find the multiple node disjoint routes from source to a given destination Also it keeps track of the route bandwidth which can be further used by the source to select the optimal routes. From the factors Link Expiration Time (LET) [19] and Drain Rate (DR) [22] it is inferred that the Link Stability:

a) Depends directly on Mobility factor
b) Depends inversely on the energy factor

Hence, Link Stability Degree (LSD) is defined as:

$$LSD = \text{Mobility factor} / \text{Energy factor} \quad (3)$$

It defines the degree of the stability of the link. Higher the value of LSD, higher is the stability of the link and greater is the duration of its existence. Thus, a route having all the links with LSD > LSDthr is the feasible. We choose the Dynamic Source Routing (DSR) [5] protocol as a candidate protocol. Modifications are made to the Route Request (RREQ) and Route Reply (RREP) packets to enable the discovery of link stable node disjoint paths. The proposed scheme has three phases: Route Discovery, Route Selection and Route Maintenance. The various phases are described as follows:

a. *Route Discovery*

The source node when needs to send packet to some destination node, starts the route discovery procedure by sending the Route Request packet to all its neighbors .In this strategy , the source is not allowed to maintain route cache for a long time, as network conditions change very frequently in terms of position and energy levels of the nodes. Thus, when a node needs route to the destination, it initiates a Route Request packet, which is broadcasted to all the neighbors which satisfy the broadcasting condition. Route Request packet of NDMLNR is shown in figure.

SA	DA	Type	ID	TTL	Hops	Bandwidth	LSD	Path	Velocity	Direction	Position

Fig. (d) : RREQ packet

Type (T) field: It indicates the type of packet.

SA (Source Address) field: It carries the source address of node.

ID field: unique identification number generated by source to identify the packet.

DA (Destination Address) field: It carries the destination address of node.

Time to Live (TTL) field: It is used to limit the life time of packet, initially, by default it contains zero.

Hop field: It carries the hop count; the value of hop count is incremented by one for each node through which packet passes. Initially, by default this field contains zero value.

LSD field: when packet passes through a node, its LSD value with the node from which it has received this packet is updated in the LSD field. Initially, by default this field contains zero value.

Bandwidth field: carries the cumulative bandwidth of the links through which it passes; initially, by default this field contains zero value.

Path field: It carries the path accumulations, when packet passes through a node; its address is appended at end of this field.

The node's current velocity, direction and position are updated at each node in the respective fields before forwarding the RREQ packet.

Every node maintains a Neighbor Information Table (NIT), to keep track of multiple RREQs. With following entries Source Address, Destination Address, Hops, LSD, ID and bandwidth.

SA	DA	ID	Hops	LSD	Bandwidth

Fig (e) : Neighbor Information Table (NIT)

As RREQ reaches a node it enters its information in the NIT. It makes all the entries for the requests till Wait Period. At the end of the Wait Period, it accepts the request with the highest value in LSD field. It adds the value of the link bandwidth to the Bandwidth field of the RREQ packet. If two RREQs have same LSD values, the one with lesser value of hop count is selected. In case, hops are also same, one with higher bandwidth is selected. In the worst case, RREQ is selected on First-come-first -serve basis. This prevents loops and unnecessary flooding of RREQ packets. None of the intermediate nodes is allowed to send RREP if it has the current route to the destination. As doing this may lead to those paths which do not fulfill current QoS requirements.

b. *Route Maintenance*

In case, LSD of a node falls below LSDthr, it informs its predecessor node of the node failure by sending the NODEOFF message. Once a node receives such a message, it sends the ROUTEDISABLE message to the source node. Source can then reroute the packets to the backup routes. If no backup route exists, the source then starts the route discovery procedure again.

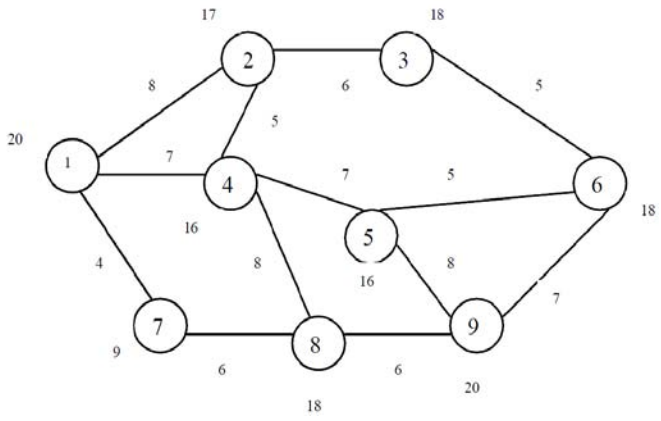


Fig (f) : An example network

Let us illustrate our technique with the following example network shown in figure (e). Suppose node 1 is the source node and node 6 is the destination. Let LSD equals to 15. Let B equals to 5 mbps. To send the packet, node 1 checks its neighbors (2.4.7) for their LSD value Out of these node 7 has value 9<15. So, node 1 sends the packets only to nodes 2 and 4. Node 2 receives this packet for the first time, makes entry in its NIT for the RREQ packet as (1, 6, 1, 1, 20, and 8) and starts Wait Time, 5 secs here. Node 2 now checks its neighbors, updates the path field as, 1-2 and the bandwidth field to 8 and forwards RREQ to both 4 and 3. At node 4, it may receive two RREQ packets during Wait Time. One from node 1 directly and the other via node 2. It has two entries in its NIT (1,6,1,1.20,8) and (1,6,1,2,17,13). At this moment it selects the one from node 1 with higher LSD value, 20. It updates the path field of the RREQ packet as 1-4 and the bandwidth field to 7. It forwards the packet to both its neighbors, 5 and 8, with LSD values 16 and 18 respectively. Node 3 has only one neighbor, 6 which satisfies the LSD value and hence, it updates RREQ path field as 1-2-3 and the bandwidth field to 14 and forwards the packet to node 6. Node 6 now receives a path from source node 1. It appends its own ID to it. Thus, first path is 1-2-3-6 and bandwidth of this path is 17. Node 5 after receiving the RREQ packet with path 1-4, checks for its neighbors and forwards RREQ with updated path field to 1-4-5 and bandwidth field to14 to nodes 9 and 6 Node 6 now receives another path,1-4-5.It appends its ID to it, to get the path, 1-4-5-6 with bandwidth 19. Node 8 after receiving the RREQ packet forwards it to its neighbor, 9, after updating path field to 1-4-8 and bandwidth field to 15 Node 9 can receive two packets in its wait time, one from node 5 and the other from node 8. It updates its NIT as (1,6,1,3,16,22) and (1,6,1,3,18,21). To select from the one, it chooses one from node 8 as its LSD value is higher, 18. It then forwards the request after updating the path field as 1-4-8-9 and bandwidth field to 21. Node 6 again receives another path 1-4-8-9.It appends its ID to this path to get 1-4-8-9-6 with bandwidth 28.Now node 6 receives two paths 1-4-5-6 and 1-4-8-9-6 with node 4 as common node. It selects the one with higher bandwidth i.e. Path, 1-4-8-9-6 with bandwidth 28.

IV. Conclusion

In this paper, we proposed a routing protocol that establishes two node-disjoint routes between source and destination nodes based on AODV protocol for MANETs. NMN-AODV uses three control packets for establishes two routes, but MP-AODV uses five control packets. Thus NMNAODV has law overhead to MP-AODV. In addition, two routes will not break at the same time because the protocol uses node-disjoint multiple routes that are not duplicated between main and backup routes. NMN-AODV establishes two node-disjoint faster than MP-AODV because NMNAODV starts to establish backup route faster than MP-AODV. Thus nd-to-end delay is lawyer than MP-AODV. Also this protocol sends the data immediately after the main route is found by separating the main route and backup route discovery process to reduce the data transmission delay. In the future work, we will compare NMN-AODV with other multipath routing protocols based on AODV such as AOMDV, AODVM and AODV-BR.

References Références Referencias

1. W. Cheng, A. Y. Teymorian, L. Ma, X. Cheng, X. Lu, and Z. Lu. Underwater localization in sparse 3d acoustic sensor networks. In *IEEE INFOCOM*, 2008.
2. D. Goldenberg, A. Krishnamurthy, W. Maness, Y. R. Yang, A. Young, A. S. Morse, A. Savvides, and B. Anderson. Network localization in partially localizable networks. In *IEEE INFOCOM*, 2005.
3. D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, pages 153–181, 1996.
4. S.-J. Lee and M. Gerla. Split multipath routing with maximally disjoint paths in ad hoc networks. In *ICC*, 2001.
5. S. Li and Z. Wu. Node-disjoint parallel multipath routing in wireless sensor networks. In *ICESS*, 2005.
6. C. E. Perkins and E. M. Royer, "Ad hoc On-Demand Distance Vector Routing (AODV) ", IETF RFC 3561, 2003.
7. Z. Hass and R. Pearlmann, "Zone routing Protocol", IETF Internet Draft, 1999.
8. RFC2386.
9. S.Chen and K.Nahrstedt, "An Overview of Quality-of-Service Routing for the next Generation High -Speed Networks: Problems and Solutions", IEEE Network Magazine, vol12, 1998, pp. 64 -79.
10. M. K. Marina and S. R. Das, "On-Demand MultiPath Distance Vector Routing in Ad hoc Networks", Proceedings of the Ninth International Conference on Network Protocols (ICNP}, IEEE Computer Society Press, 2001, pp. 14-23.

11. X. Hong, K. Xu, M. Gerla, "Scalable Routing Protocols for Mobile Ad Hoc Networks," IEEE Network, Vol. 16, No. 4, pp. 11-21, 2002.
12. L. Blazevic, S. Giordano, and J. Le Boudec, "Self Organized Terminode Routing," Cluster Computing, Springer Science Business Media, pp. 205-218, 2002.
13. Y. Ge, G. Wang, Q. Zhang, and M. Guo, "Multipath Routing with Reliable Nodes in Large-Scale Mobile Ad-Hoc Networks," IEICE Transactions on Information and Systems, Vol. E92-D, No. 9, pp. 1675-1682, Sept. 2009.
14. M.T.Toussaint, "Multipath Routing in Mobile Ad Hoc Networks", *TUDelft/ TNO Traineeship Report*.
15. Chang-Woo Ahn, Sang-Hwa Chung, Tae-Hun Kim, Su- Young Kang, "A Node-Disjoint Multipath Routing Protocol Based on AODV in Mobile Ad-hoc Networks", International Conference on Information Technology, IEEE, 2010.

This page is intentionally left blank

Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 17 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cloud-Based Mobile Video Streaming Techniques

By Saurabh Goel

Abstract - Reasoning processing is changing the landscape of the electronic digital multi-media market by moving the end customers concentrate from possession of video to buying entry to them in the form of on-demand delivery solutions. At the same time, the cloud is also being used to store possessed video paths and create solutions that help audience to discover a whole new range of multi-media. Cellular devices are a key car owner of this change, due to their natural mobility and exclusively high transmission rate among end customers. This document investigates cloud centered video streaming methods particularly from the mobile viewpoint. The qualitative part of the research contains explanations of current video development methods, streaming methods and third celebration cloud centered streaming solutions for different mobile which shows my realistic work relevant to streaming methods with RTMP protocols family and solutions for iPhone, Android, Smart mobile phones, Window and BalackBerry phones etc.

Keywords : *QCIF, CIF, 4CIF, HD, FFMPEG encoding/ streaming, zencoder cloud based encoding API , amazon cloud front service, video streaming, H.264, MPEG- 4, RTMP, RTMPT, RTMPE, RTMPTE.*

GJCST-E Classification : *C.2.4*

Strictly as per the compliance and regulations of:

Cloud-Based Mobile Video Streaming Techniques

Saurabh Goel

Abstract - Reasoning processing is changing the landscape of the electronic digital multi-media market by moving the end customers concentrate from possession of video to buying entry to them in the form of on-demand delivery solutions. At the same time, the cloud is also being used to store possessed video paths and create solutions that help audience to discover a whole new range of multi-media. Cellular devices are a key car owner of this change, due to their natural mobility and exclusively high transmission rate among end customers. This document investigates cloud centered video streaming methods particularly from the mobile viewpoint. The qualitative part of the research contains explanations of current video development methods, streaming methods and third celebration cloud centered streaming solutions for different mobile which shows my realistic work relevant to streaming methods with RTMP protocols family and solutions for iPhone, Android, Smart mobile phones, Window and BalackBerry phones etc.

Keywords : QCIF, CIF, 4CIF, HD, FFMPEG encoding/ streaming, zencoder cloud based encoding API , amazon cloud front service, video streaming, H.264, MPEG- 4, RTMP, RTMPT, RTMPE, RTMPTE.

I. Introduction

Developing multi-media content for effective indication over reasoning of cloud based centered mobile system with limited data rates, such as the 3G-324M system needs skills and knowledge. It needs an knowing of the fundamentals that have an effect on movie quality, such as codec choice and compression, and the use of specific resources, such as the FFMPEG Development, and Zencoder Cloud centered development API which can be used to validate that the material of videos clip data file are effectively specified for end customers.

II. Video Fundamentals

Due to bandwidths of mobile networks are limited, video data must be encoded/compressed considerably. This part wraps the fundamentals of encoded video and its characteristics within different networks.

a) Bandwidth

In multi-media streaming programs, video encoding is used for the reason that uncompressed video needs huge information space to store data. In fact, High definition (HD) films on DVD or Blu-ray are already in a compacted format that provides information of 4 - 6 Megabyte per second. For cellular streaming systems, which can require information rates as low as 30 kilobytes per second, this means that it clip must be compacted thousands of times or more to achieve the required information. With the growth of cellular multi-media streaming, you should work within the information restrictions of the network and the ability of the endpoint. Although 3G and next generation systems provide much higher bandwidths to cellular phone devices, as more and more endpoints use these systems for multi-media projects, conformance to focus on end customers bitrates will become more essential than today [1].

b) Networks for Video Streaming

TABLE I illustrates the network atmospheres used for distributing video services with different aspects [1]:

Table I : Networks Used For Streaming Video Services

Network	Bandwidth	Terminals	Codecs	Image Size
3G-324M	64 Kbps	Video Handsets	H.263,MPEG-4,H.264	QCIF,CIF
3G Wireless	256-768 Kbps	Video handsets, smart phones	H.263, H.264, MPEG-4	QCIF, CIF
Broadband IP	768 Kbps	Smart phones, soft client on PC	H.264	QCIF, CIF
Enterprise	2-5 Mbps	Soft client	H.264	CIF, 4CIF, HD
WiMax, LTE	2-100 Mbps	PC, TV, portable devices	H.264	CIF, 4CIF, HD

c) Audio/Video Codecs

An audio codec is a system applying criteria that encode and decode electronic digital audio information according to a given sound extendable or movies online sound structure. The item of the criteria is to signify the great stability sound indication with lowest bitrates while protecting the excellent.

Author : E-mail : saurabh.goyal6@gmail.com

Examples: AAC, ADPCM, MP3, WMA, PCM, Vorbis, Dolby AC-3.

A video codec, brief for Encoder/Decoder, is used to encode video information to accomplish a very low bitrate.

Examples: MPEG-2, H.263, MPEG-4 and H.264.

To accomplish such small bitrate audio/video, codecs make use of both lossless and lossy compression methods. We can accomplish this by third celebration system like FFMPEG open source libraries and Zencoder cloud-based encoding API.

Compression performance is the capability of a codec to encode or decode more video/audio features into an information flow described by fewer bits. The more effective a codec is at compression, the better the quality and sharpness of the video/audio clip.

III. Video Streaming

In streaming procedure, it clip data file is sent to the end individual in a (more or less) continuous flow. It is simply a strategy for shifting information such that it can be prepared as a stable and ongoing flow and it is known as Streaming or encoded movie that is sent across information system is known as Streaming. Streaming movie is a series of "moving images" that are sent in compacted form over the Internet and shown by the audience as they appear [4]. If a web individual is getting the information as sources then he/she does not have to wait around to obtain a large data file before viewing it clip or enjoying the sound.

a) Streaming Principle

Real-time video applications require media packets to arrive in a timely manner; excessively delayed packets are useless and are treated as lost [6]. In streaming programs it is necessary for the information packets to reach their location in regular basis because the wait can cause the network blockage, and can result in the decrease in all those packets suffering from extreme wait. This causes decrease in quality of information, the synchronization between customer and hosting server to be damaged and mistakes to distribute in the provided movie.

There are two types of steaming, one is real-time and other is prerecorded streaming. The protocol used for streaming purpose is UDP (User Datagram Protocol), which delivers the multi-media flow as a sequence of small packets [4]. The majority of transport protocols perform over an RTP stack, which is implemented on top of UDP/IP to provide an end-to-end network transport for video streaming [2].

b) Video Streaming Architecture

A cloud based mobile movie streaming scheme is represented in Fig. 1. A cloud based source implements a streaming hosting server which is responsible for retrieving, sending and adapting it clip flow. Depending on the application, it clip may be protected on-line for a real-time broadcasting or pre - encoded and stored for broadcasting an on demand [3].

Programs such as interactive movie, live broadcast, mobile movie streaming or interactive online games require real -time encoding. However, applications such as movie on-demand require pre-encoded movie. When the multicast session is initialized, the streaming hosting server retrieves the compressed movie and begins the loading with the adequate bitrate stream.

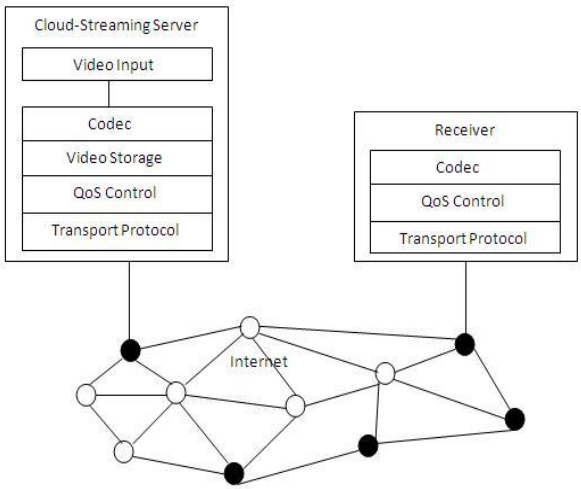


Fig. 1 : Video Streaming Architecture

IV. Video Encoding Techniques

Video codecs employ a range of encoded/decoded methods to fit videos signal into the allocated channel bandwidth. These encoding methods can influence the generating quality of it differently. An understanding of development concepts can help a material provider determine what material will look best on a mobile phone, and emphasize some of the expected tradeoffs when generating multi-media data files.

Rapid bandwidth decrease can be carried out by using video encoded/decoded methods such as [1]:

a. Eliminating mathematical redundancies
b. Dropping quality size (CIF to QCIF)
c. Using less frames per second (15 fps to 10 fps)

Further bandwidth decrease can be carried out by utilizing the styles within it information and eliminating redundancies. Image compression depends on removing information that is indiscernible to the audience. Motion settlement provides interpolation between frames, using less information to signify the change. The objective of videos encoder/decoder is to take out redundancies in it flow and to scribe as little information as possible. To achieve this objective, the encoder examples it flow in two ways:

a. In time durations from successive frames (temporal domain)
b. Between nearby pixels in the same frame (spatial domain)

A video decoder pieces it flow together by treating the development process. The decoder reconstructs it flow by adding together the pixel variations and shape variations to form complete video. In current video encoding principles requirements such as MPEG and H263 families.

a) Encoded Video Stream

An encoded video stream consists of two types of encoded frames [1]:

1) ***I-frames***
2) ***P-frames***

I-frames:

An I-frame is encoded as a single image, without referencing to any other frames. Each 8x8 block is first transformed from the spatial domain into the frequency domain [5]. It is also called a key frame, because it symbolizes the referrals key of it clip flow. All pixels that describe the image are defined in the I-frame. Videos clip decoder must begin with an I-frame to decode it clip flow because without an I-frame, a movie decoder has no referrals to determine how movie pixels have changed as the earlier frame. For this reason, compressed movie recordings normally do not begin until an I-frame is received by the videos device.

P-frames:

A P-frames is encoded relative to past reference frame [5], which can either be an I-frame or a before P-frame. The quantity of information in a P-frame is many times small than the quantity of information in an I-frame. If videos clip begins understanding on a P-frame at an endpoint, an individual might see either scrambled movie or no movie, because there is no referrals frame.

b) Video Streaming package (.MP4, .3GP)

When streaming multi-media files to cellular handsets, it clips and audio data must be placed in the proper structure. The package structure for cellular multi-media streaming is the .3gp, defined by the 3rd Generation Partnership Project (3GPP) [1] and .mp4 file for delivery to cellular phone devices. Because the bandwidths of movie telephony networks are limited, it clips and audio data included in a .3gp file is compressed significantly. Within the .3gp package, movie can be encoded with specific movie codecs specified by the 3GPP. FFMPEG Encoding and Zencoder cloud based Encoding API support .3gp,. mp4 files with the H.263, MPEG-4, and H.264 movie codecs.

Table I : Overview of Different Versions of Two Standard Families

Standards	Applications	Bit rate
H.261	Video teleconferencing over ISDN	64 Kbs
MPEG- 1	Video on digital storage media (CD-ROM)	1.5 Mbs
MPEG- 2	Digital TV	2-20 Mbs
H.263	Video telephony over PSTN	>34 Kbs
MPEG- 4	Multimedia over internet, Object based coding	Variable
H.264/MPEG- 4	Improved video compression	10's-100's Kbs

c) Video Streaming limitations

Video streaming is constrained by the network channel capacity, 3G-324M channel bandwidth, Multi-coded stream, Transcoding, Packet loss, Bandwidth management and endpoint capabilities.

V. Video Streaming Techniques

There are various streaming techniques for different mobiles, Smartphone describe below:

a) Progressive Download

The mobile customer has the option to use HTTP or HTTPS to gradually download a pre-created press data file partitioned in the appropriate codecs for the product to play. As the data file starts to gradually download, play-back is started enabling an almost immediate watching of the material [8]. In the qualifications, the press gamer is constantly on the download the rest of the material. By comparison, without modern download the user would have to wait for the whole data file to obtain to the product before watching would start. During the play-back process, audiences are able to seek back and forth through the whole press data file. If the audience looks for forward to a point in the schedule that has not yet downloadable, the press gamer stop play-back until the data comes.

b) HTTP Live Streaming

HTTP Live streaming (also known as HLS) is an HTTP-based media streaming communications protocol implemented by Apple Inc. as part of their QuickTime X and iPhone. Apple's HTTP Live Streaming protocol (HLS), is an adaptive streaming video delivery protocol for iOS devices. It utilizes the H.264 video codec, which is segmented and encapsulated in MPEG2 transport streams, and .M3U8 index files to deliver live and on-demand video. The device automatically selects the

most appropriate stream given available bandwidth, CPU and platform constraints, downloads a manifest for that stream, and then downloads segmented chunks to the buffer for the playback.

HLS streaming provides the best user experience, but its benefits also include good IT practices and important business considerations:

1) The best user experience: Since the server can maintain multiple versions of the video clips in different formats, an iPad user with a Wi-Fi connection can stream a higher quality version of the video than an iPhone user viewing over a 3G connection.
2) Reach more viewers: Routers, NAT, and firewall settings are more likely to support video delivered with HTTP than other transfer protocols, so more users will be able to access your video.
3) Save on data transfer: As opposed to a progressive download of a video, with HLS, only a few segments of video are downloaded at time. If a viewer only watches five minutes of streamed video, publishers only pay for that data transfer. Moreover, the HTTP chunks are cacheable by CDNs and across network infrastructure, so files are served from an origin server only once and cached close to users.
4) Secure video content: The HLS specification has provisions to ensure security of the stream, which is great news for broadcasters or publishers who want to stream licensed content. The entire HLS stream can be encrypted using AES-128.

Fig. 2 and Explanation, shows my practical work for mobile video streaming on Cloud with streaming server by using Amazon CloudFront services which have lots of components which are playing key role.

Explanation of R&D work

Live streaming with Amazon Web Services allows you to use the features of Adobe Flash Media Server version 4.5, including live video streaming where your live video is delivered by a series of HTTP requests from the player that is controlled by manifest files. Flash Media Server 4.5 supports two HTTP file formats: HLS (HTTP Live Streaming) for iOS devices and HDS (HTTP Dynamic Streaming) for Flash applications. You can stream high-quality media using the free Flash Media Live Encoder desktop application either for Windows or for Mac OS.

CloudFront content delivery service would support on-demand RTMP streaming from Flash Media Server 4.5. In practice, this offers a new, flexible low-cost CDN solution, particularly for users with relatively small or intermittent streaming delivery needs. AWS charges only for bits stored and bits transferred. There's no monthly minimum, no sign up fee or setup fees, and no ongoing costs unless you're actually using the service [10].

In this example, we will walk through the steps of setting up CloudFront streaming and getting it working on your site:

a. Set up an AWS Simple Storage Service (S3) account where content will live.
b. Create a "bucket" in S3 to store media files.
c. Shift content to S3 bucket and set its permissions to allow public access.
d. Set up a CloudFront streaming distribution that point at S3 storage bucket.
e. Now you are ready to stream.

CloudFront uses Adobe Flash Media Server 4.5 to stream on-demand content with Adobe's Real-Time Messaging Protocol (RTMP). CloudFront accepts RTMP requests over port 1935 and port 80.

CloudFront supports the following variants of the RTMP protocol:

a. RTMP—Adobe's Real-Time Message Protocol
b. RTMPT—Adobe streaming tunneled over HTTP
c. RTMPE—Adobe encrypted over HTTP
d. RTMPTE—Adobe encrypted tunneled over HTTP

To secure it, just use the RTMPE protocol instead of the regular RTMP.

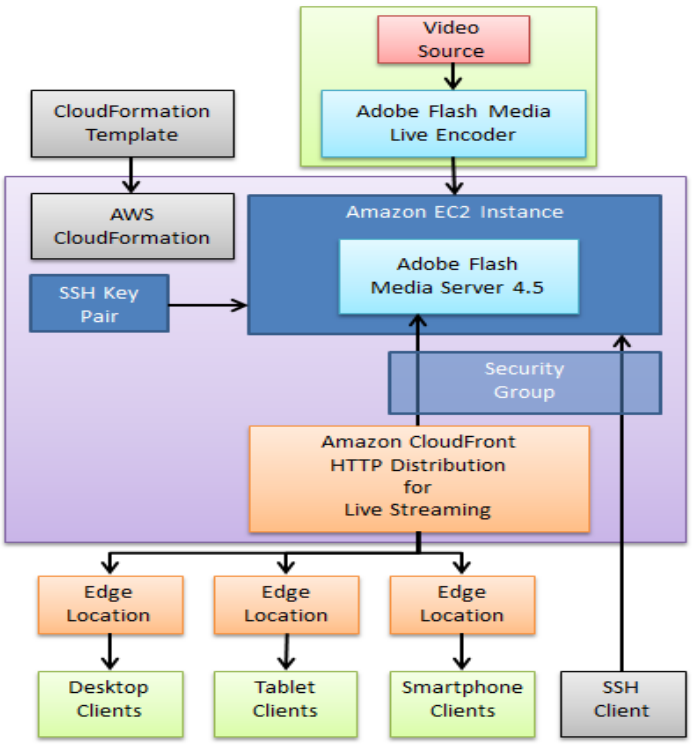


Fig. 2 : CloudFront Live streaming architecture

Many reputed IT companies are using HTTP Live streaming service to enhance the streaming power in their mobile domain infrastructure.

- Adobe Systems established an update to its Adobe Flash Media Server product supporting HTTP Live streaming.

- Livestation streams numerous TV channels such as France 24, RT, and Al Jazeera English.
- Microsoft added support for HTTP Live Streaming in IIS Media Services 4.5.
- Google added HTTP Live streaming support in Android 3.0 Honeycomb.
- HP added HTTP Live streaming support in webOS 3.0.5.
- FFMPEG added HTTP Live Streaming and Encoding support for various mobile devices [11] [12].
- Zencoder Cloud based Encoding API added HTTP Live streaming support for iPad, iPod Touch and Apple TV [13].

VI. Conclusion

In this paper, we have discussed firstly in audio/video basics which deliver video on network with required bandwidth and codecs then after we discussed about the video streaming architecture that develop streaming servers which are responsible for retrieving, sending and adapting the video stream data in 3G or others network.

For streaming the multimedia file over network, video compression techniques are major issue to encode the different types of audio/video file for different mobile devices. Compression can be performed by FFMPEG Encoding; Zencoder cloud based Encoding API which provides lots of Encoding techniques which are solution for the cloud based environments.

Then we presented the main issue of video streaming techniques for streaming the video over the internet or cloud based network for iPhone, Android, Window phone and Smartphone. Apple Company provides the solution for video streaming in terms of HTTP Live streaming which are accepted by many reputed companies for mobile devices for video streaming purpose for future perspective by using RTMP family protocols.

I believe that a lot of effort should be done in this paper to propose efficient and viable solution for mobile video streaming in cloud based environment.

VII. Acknowledgment

There are some key personalities involved, whose role has been very vital to pave way for success of the paper. I take the opportunity to express my sincere thanks and gratitude to them.

I would like to thank my R&D team members of Pariksha Labs Pvt. Ltd, Gurgaon, India. Last but not the least, I would like to extend my heartfelt regards to all those who helped me directly or indirectly in the accomplishment of the paper.

References Références Referencias

1. Considerations for Creating Streamed Video Content over 3G-324M Mobile Networks, White paper. www.dialogic.com
2. Prof. Nitin. R. Talhar, Prof. Mrs. K. S. Thakare "Real-time and Object-based Video Streaming Techniques with Application to Communication System", Proc .of CSIT vol.1 (2011) © (2011) IACSIT Press, Singapore.
3. Hatem BETTAHAR, "Tutorial on Multicast Video Streaming Techniques", SETIT 2005, 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications March 27- 31, 2005 –TUNISIA.
4. Mamoona Asghar, Saima Sadaf , Kamran Eidi, Asia Naseem, Shahid Naweed "SVS - A Secure Scheme for Video Streaming Using SRTP AES and DH", European Journal of Scientific Research ISSN 1450-216X Vol.40 No.2 (2010), pp.177-188 © EuroJournals Publishing, Inc. 2010.
5. Jian Zhou, "New Techniques for Streaming MPEG Video over the Internet", UMI Microform 3111144, Copyright 2004 by ProQuest Information and Learning Company, pp. 11-26.
6. M D Walker, M Nilsson, T Jebb and R Turnbull "Mobile video-streaming", BT Technology Journal-Vol 21 No 3- July 2003.
7. Jianyu Dong "Efficient and Effective Streaming Technologies for 3-D Wavelet Compressed Video", the Ohio State University 2002.
8. Delivering content to Apple iPhone, iPod Touch and iPad using RealNetworks Helix Solutions ©2010 RealNetworks, http://www.real.com
9. Streaming media from Wikipedia available at http://en.wikipedia.org/wiki/Streaming_media
10. Amazon CloudFront available at http://aws.amazon.com/cloudfront/
11. FFMPEG StreamingGuide available at http://ffmpeg.org/trac/ffmpeg/wiki/StreamingGuide
12. FFMPEG x264 Encoding Guide, http://ffmpeg. org/trac/ffmpeg/wiki/x264EncodingGuide
13. Zencoder cloud based iOS/Mobile Encoding, https://app.zencoder.com/docs/guides/encoding-settings/ios-and-mobile.

Global Journals Inc. (US) Guidelines Handbook 2012

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 .

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

R

S

T

U

V

W

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