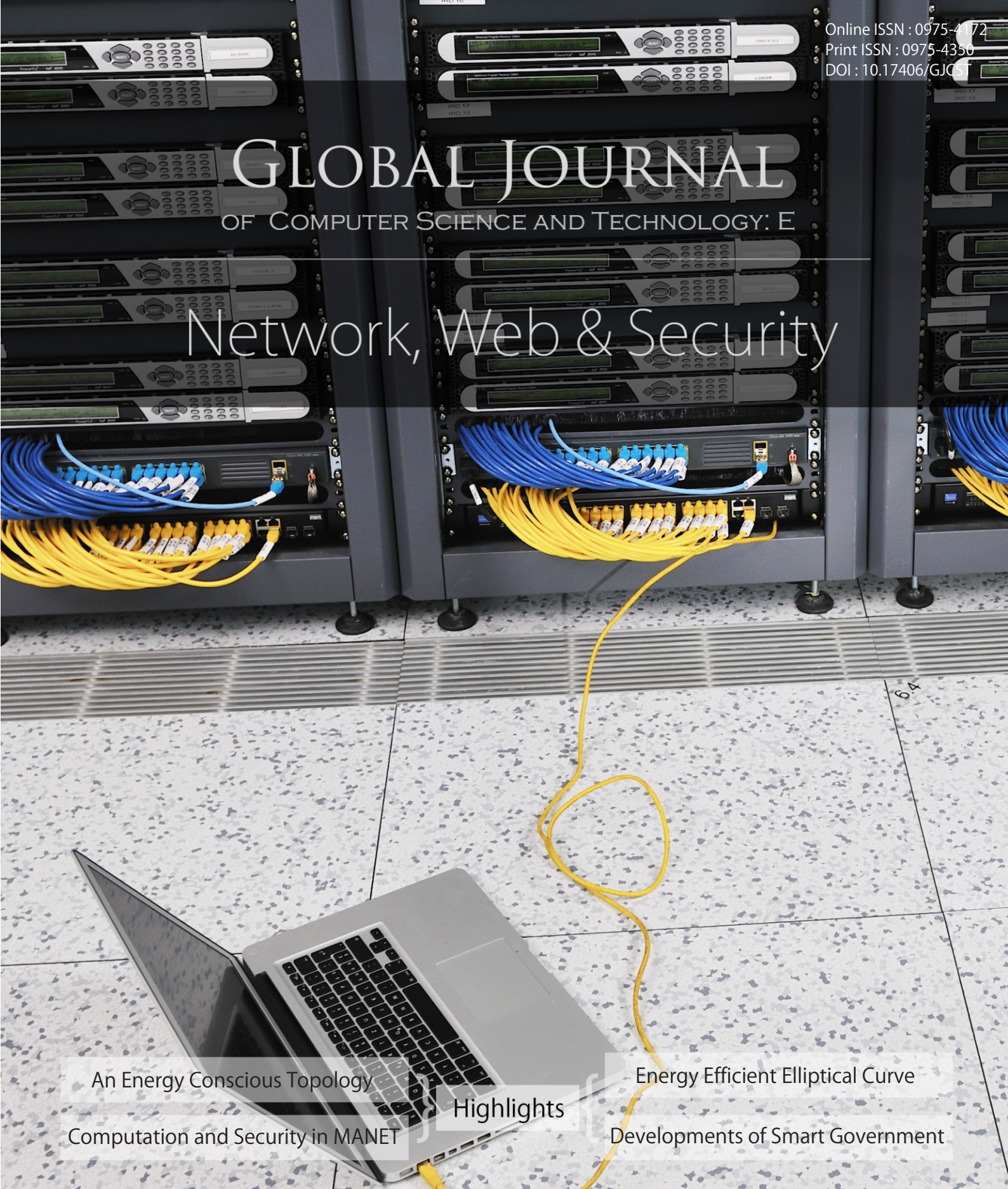
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security



An Energy Conscious Topology

Computation and Security in MANET

Highlights

Energy Efficient Elliptical Curve

Developments of Smart Government

Discovering Thoughts, Inventing Future

Volume 16 Issue 3 Version 0.1

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

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

Volume 16 Issue 3 (Ver. 1.0)

Open Association of Research Society

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

Global Journals Inc.

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

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals Headquarters
301st Edgewater Place Suite, 100 Edgewater Dr.-Pl,
Wakefield MASSACHUSETTS, Pin: 01880,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin: 452009, 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: *investors@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)

Integrated Editorial Board
(Computer Science, Engineering, Medical, Management, Natural Science, Social Science)

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 Issue

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Energy Conscious Topology Augmentation Methodology for On-Chip Interconnection Networks

By Samta Jain, Vaishali Sodani & Naveen Choudhary
College of Technology and Engineering, India

Abstract- On-chip communication, modular, scalable packet-switched micro-network of interconnects, generally known as Network-on-Chip (NoC) architecture can be designed as regular or application-specific (irregular) network topologies. Application specific custom network topologies are advantageous in terms of optimized design according to given performance metrics and regular network topologies are advantageous in terms of its modularity, lower design time and efforts required and thus are suitable for mass production. So to offer the advantages of both the topologies this paper proposes a methodology to augment the regular topology according to the application characteristics. The experimental results demonstrate that the proposed methodology can reduce dynamic communication energy consumption by on average of 32.79% and reduction in average per flit latency by on average of 16.22% over regular 2D NoC architecture.

Keywords: network-on-chip, application specific topology, interconnection network, dynamic communication energy.

GJCST-E Classification : C.1.2, C.2.0, C.2.1

Strictly as per the compliance and regulations of:

An Energy Conscious Topology Augmentation Methodology for On-Chip Interconnection Networks

Samta Jain [α], Vaishali Sodani [σ] & Naveen Choudhary [ρ]

Abstract- On-chip communication, modular, scalable packet-switched micro-network of interconnects, generally known as Network-on-Chip (NoC) architecture can be designed as regular or application-specific (irregular) network topologies. Application specific custom network topologies are advantageous in terms of optimized design according to given performance metrics and regular network topologies are advantageous in terms of its modularity, lower design time and efforts required and thus are suitable for mass production. So to offer the advantages of both the topologies this paper proposes a methodology to augment the regular topology according to the application characteristics. The experimental results demonstrate that the proposed methodology can reduce dynamic communication energy consumption by on average of 32.79% and reduction in average per flit latency by on average of 16.22% over regular 2D NoC architecture.

Keywords: network-on-chip, application specific topology, interconnection network, dynamic communication energy.

I. Introduction

Network-on-Chip designs consist of a number of interconnected devices (e.g. general or special purpose processors, peripherals, memories etc.) where communication between these system modules is achieved by sending packets over an interconnection network. Packets are transported from one to another module via the interconnection networks [1]. Thus, the interconnections among multiple cores on a chip have a significant impact on communication and performance of the chip design in terms of dynamic energy consumption, latency, throughput etc. So topology selection is an important choice in the design of NoC and in Network on Chip topology design is one of the significant factor that affects the net delay of the system and the dynamic communication energy of the system. Topological parameters, like hop count, wiring layout are closely related to the performance and power dissipation of a network [13]. In other words, it can be said that the NoC performance can be greatly affected by the underlying topology and the routing function followed by the communication cores.

NoC architecture can be designed as regular or application specific network topology. Application-specific network topologies are designed to make the system more application centric [2]. As a result, the performance objectives such as power consumption, latency, area of the chip, number of routers in the system can be optimized effectively with the given design constraints [3]. However the loss of modularity in application-specific NoC generally leads to increased time-to-market in comparison to the modular generic standard NoC topologies.

Regular topologies like 2D mesh are more structured and built not considering much about the application characteristics. A regular NoC topology assumes a homogeneous distribution of routers, which leads among others to lower design time and cost. Therefore regular NoC topologies are suitable for mass production due to lower design cost and effort required. Additionally, regular topologies are highly reusable and impose the minimum re-design effort, in case they are employed to different applications.

However, due to the lack of fast paths between remotely situated nodes and many hops between different communicating nodes regular topology architectures for a given routing methodology may suffer from long packet latencies and higher communication power dissipation. Although the regular structure significantly address the implementation issues, such as floor planning, unequal lengths of wire, hence results in poorly controlled electrical parameters.

In order to meet the communication requirements, accelerate time-to-market and cut down the communication energy consumption, there is a great need to find new design alternatives of customizing the regular architectures as per the communication requirements. We therefore focused our research on exploring and finding an efficient methodology to tailor the regular 2D mesh topology so that the dynamic communication energy can be optimized. The methodology will optimize the dynamic communication energy consumption by reducing the hop count or by reducing the number of short links according to the traffic characteristics of the application for a given routing function. Tailoring the regular topology shall reduce the design time in comparison to the design of application specific NoC from stretch with reasonable performance advantages.

Author α σ ρ: Deptt. of CSE, CTAE, MPUAT, Udaipur.
e-mails: samtajain1991@gmail.com, vaishalisodani@gmail.com, naveenc121@yahoo.com

In [4], the authors introduce additional random links to the mesh and torus network and investigate the performance of these networks. In [5], authors present a methodology to automatically synthesize an architecture where a few application-specific long-range links are introduced on a regular mesh network. Drawing inspiration from such work this paper proposes the methodology to insert energy conscious shortcut links with practical design constraints such as link length, port constraints. The proposed design also strives to add minimum number of shortcuts so as not to distinguish the original design in terms of area and floor-planning.

In section 2, NoC communication energy and routing functions are discussed. In section 3, the proposed methodology is given. In the next section, the experimental results are discussed and in the last section the conclusion is presented based on the results.

II. NoC Communication Energy and Routing Function

a) Dynamic Communication Energy Model

The dynamic communication energy model [7] for the network on chip can be defined as:

$$E^{bit\ (ti,\ tj)} = n^{hops} \times E^{rbit} + (n^{hops-1}) \times E^{LBit} \quad (1)$$

Where $E_{bit}^{(ti,\ tj)}$ = the average energy consumption for sending one bit of data from t_i to tile t_j, n_{hops} = the number of routers the bit traverses from tile t_i to tile t_j, E_{rbit} = the energy consumed by the router for transporting one bit of data, E_{Lbit} = the energy consumed by unit link/channel for transporting one bit of data. For the NoC networks with unequal link length, the ((*nhops* - 1) x E_{Lbit}) can be replaced as the summation of bit energy consumed by each link in the path/route, the bit follows from source tile to the destination tile [21].

Hop count is the number of routers the bit traverses from source tile to tile destination tile. The communication energy model [7] for the network on chip clearly shows that the latency and power consumption linearly relates to the average number of hops the packet traverse, hence to the network topology. So we will optimize the latency and power consumption by reducing the hop count between the source tile and destination tile for a given routing function.

b) Routing Function in NoC

Routing function determines how the data is transmitted from source tile to destination tile. Routing algorithm can be grouped according to different criteria. According to the place where routing decision is made, routing algorithm can be classified as centralized, source and distributed routing algorithm. In centralized the route is chosen by a central controller, in source the route is chosen by a source router prior to a sending the packet, in distributed the route is chosen by an intermediary routers [16, 17]. According to how a route is defined to route the packets, routing algorithm can be deterministic or adaptive. In deterministic routing, one path is calculated between source and destination and routing is done through that fixed path only.

Deterministic routing algorithm always routes the packets from source to destination along that same path [15]. Deterministic algorithm does not take into account network traffic situation or the network condition before choosing a path from source to destination. In adaptive routing algorithms multiple paths are calculated between source and destination but routing is done in one selected path depending upon the network traffic. In adaptive algorithm network traffic situation (such as network load, traffic condition) are taken into consideration. Limitations of adaptive routing algorithm are its implementation cost, complexity and more power consumption [16]. Deterministic routing algorithm is popular in NoC due to simplicity, low latency, simple routing logic, packet reach destination in correct order and reordering is not necessary [7]. It is a greedy algorithm because it always chooses a shortest path to deliver a packet from source to destination [17].

The design space of efficient deadlock-free routing is an important aspect which is more implicitly affected by the routing algorithm which determines which routes packets can take from source to destination. A deadlock is a situation where packets are involved in a circular wait for resources. Deadlock freedom is an important property for networks, since a packet deadlock can destroy possibilities of communication [18]. Deadlocks in a network may block communication between cores and may even lead to a complete failure of network. Therefore it is essential to have algorithms which have ability to handle them. The deterministic routing [7] (e.g. XY routing [14, 19] and odd-even routing [15, 19]) are the most widely used deadlock free routing algorithms for the popular 2D-mesh based on chip networks.

III. Proposed Methodology

In the presented work, an energy conscious topology augmentation methodology is proposed for application specific on-chip interconnection networks. In the proposed methodology a customized NoC topology is synthesized by tailoring the regular 2D mesh topology to achieve energy efficient communication.

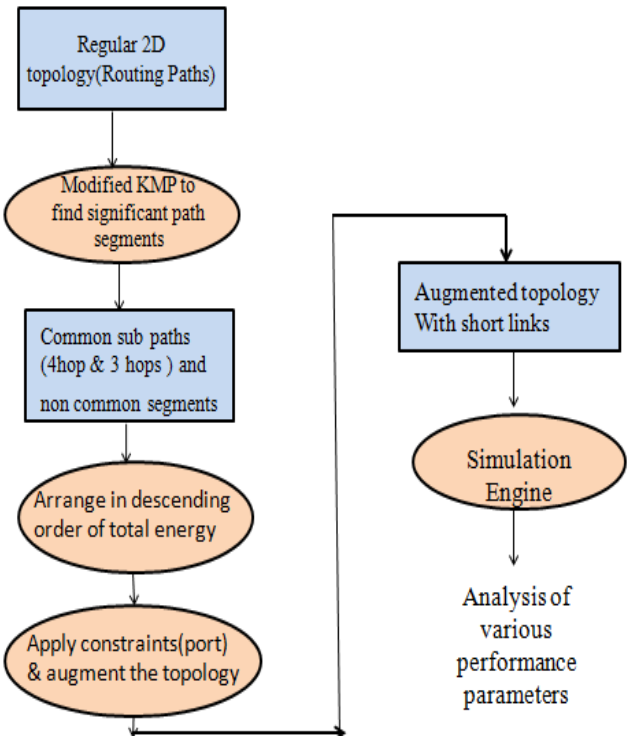


Figure 1 : Architecture of Proposed Methodology

Equation 1 clearly shows that dynamic communication energy linearly relates to the number of routers/hops the packet traverses from the source tile to the destination tile i.e. as the routers in communication path increases, the communication energy also increases. In the regular grid like NoC architecture, there is lack of fast path between two distant nodes so the packets have to traverse many hops between any two remotely situated nodes (source and destination), leading to poor dynamic communication energy dissipation. If we can able to reduce the number of hops in the communication path for a chosen routing function, the considerable amount of energy saving can be achieved in the regular NoC architecture. The reduction in the number of hops in communication path can be done by augmenting the regular mesh by inducing significant shortcut links according to the application characteristics and also constraining parameters such as length of the shortcut link and the port availability per tile. The length of the shortcut link is constrained because in NoC communication generally needs to be clock synchronized and to avoid the long wiring complexity and area overhead short links are generally preferred. The port availability per tile means add the shortcut link to a tile only if there free port is available. The augmentation of regular topology can be done by adding the significant shortcut links to the communication path segments which are carrying maximum traffic load for all the communication/routing paths for a routing function while taking the above mentioned constraints into consideration. In the proposed methodology these significant shortcut links are find out with the help of modified KMP string matching algorithm [12].

Figure 1 gives architecture of the proposed methodology. The proposed methodology augments the regular 2D mesh topology which is customized using any of the deterministic routing function. In the proposed methodology the routing paths (decided according to chosen deterministic routing function) are input to the modified KMP [12] string matching algorithm. Here this algorithm actually dealing with the routing paths as a string. This algorithm find out the path segments of 3 consecutive and 2 consecutive links (in other words of 4 hops and 3 hops respectively) which are common in other routing paths and also gathers non common path segments. In the next step the proposed methodology arranges all these segments (common sub paths of 4 & 3 hops and non-common segments) in the descending order of total communication energy consumed by these segments. This ordering has been done so that the segments with higher dynamic communication energy consumption will be considered earlier or in other words the segments which carry the maximum traffic load can be addressed earlier, so that maximum benefits can be achieved. After that, it will add the shortcut link to the routing paths which contains that segment in the regular 2D mesh topology according to the order by keeping in check the input constraints (port availability per tile). Here adding the shortcut link to segment of 3 consecutive links or to segment of 2 consecutive links means skipping 2 hops or 1 hop in the corresponding routing path respectively. Hence by doing this we are constraining the length of additional link (shortcut link) in the augmented topology. This augmented topology is referred as shortcut inclusive 2D mesh (SI-2D mesh). For the analysis of various performance parameters SI-2D mesh is validated on NoC simulator NC-G-SIM [20].

IV. Experimental Results

The performance of SI-2D mesh derived from the regular 2D mesh is validated on a network on chip simulator NC-G-SIM. It is a discrete event cycle accurate simulator for Network-on-Chip performance simulation [20]. NC-G-SIM supports regular as well as irregular topology framework with source and table based routing. E_{Lbit} is calculated according to the analytical energy model presented in [8][9]; E_{rbit} for a router is calculated the help of power simulator Orion [10] for 0.18µm technology. The communication is assumed to be of constant bit rate. Number of application (traffic) characteristics data sets were randomly generated using TGFF [11], with diverse bandwidth requirement of the IP Cores and randomly generated communication bandwidth requirement. The simulation is run for 10000

clock cycles. The average total communication energy per flit received at destination and average per flit latency are taken as performance metric. The methodology is applied to 6 set of different 2D mesh topology, for each topology 10 different test cases were generated and executed. After having experimented on

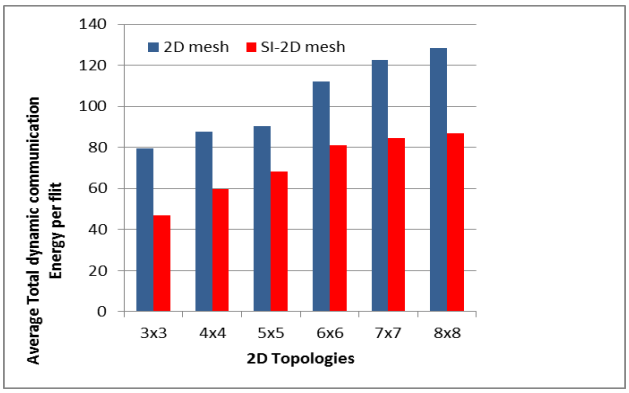


Figure 2 : Average total dynamic communication energy per flit comparative results between 2D mesh and SI-2D mesh topology

As shown in Figure 2, the short cut inclusive 2D mesh (SI-2D mesh) generated using the proposed methodology saves about on average 32.79% of dynamic communication energy consumption compared to regular 2D mesh because SI-2D mesh needs less number of hops to traverse from the source tile to the destination tile, leading to reduced dynamic communication energy and latency. Figure 3 shows comparison in terms of average per flit latency between 2D mesh and SI-2D mesh for various topologies and it depicts that the average latency per flit gets reduced by on average of 16.22% in SI-2D mesh compared to the regular 2D mesh

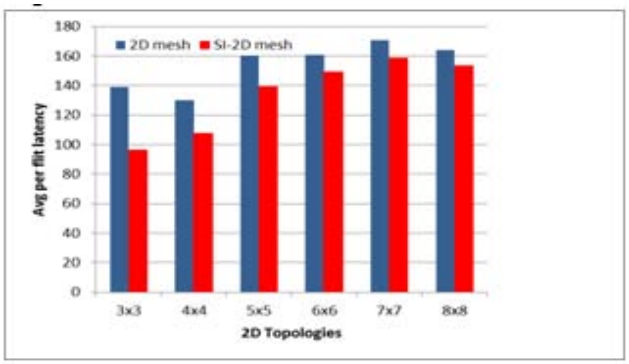


Figure 3 : Average per flit latency comparative results between 2D mesh and SI-2D mesh

It is clear that we are getting marginal reduction in latency as compared to the dynamic communication energy; the reason behind this is the occurrence of the congestion due to the generation of hotspot at the induced routers which are heavily loaded as they are bearing the traffic load which was earlier getting spread number of topology sets, the average of obtained results is represented to demonstrate the effectiveness of the proposed methodology. The configuration files for a given traffic pattern are generated using the proposed methodology and supplied to the simulator as an input. over multiple routers. However still there is gain in latency as the switching delay in path from source to destination for various application characteristics is reduced due to decrease in number of routers in the corresponding paths.

V. Conclusion

In this paper, a greedy energy conscious topology augmentation methodology for on-chip interconnection networks is proposed. Using the proposed methodology a shortcut inclusive topology is designed according to the traffic characteristics. The proposed methodology is greedy but fast and uses fast modified KMP string matching algorithm [12] for exploring the effective and efficient shortcuts to be augmented in the given regular architecture. The experimental result clearly shows that shortcut inclusive topology generated using proposed methodology is able to reduce dynamic communication energy leading to significant energy savings and also reduction in the average per flit latency as compared to the regular topology.

References Références Referencias

1. Dally, W. J., and Towles, B. (2001). Route packets, Not wires: On-chip interconnection networks. In Design Automation Conference, Proceedings, pp. 684 -689, IEEE.
2. Umamaheswari, S., Rajapaul, P., J. (2011). Energy, Throughput and Area Evaluation of Regular and Irregular Network on Chip Architectures. nternational Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.5.
3. Yu Bei, Dong Sheqin (2010). Floorplanning and Topology Generation for Application-Specific Network-on-Chip. Design Automation Conference (ASP-DAC), 2010 15th Asia and South Pacific. IEEE: 535 – 540.
4. Fuks, H., Lawniczak, A. (1999). Performance of data networks with random links. Mathematics and Computers in Simulation, vol 51.
5. Ogras Umit, Y. and Marculescu, R. (2005). Application Specific Network-on-Chip Architecture Customization via Long Range Link Insertion.
6. Ogras Umit, Y. and Marculescu, R. (2006). It's a Small World After All: NoC Performance Optimization via Long Range Link Insertion. IEEE, VOL. 14, NO. 7.
7. Hu, J., Marculescu, R. (2005). Energy and performance-aware mapping for regular NoC architectures. Computer- Aided Design of Integrated Circuits and Systems, Vol. 24: 551-562.

8. Hu, J., & Marculescu, R. (2003). Energy-aware mapping for tile-based NoC architectures under performance constraints. In Proceedings of the Asia and South Pacific Design Automation Conference, pp. 233-239.
9. Choudhary, N., Gaur, M. S., Laxmi, V., & Singh, V. (2011). GA based congestion aware topology generation for application specific NoC. In Sixth IEEE International Symposium Electronic Design, Test and Application (DELTA), pp. 93-98.
10. Kahng, A. B., Li, B., Peh, L. S., & Samadi, K. (2009). Orion 2.0: A fast and accurate NoC power and area model for early-stage design space exploration. In Proceedings of the conference on Design, Automation and Test in Europe, pp. 423-428.
11. Dick, R. P., Rhodes, D. L., & Wolf, W. (1998). TGFF: task graphs for free. In IEEE Computer Society, Proceedings of the 6th international workshop on Hardware/software co-design, pp. 97-101.
12. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein. (2009). Introduction to Algorithms. The MIT Press Cambridge, Massachusetts London, England, 3rd edition.
13. George, B. (2009). Energy consumption in networks on chip: efficiency and scaling. IEEE 15th International Symposium, pp. 250–261.
14. Dehyadgari, M., Nickray, M., kusha, A., Navabi, Z. (2005). Evaluation of Pseudo Adaptive XY Routing Using an Object Oriented Model for NOC.
15. Duato, J., Yalamanchili, S., Ni L. (2003). Interconnection Networks: An Engineering Approach. Morgan Kaufmann Publishers, San Francisco.
16. Singh J. K. Performance evaluation of different routing algorithm in network on chip master dissertation National Institute of Technology Rourkella, Odesha.
17. Adamu, G., Chejara P., Garko, A., B. (2015). Review of deterministic routing algorithm for network-on-chip. International conference on science, technology and management.
18. Holsmark, R., Palesi, M. and Kumar, S. (2006). Deadlock Free Routing Algorithms for Mesh Topology NoC Systems with Regions. Digital System Design: Architectures, Methods and Tools, 9th EUROMICRO Conference, Dubrovnik, pp. 696-703.
19. Choudhary, N. (2012). Network-on-Chip: A New SoC Communication Infrastructure Paradigm. International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, vol.1, 332-335.
20. Vyas, K., Choudhary, N. and Singh, D. (2013). NC-G-SIM: A Parameterized Generic Simulator for 2D-Mesh, 3D Mesh & Irregular On-chip Networks with Table-based Routing. Global Journal of Computer Science and Technology (GJCST-E) on Network, Web & Security 13: 7- 12.
21. Wadhwani, P., Chaudhary, N., Singh, D. (2013). Energy Efficient Mapping in 3D Mesh Communication Architecture for NoC. Global Journal of Computer Science, and Technology (GJCST-E) on Network, Web & Security 13: 1-5.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

MQMF : Multiple Quality Measure Factors for Trust Computation and Security in MANET

By Kotari Sridevi & Dr. M. Sridhar
Muffakham Jah College of Engineering and Technology, India

Abstract- Identification of the mobile ad hoc network node in a secure, reliable communication is a very important factor. It will be a node in the service of reconciliation and node behaviour leads to uncertainty. It is always challenge to manage node security and resource due to the complexity of high mobility and resource constraints. Trust based security provides light-weight security computing for individual node trust to provide reliable and quality of service. In this paper we present a multiple quality measure factors (MQMF) approach for computing node trust to improvise the quality of service. It compute four quality measure factors based on node throughput and packet drop during communication to measure the node individual trustworthiness. It prevent the network from anomalous and malicious nodes to improvise the security and throughput. The evaluation measures shows an improvisation in throughput with less packet drop and computational overload in compare to existing protocols.

Keywords: *MANET, security, QOS, multiple quality measures, trust computation.*

GJCST-E Classification : *D.4.6, F.1.1*

Strictly as per the compliance and regulations of:

MQMF : Multiple Quality Measure Factors for Trust Computation and Security in MANET

Kotari Sridevi [α] & Dr. M. Sridhar [σ]

Abstract- Identification of the mobile ad hoc network node in a secure, reliable communication is a very important factor. It will be a node in the service of reconciliation and node behaviour leads to uncertainty. It is always challenge to manage node security and resource due to the complexity of high mobility and resource constraints. Trust based security provides light-weight security computing for individual node trust to provide reliable and quality of service. In this paper we present a multiple quality measure factors (MQMF) approach for computing node trust to improvise the quality of service. It compute four quality measure factors based on node throughput and packet drop during communication to measure the node individual trustworthiness. It prevent the network from anomalous and malicious nodes to improvise the security and throughput. The evaluation measures shows an improvisation in throughput with less packet drop and computational overload in compare to existing protocols.

Keywords: MANET, security, QOS, multiple quality measures, trust computation.

I. Introduction

Mobile ad hoc networks are self-organized and self-controlling wireless networks without infrastructure support. Due to the unavailability of any fixed prevention and security mechanism and centralized controlling and management system, an ad hoc network is facing major security issues and threats. It is a high challenging task to prevent ad hoc communication network form different attacks and intrusions. Even though many security protocols are proposed in this direction, but they all attained high overload due to the complexity in security mechansim. It requires a light-weight security protocol through which it will be able to provides a good quality of service and also prevent the node and network from attacks. The quality of service is reflected in the expectations and behaviour of the target node through a measures of its trust, honesty, availability, past and future activity. One of the nodes which are connected to each other on the relationship, reflecting the behaviour of a node which will be reflect by its trust, reliability, and trustworthiness [3],[7].

The network node provides the coordination between the nodes in the route protocol packets to route and rely on neighbourhood relationships [8]. To achieve a quality and secure performance standard a strong, stable and secure routing protocol is needed, which can maintain node link and mobility effectively. These effectiveness will be achieve the highest security and results against the aggressive nature of the environment. It also helps the nodes to form a secure cooperate link with other nodes and identifying the misbehaving network nodes that does not try to create instability [9]. The presence of misbehaving mainly carried out routing updates, or to advertise the wrong routing information and answer the old routing information from injecting false routing updates that make detection more difficult [1],[2].

In mobile ad hoc networks (MANET) trust-based security is an important feature. This enables organizations to deal with the uncertainty caused by the uncontrolled and open motivation to others [6]. Trust estimation and management are complex issues in MANETs due to the computational complexity of the issues and movements representing the most nodes [11], [16]. This prevents direct methods of other networks. In MANET, unreliable node can cause serious harm and adversely affect the quality and reliability of the data. Therefore, the trust and confidence level of the analysis of a node has to be positive impact on the trust with which the node conducts operation with the other node [5], [21]. In this paper, we present a protocol based on multiple quality measure factors (MQMF) to compute neighbour nodes trust and to achieve a quality and protected communication in mobile adhoc network. Mostly conventional schemes [10],[14],[19] proposed for ad hoc network trust computation have a high variation in realistic results [18]. This proposal provides a unified unit trust identification protocol enhances in MANETs security management node level of confidence and trust identity.

The rest of the paper is organized as follows. Section-2 presents the related work on trust based routing and security enhancement. In section-3, we present the proposed MQMF approach description and its mechanism. Section-4 describes the experiment and results evaluation and section-5 describes the conclusion of the paper.

II. Related Works

There are many related works performed in MANET for securing routing to achieve high quality throughput. It can be categorized in two different

Author α: Research Scholar , Acharya Nagarjuna University, Nagarjuna Nagar , Guntur , Andhra Pradesh, India. e-mail: devijak@gmail.com
Authorσ: Associate Professor, Department of Computer Applications, R.V.R & J.C College of Engineering, Guntur, Andhra Pradesh, India.

category based on their securing mechanism for different type of attacks.

In the first category, the most common method used to create a security association between the source and destination in most on-demand routing protocols, such as DSR, DSDV and AODV to ensure security [22]. In [26], the authors proposed a proactive SRP, called SEAD, according DSDV using one-way hash chains to provide authentication for the attack and modify routing information broadcast and replay attacks. In [27], in order to ensure on-demand protocols such as AODV and DSR, the authors proposed an authenticated routing protocol, called ARAN with digital signatures to provide end-to-end authentication, message integrity, and nonrepudiation. In the second category, the main goal is to protect against internal attacks in the routing traffic. In [28], the authors proposed to use both path and message redundancy to detect behavioral state by comparing different copies of a message received on a different path. The accumulated path is protected by the accumulation of signature schemes [29], which is even more expensive than RSA signatures.

Trust have an attention to a number of areas of implementation towards secure system, and it also has a wireless network to gain importance as well [13], [17]. Each has its own disciplinary procedures of literature and it has a difficulty with the filters. Studies have recently been studied in many literatures, the security systems based on trust, identity-based methods are important in MANETs [15].

In [4] and [12] trust based on direct observation of the value of a trusted node is obtained using Bayesian methodology. Sun et al. [23] found to be working well, and the entropy values of trust by a trust model is used to evaluate and plan and direct observation of uncertainty in the case of the Trust. Trust based research compared with direct observation, indirect observation or second-hand information that may be important to assess the integrity of the node. For example, the collection of evidence from the neighboring nodes when not performing the quality of the other node in a situation that other people will detect of behavior.

Ariadne [20] protocol confirmed by a route using one of three procedure: a secret key between each pair of nodes, shared secret operation of end-to-end along with the broadcast authentication. But Ariadne will ensure that lie routing requests or replies do not get source or destination, where they did not know the node caused by forged or falsification.

Secure Routing Protocol (SRP) [24] is a route discovery protocol that moderate the unfavorable effects of misbehaving activities. This protocol assumes that the security relationship between any two nodes that want to communicate exists. The source and destination will be able to use cryptographic techniques to protect their relationship on the basis of the security associations. It requires a security check only between the source and destination of the route using the MAC RREQ and RREP packets. SRP does not implement any two nodes relay route request and route reply, which said protocol lightweight and insecure authentication to various attacks.

Security-aware ad hoc Routing (SAR) [25] protocol transforms AODV [22] routing protocol to include trust hierarchies with the incorporated nodes for path evaluation and selection. Protocol implements the trust level in the organizational hierarchy using share key in each level that each nodes can express their security requirements for the requested route and only nodes which meet the following requirements only will allow to participate in the route. However, as of the node trust, key distribution, knowledge of other key components are not addressed in this proposal work.

The level of trust in their approaches to the understanding of faith, measure and calculate that work in a variety of characteristics. Given the context of a node, the node trust, reliability and the accuracy of the information received from or traversing the node is a representative of the subjective evaluation. We tested the idea protocol in comparison with SAR [25] to evaluate the use of a MANET routing protocol and procedures for distribution of trust in identity important and promising approaches and routing mechanism in the following sections.

III. Multiple Quality Measure Factors Approach

The propsed MQMF approach performs its operation in three different stages as, Acquisition of CA certificates, computation of trust using MQMF factors, and MQMF based Trust Routing Mechanism. We assume that, both kind of internal and external attacks are present in the network, and all the node present in the network are considered as trustworthy. A secure identification key as *id_key,* for each node will be provided using a asymmetric cryptography mechanism in a network. This *id_key* is utilized to protectthe message fabrication through a message encryption.

a) Acquisition of CA Trusted Certificate

Acquisition of CA trusted certificate will be obtained from a trusted third party authority, before joining the network. This certificate is loaded one time and it remain in the node till it revoke. It validity remain for lifetime, but it become ineffective if the node trustworthiness degrades below the threshold level decided. The notations used in trusted certificates for a node Certificate representation as N_{CA_cert} are denoted as,

Notation	Description
$CA\_T_{pub\_key}$	Certificate authority Trusted Public Key
$CA\_T_{pvt\_key}$	Certificate authority Trusted Private Key

N_T_{key}	Node Trusted Key
N_{add}	Node Unique Address
N_{pub_key}	Node Public Key
N_{pvt_key}	Node Private Key

and, the certificate issued by a trusted CA is represented as,

$$N_{CA\_cert} = \boldsymbol{E}_{\boldsymbol{CA\_T_{pvt\_key}}}[N_{add}, N_{pub\_key}, CA\_T_{pub\_key}, E(N\_T_{key})_{N_{pvt\_key}}]$$

A trusted CA certificate provides a Public and Private key, which will be used for enccryption and decryption. Along with the CA key the certificate also provides, nodes address, it's public and private key, and a trusted key. All these are bundled and encrypted by node private key N_{pvt_key}, and the entire certificate is secured with CA private key, as $CA\_T_{pvt\_key}$. A node performs the verification of the other node by comparing their trusted CA public key, $CA\_T_{pub\_key}$ which is provided in the certificate.

b) Computation of Trust using MQMF factors

The proposed MQMF approach performs the trust computation as *T*, based on four factors as, *Correct_mf*, *Incorrect_mf*, *Lost_mf* and *Throughput_mf* rate. A *Correct_m ,as* C_{mf}, measures the node identity correctness being produced by a node during the verification, and an *Incorrect_mf as* I_{mf}, measures the rate of identity failure or wrongly produced the key for the verification. These two, C_{mf} and I_{mf} factors are being used for trust computation. *Lost_mf as* L_{mf}, calculates the data packets lost or dropped during communication, and *Throughput_mf* as T_{mf}, calculates number of data packets delivered. L_{mf} and T_{mf} factors are used for the quality measures computation. The equations for the calculation of C_{mf}, I_{mf}, L_{mf} *and* T_{mf} are shown below.

$$C_{mf} = \sum_{i=0}^{n} correct\_measure \qquad (1)$$

$$I_{mf} = \sum_{i=0}^{n} Incorrect\_measure \qquad (2)$$

$$L_{mf} = \sum_{i=0}^{d} lost\_pkts \qquad (3)$$

$$T_{mf} = \sum_{i=0}^{d} pkt\_delivered \qquad (4)$$

Where, *n* represents different iteration cycles performed for the node identification during communication cycle, and *d* represents the number of data packets communicated during the communication cycle.

Based on the above computation value of C_{mf}, I_{mf}, L_{mf} and T_{fmf} of a node, trust rate as NT_{rate} will be computed for each node using equation-5, and throughput rate as PD_{rate} will be computed for packet delivery using equation -6.

$$NT_{rate} = \frac{(C_{mf} - I_{mf})}{n} \times 100 \qquad (5)$$

$$PD_{rate} = \frac{(T_{mf} - L_{mf})}{d} \times 100 \qquad (6)$$

Using , NT_{rate} and PD_{rate} we will compute the final Trust Computation as $T_{measure}$ for each node to perform a trust decision during communication using equation-7. The runtime decision different trust threshold limit value will be considered for the evaluation of throughput. The following section discusses the routing mechanism using as $T_{measure}$.

$$T_{measure} = \frac{(NT_{rate} + PD_{rate})}{2} \qquad (7)$$

c) MQMF based Trust Routing Mechanism

All routing protocols objectives is to perform efficient routing in mobile adhoc network. In the initial stage generally routing protocol discover the routes to send data. But, in MQMF protocol, along with route discovery it also compute $T_{measure}$ for each node before sending data. In MQMF routing mechanism, we initially considered that all nodes are normal and trustworthy. The routing mechanism for the data routing is described in Alogrithm-1 using MQMF $T_{measure}$ which is computed using equation-7.

Algorithm 1: MQMF based Trust Routing Mechanism

Source node N init data forwarding → *forwardData* (D_{addr}, *Data*, *pkt_seqno*)

Method1: forwardData (Dest$_{addr}$, Data, sqno)

Trust_Threshold_limit = 25;

N gets the first hops nodes from the route table → $Node\_F_{hop}[]$

For "*p=0; p <= number of packet to send*" **Loop**
  For "*h=0, h<= number of hops*" **Loop**
    $Node\_F_{hop}[h]$ → *first_hop*
    Compute_NodeTrust_Rate (f_hop) → NT_{Rate}
    Compute_PacketDelivery_Rate(f_hop) → PD_{rate}
    Compute_Trust_Measure (NT_{Rate}, PD_{rate}) → $T_{measure}$

    if $T_{measure}$ >= *Trust_Threshold_limit* **then**
      forwardData → *first_hop*
    else
      Compute next forwarding hop $T_{measure}$ from $Node\_F_{hop}[]$
    end if
  End for
End for

Every intermediate node in the route verify the $T_{measure}$ of their next hop before forwarding data in the route. A source node initiates the data packets routing using the path discovered. Each node in the path verifies its neighbour node identity by producing a trust key, N_T_{key} which secured with encryption using $CA\_T_{pub\_key}$. On successful verification the node identity its *correct_measure* is incremented, in case of wrong identity its *incorrect_measure* is increased by 1. The identified neighboring node checks the $T_{measure}$ value of each firt hops node before passing up the data packets. The node sends the data packets to node which have the highest $T_{measure}$ value. This mechanism will guarantees the source the successful delivery of data packets through the trusted nodes. On successful delivered *pkt_delivered* is incremented, and in case if loss or drop *lost_pkts* is incremented by 1.

All intermediate nodes must send a signed confirmation of the previous hop for the delivery of a data packet to the next hop. If the next hop is not able to provide the confirmation to the intermediate node then it send an error the next hops. If an intermediate node on the path to the target jumps all else fails, send an error message to the source path. Source punishes all nodes in the path by reducing their $T_{measure}$ value, such that in the future such nodes can be avoided for the communication.

IV. Experiment Evaluation

a) Simulation Setup

To evaluate MQMF approach we modified the AODV protocol and evaluated the effect of our proposed protocol in comparison with SAR[25] and AODV[22] using Glomosim Simulator. The packet header size of route request and routing has increased as we added the security parameters. We simulate the simulation with the following setup parameters as described in Table-1.

Table 1 : Simulation Parameters

Configuration	Parameter Values
Simulation Area	1200m X 1200m
No. of Nodes	50
Mobility Speed	0 to 20 m/s
Source-Destination Pairs	20
Packet Size	512 bytes
CBR Rates	4 pkts/sec
Mobility	RWP
Mobility Speed (m/s)	0,20,40,60,80,100

The experiment analysis is perform using the parameter described in Table-1. The simulation evaluated for 600 seconds with varying the mobility speed from 0 to 100m/s in a Random Way-point model mobility. We consider mobility changes for the evaluation, as it have high impacts on the performance of throughput. For the security and for the trustworthiness measure evaluation we introduced 25% of malicious nodes.

During the route discovery all nodes in the network are normal and trustworthy, but during simulation a 25% of the malicious nodes are chosen dynamically to disrupt the network. These malicious node in network generally drop all the packets it receives and produce invalid identification during verification. However all of the data modification attacks can be detected using signature verification in MQMF approach and dropping of the financial data packets misbehaving by the network. For this evaluation we measured throughput and control overhead.

V. Results Evaluation

a) Throughput

Throughput is measure based on the total number of packet delivered against the total number of data packets originated. The evaluation of throughput result is presented in the absence and presence of malicious nodes.

Figure-1 and 2, presents the throughput performance comparison between the protocol. All protocol shows relatively drop of throughput with increasing of speed in both presence and absence of malicious nodes. The MQMF protocol shows an improvisation compared with AODV and SAR protocols in the presence of malicious nodes. The improvisation of the secure data throughput due to routing through a trusted node. In the absence of malicious illustrates the average performance due to the cryptography overhead. The proposed MQMF shows 25% improvisation in throughput and 10-20% downfall of throughput in presence of malicious nodes.

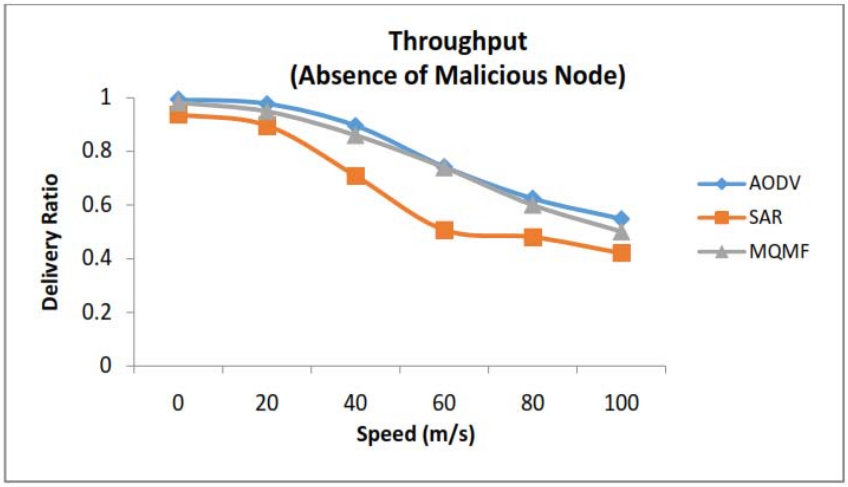


Figure 1 : Throughput in Absence of Malicious Nodes

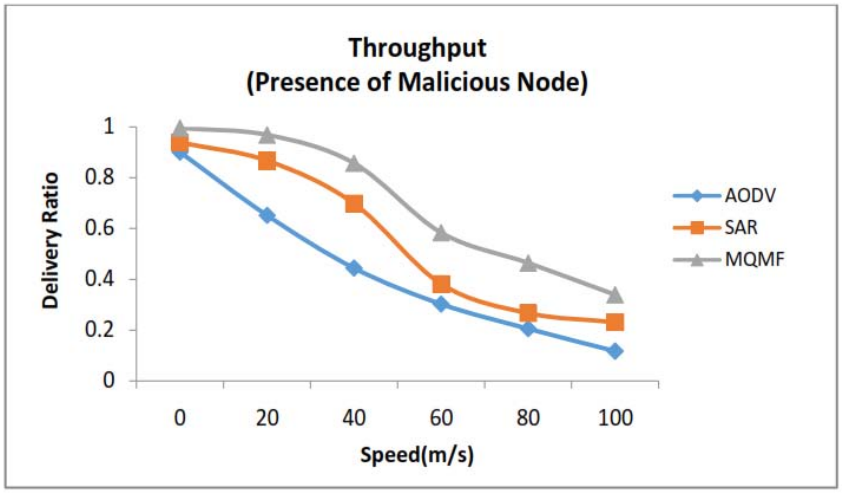


Figure 2 : Throughput in Presence of Malicious Nodes

b) Control Overhead

Control overhead measures the computational load over the network to perform the protocol execution. Its computed based on the total number of control packets exchanged during the complete communication cycle of the simulation.

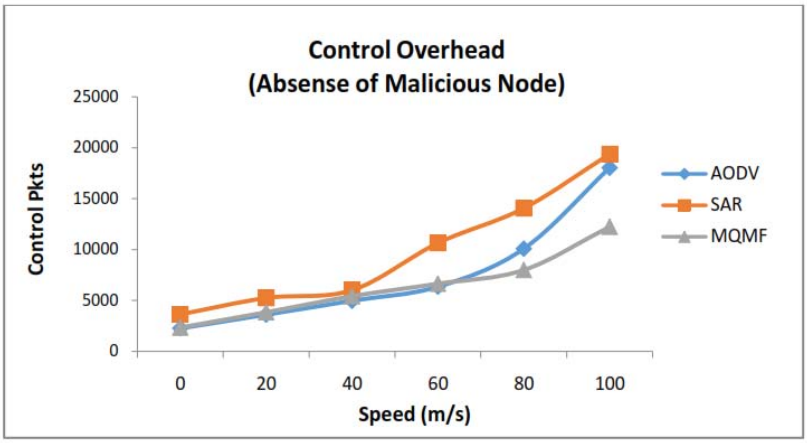


Figure 3 : Control Overhead in Absence of Malicious Nodes

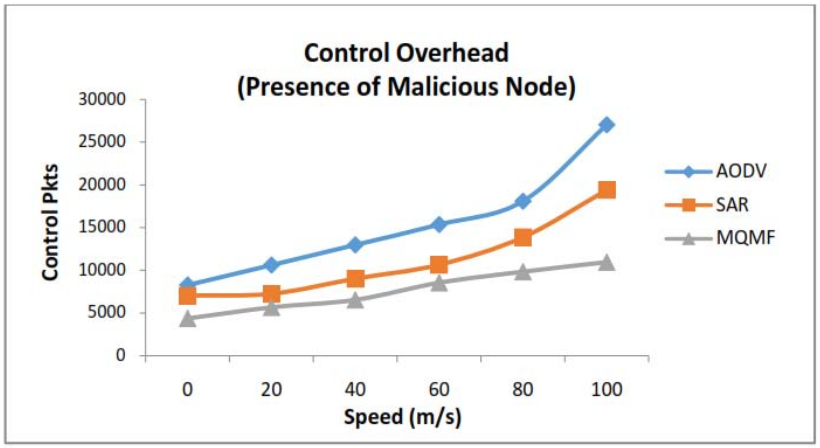


Figure 4 : Control Overhead in Presence of Malicious Nodes

Figure-3 and 4 shows control overhead in the absence and presence of malicious nodes between MQMF and other protocols. All protocol shows relatively increase in overhead with increasing of speed in both presence and absence of malicious nodes. MQMF shows low overhead incompares to others in presence of malicious nodes due to the trust computation and node identification which builds a secure path, where as SAR protocol carry out safety inspections repeatedly during communication and in AODV a lot of link failure with varying speed and the presence of a malicious node increases the high number of control packet exchange, which increases their routing overhead in compared with MQMF protocol.

c) *End-2-End Delay*

End-2-End delay evaluation measures the time taken by a data packets to reach the destination from source. The evaluation of our proposal in compare to AODV and SAR is presented in Figure-5 and 6 in the absence and presence of malicious nodes. In the case of absence of malicious node AODV performs superior in minimum speed but makes high delay in case high mobility in compared to SAR and MQMF. SAR and MQMF also shows an increase in delay with mobility speed due to more number link lost, but maintains low in compare AODV due to regular monitoring of their neighbour nodes. In case of presence of malicious node AODV suffers due to high no route loss due to malicious node and link failure due speed. But, MQMF and SAR mechanism identifies the low trust node effectively make them route data safely to the destination. In compare MQMF show low delay against SAR because MQMF $T_{measure}$ helps to dynamically route the data through trusted node which minimize the delay and improve the throughput and quality of service.

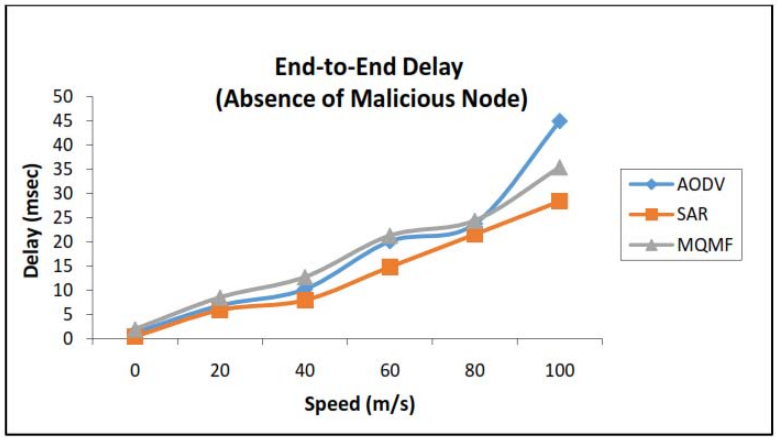


Figure 5 : End-2-End Delay in Presence of Malicious Nodes

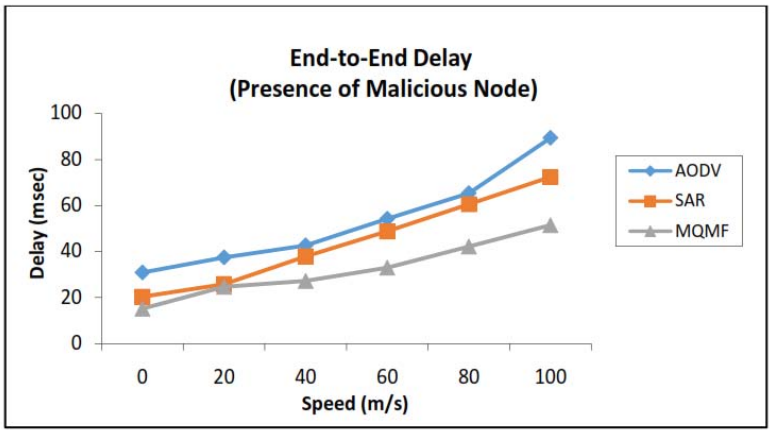


Figure 6 : End-2-End Delay in Presence of Malicious Nodes

VI. Conclusion

We proposed a new trust-based secure routing protocol as MQMF exclusive for mobile networks. MQMF authenticated routing node based on trust certificate and their hope is to identify the computer at the time of the communication. MQMF handle data routing through many paths to each destination. Every other node in the network store a local trust value and in the path table. This mechanism will guarantees the source the successful delivery of data packets through the trusted nodes. The simulation performed and compared with the performance of MQMF with AODV and SAR. MQMF achieves the similar throughput in compare to AODV and SAR in absence of no misbehaving nodes in the network, where as in the presence of misbehaving nodes MQMF shows an outperform over AODV and SAR in the throughput with a minimal overhead variation. In both cases, MQMF achieve high througput with establishing a reasonable network overload. The increase in the value of the trust for the period of time can lead to convergence. Also, a study to measure the effects of changes in that aspect of the protocol activities in the future are required.

References Références Referencias

1. Hui X., Zhiping J, Xin, Lei J, Edwin H.M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks", Elsevier, Vol-11 (n.d), p-2096-2114, 2013.
2. Ch En Xi, S Liang, MA JianFeng, MA Zhuo, "A Trust Management Scheme Based on Behaviour Feedback for Opportunistic Networks", Network Technology And Application, China Communications, April 2015.
3. Z. Wei, H. Tang, F. Richard Yu, M. Wang and P. Mason, "Security Enhancements for Mobile Ad Hoc Networks With Trust Management Using Uncertain Reasoning", IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, November 2014.
4. Ing-Ray C., Jia G., Fenye B. ,Jin-Hee C., "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", Elsevier, p-59-74, 2014.
5. K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, Vol. 14, No. 2, Second Quarter 2012.

6. Ming Li,S. Salinas, Pan Li, Jinyuan S., and X. Huang, "MAC-Layer Selfish Misbehaviour in IEEE 802.11 Ad Hoc Networks: Detection and Defence", IEEE Transactions On Mobile Computing, Vol. 14, No. 6, June 2015.
7. W. Liu and Ming Y., "AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments", IEEE Transactions On Vehicular Technology, Vol. 63, No. 9, November 2014.
8. Changiz R., Halabian H., F.R. Yu, I. Lambadaris, and H. Tang, "Trust establishment in cooperative wireless relaying networks," Wireless Commun. Mobile Comput., Sep. 2012
9. Yu F. R., Tang H., Bu S., and Zheng D., "Security and Quality of Service (QoS) co-design in cooperative mobile ad hoc networks," EURASIP J. Wireless Commun. Netw., vol. 2013, pp. 188-190, Jul. 2013.
10. Sarvanko H., Hyhty M., Katz M. and Fitzek F., "Distributed resources in wireless networks: Discovery and cooperative uses," in 4th ERCIM eMobility Workshop in conjunction with WWIC'10, 2010.
11. J. Lopez, R. Roman, I. Agudo, and C. F. Gago, "Trust management systems for wireless sensor networks: Best practices", Computer. Communication. vol. 33, no. 9, pp. 1086-1093, 2010.
12. H. Deng, Y. Yang, G. Jin, R. Xu, and W. Shi, "Building a trust-aware dynamic routing solution for wireless sensor neworks," in Proc. IEEE GLOBECOM Workshop,pp. 153-157, Dec-2010.
13. J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," IEEE Commun. Surv. Tuts., vol. 13, no. 4, pp. 562-583, Fourth Quarter, 2011.
14. M. A. Ayachi, C. Bidan, T. Abbes and A. Bouhoula, "Misbehavior detection using implicit trust relations in the AODV routing protocol," in International Symposium on Trusted Computing and Communications, Trustcom, pp. 802-808, 2009.
15. S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 3, pp. 1025-1036, Mar. 2011.
16. Xia H., JiaZ.,Ju L, X. Li, and Y. Zhu, "A subjective trust management model with multiple decision factors for MANET based on AHP and fuzzy logic rules", in Proc. IEEE/ACM Green Computer Communication., 2011.
17. J. Hassan, H. Sirisena, and B. Landfeldt, "Trust-based fast authentication for multiowner wireless networks," IEEE Trans. Mobile Comput., vol. 7, no. 2, pp. 247-261, 2008.
18. Q. Nguyen, L. Lamont and P. C. Mason, "On trust evaluation in mobile ad hoc networks," Security and privacy in mobile information and communication systems, Springer, vol. 17, pp. 1-13, 2009.
19. Boukerch A., L. Xu and K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks," Computer Communications, no. 30, pp. 2413-2427, 2007.
20. Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Wireless Networks, 11(1-2):21-38, 2005.
21. L. Kagal, T. Finin and A. Joshi, "Trust-based security in pervasive computing environments," IEEE Computer, vol. 34, pp. 154-157, 2001.
22. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561, Jul. 2003.
23. Sun .Y,W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 305-317, Feb. 2006.
24. Z. Haas and P. Papadimitratos, "Secure routing for mobile ad hoc networks", In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), Jan. 2002.
25. S. Yi, P. Naldurg, and R. Kravets, "Security-aware ad-hoc routing for wireless networks", In MobiHOC Poster Session, 2001.
26. Y.C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks", In Proc. 4th IEEE Workshop Mobile Computing Syst. Applications, June 2002.
27. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. BeldingRoyer, "Authenticated routing for ad hoc networks", IEEE Journal Selective Areas Communincation, Vol. 2, No. 1, Mar. 2005.
28. M. Yu, S. Kulkarni, and P. Lau, "A new secure routing protocol to defend Byzantine attacks for ad hoc networks",In Proc. IEEE Int. Conf. Networks (ICON'05), vol. 2, pp. 1126-1131, Nov. 2005, Kuala Lumpur, Malaysia.
29. D. Boneh, C. Gentry, H. Shacham, and B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps", in Proc. Advances in Cryptology - Eurocrypt-03, LNCS, 2003.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Developments of E-Government on Smart Government and the Risks and Warnings about the Applications and Programs

By Dr. Yasser Elmalik & Ahmed Seleman
Bisha University, Saudi Arabia

Abstract- Smart government is a model of evolution of egovernment, e-government in general is government public services on the Internet through Web portals applications (Life Events & Business Episodes), smart government and its applications come to complement what has been built and invest in cross closer to citizen on the one hand, the direct and simultaneous interaction with data deployed in society and economic, social and security and its components on the other. Instruments Smart sensors have evolved (Smart Sensors) which are connected to the Internet, such as security surveillance cameras in cities and climate sensors and measuring energy and power associated with the Internet network government consumption.

Smart government is the electronic services digital means for us dispense with many things, including the excessive use of paper and time lost in follow-up transactions between departments is an excellent step in the evolution of government services in the state system and the speed of completion of transactions and customer convenience in first class, which he could accomplish his business through his Smartphone without the need to go to the place of the government department and wait.

GJCST-E Classification : *K.5.2, C.3*

Strictly as per the compliance and regulations of:

Developments of E-Government on Smart Government and the Risks and Warnings about the Applications and Programs

Dr. Yasser Elmalik [α] & Ahmed Seleman [σ]

Abstract- Smart government is a model of evolution of e-government, e-government in general is government public services on the Internet through Web portals applications (Life Events & Business Episodes), smart government and its applications come to complement what has been built and invest in cross closer to citizen on the one hand, the direct and simultaneous interaction with data deployed in society and economic, social and security and its components on the other. Instruments Smart sensors have evolved (Smart Sensors) which are connected to the Internet, such as security surveillance cameras in cities and climate sensors and measuring energy and power associated with the Internet network government consumption.

Smart government is the electronic services digital means for us dispense with many things, including the excessive use of paper and time lost in follow-up transactions between departments is an excellent step in the evolution of government services in the state system and the speed of completion of transactions and customer convenience in first class, which he could accomplish his business through his Smartphone without the need to go to the place of the government department and wait.

I. Introduction

The shift from E-government to smart government needs a lot of continuous work to ensure the readiness of services that will be available to users and requires the administrator to understand the digital needs and how they are applied and completed. Therefore, the study of those needs and understand well the government departments Developing or owning a Smartphone application to enter the stage of smart government, if the department does not offer its services properly through electronic pages it is difficult to switch to smart services without going through several stages of development.

Government departments and institutions should first focus on electronic services available on the network, or even non-ready at the moment and develop properly and the use of new technologies and standards, taking into account ease of use and user experience.

The provision of services through several channels including websites, smart phones and text messages and even television.

New developments to lead to a lot of amendments to the e-government model, which is suitable to the harmonic framework updates Data input to the electronic government (Government Interoperability Framework) to match sources and format the new data with back-end systems to the government.

Fig. 1: Electronic government needs

Author α σ: Kingdom of Saudi Arabia, Ministry of Education, Bisha University PhD in Computer Science, Omdurman Islamic University M.sc in Information Technology, Newcastle (USA). M.sc in Information Technology, the National Ribat University. e-mail: Dr.yaserking@hotmail.com

In order to e-government turn into a smart government it will be working on several fronts technical and administrative, including

- Create a framework for smart government services on mobile phones and how they are assembled and endorsement serve individuals. Smart government services may be provided through a government application of a unified public service it be an element is added or removed so huge or deliberate central government to publish guidance and general guidance on how to develop services and technology to her favourite and how to design and contents of the service and how to protect service (security insurance application and confidential information) and then leave it for devices and various ministries in order to do internally developed smart government services of their own.
- Develop special guidelines smart applications and templates (Smart Government Apps Guidelines). Most governments have developed this special launching governmental Internet sites instructions but so far those governments did not work on the same application-level smart note that the time for citizen interaction with the mobile device far exceeds the time consumed by that citizen interacting with the browsers on desktop devices.
- Work on the huge open government data (Government Big Data) to promote the launch of smart applications around by programmers in the community. An example of this is that the government opens Data trade and economic transactions and the Data and transportation and communication facilities and Data import and export raw form and comes from the programming smart applications on the phones for trader's service and provide them with information to benefit them in their trade with trading partners in other countries.
- Create data government sensor networks to collect information in real and timely information about security, transport, health, climate, environment and other sectors. With what it means to allocate computing power and Data Centre private to receive process and store the sensor Data.

II. Wireless Networking Problems

In the development researcher discusses a range of topics including

- **Application Programming Interfaces (APIs)**

Using application programming interfaces (APIs) to make smart government services or functions are available for use by other applications. Thanks to Smartphone, new services replace traditional

- **Applications and web applications.**

Development of new applications quickly by blending existing services and capabilities in creative ways, is no longer applicable and single user interface, but several interfaces. These interfaces can be built using different techniques, to target different types of users, and can also be built from several interested parties before doing so. In order to enable multiple interfaces, it became the application programming interface (API) base interface for applications, whether old or new. As it has become the new application programming interfaces distribution channel for government services.

The ability to provide basic functional properties of the work of the APIs, the government entity itself turn into a platform. And here is not enough to provide a set of APIs, it must be those interfaces reliable, scalable and secure at the same time.

- **Security measures relating to the user**

When you provide smart services to the public, should not be overlooked any of the security risks, whether related to the institution or the user, when the development of smart services, taking into account the privacy and security issues related to the participation of sensitive information while using those services. With regard to the user, the service provider must (the government agency, for example) to ensure safe use of the service by the public.

III. Protection for Wireless Network

a) Security Guidance for encrypting smart applications:

When you develop smart applications, you must take many issues into consideration, including: the use of properties, and the presence of sensitive data, and share information. It should take the necessary security measures in this regard, starting from the development stage, depending on the level of security necessary for each individual case. Review the instructions below and a number of thorny issues related to security in the development of smart applications.

Protect sensitive data:

- Make sure the rating data stored according to the degree of sensitivity, and then to take security measures accordingly. Perform data processing and storage operations in accordance with those classifications.
- Store sensitive data on the server (server) rather than stored on the client machine, whenever possible, If it is necessary to store data on the client machine, use the application programming interface (API) to encrypt files, which are provided by the operating system, or through other reliable source.
- should always make sure sensitive stored data encryption, as well as the data in the cache (cached).
- In some cases, you can put restrictions on the data as a precautionary measure (to use in a different geographic location, for example).
- For safety reasons, reveal the minimum of user data; namely select the data that will be of benefit to the user, and shapes the rest of the data.

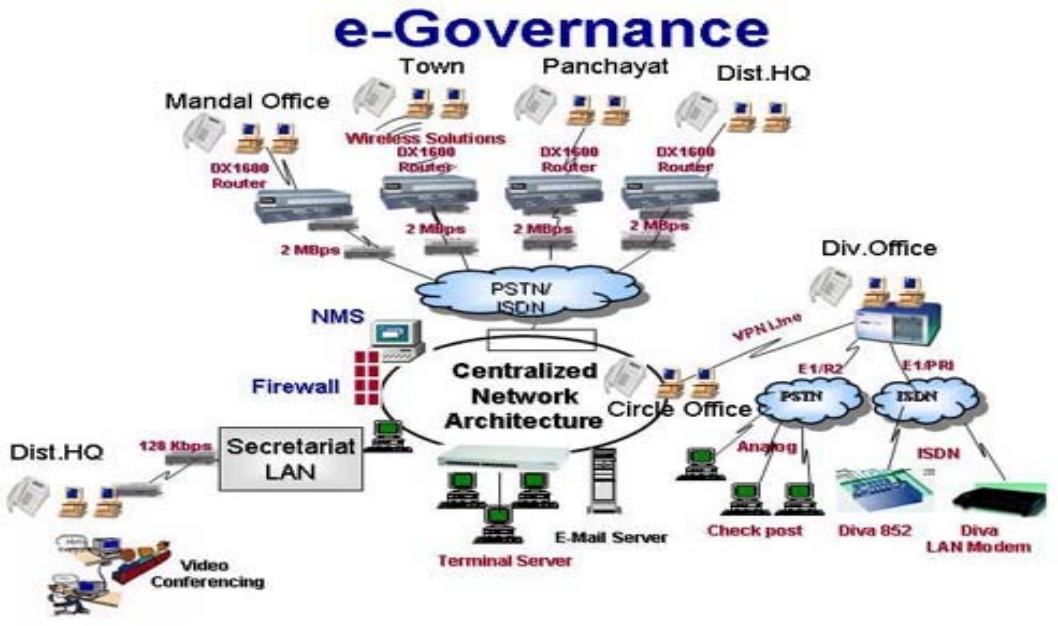


Fig. 2 : E-government services

b) Researcher discusses the data protection during transport

Always assumed that the network layer is safe, and on this basis, has taken the necessary precautions.

- When a specific application to send sensitive data wired or wirelessly, makes use of a secure channel for data transfer between two parties (SSL / TLS) is a prerequisite.
- Use strong encryption algorithms and long keys.
- Ensure that the user interface shows whether the certificates that are used are valid or not.

c) Usage Analysis and Risk

- Navigate through the application of the analysis of the basic functions and the method of work. Select network interfaces that the application uses, and select protocols and security standards it uses.
- Select the properties of the machine that could application and opportunities for piracy and potential uses (such as camera, GPS, etc.) Check out how he believes in the application of payment information, if it provides this property.
- Identify other applications that interact with smart service, and select applications that may harm the safety and privacy standards.
- Ensure that the source code analysis (source code) for the application, and to identify weaknesses.
- Check out how they carried out the ratification of the user in the application process, and identified potential risks.
- Analyze the data stored within the application process. See the algorithms used in the encryption, and whether vulnerable to known issues.
- Verify that the data that is stored in the cache memory type, and whether sensitive information was stored in the memory.
- tested the application against the "breakthrough talks" attacks in which the attacker between the interlocutors in the network sneaking unbeknownst to either of them (man-in-the-middle) to analyze the possible interventions in the application.
- Check if the sensitive data being leaked to the log files (log files).
- Be sure to maintain the security of the destination server, not the client-side only.

d) Risks from the perspective of the research

Researcher discusses a range of risks and warnings about the applications and programs Use smart devices multiple types of applications, the original or private systems and programs. From time to time, these applications and programs make updates or download programs requested in order to add new functionality to it, as is the case in smart phones and tablets. However, these programs and applications may contain vulnerabilities or malicious code. There are many risks associated with the programs and applications can be listed as follows:

Applications threats and cipher software and operating systems Installed programs contain smart devices based on certain codes unauthorized procedures.

This code can penetrate the devices by which programs are updated or installed, or applications that are downloaded, or instant messaging, or e-mail.

This code has been inconsistent with the normal operation of the device, or causes the risks of theft or loss of data. Operating systems as well as the risk of a

similar, but they may cause greater problems because their influence and ability on the device and the data is much larger than the impact of applications.

e) Internet threats

When the devices connected to the Internet, you may reach them malicious code through HTML applications or JavaScript or Flash, or other sources through Web pages that are visited. It may also cause weakness browsers in exposing the devices to the risk of external codes. Take preventive measures such as avoiding users' access to unreliable sites through the use of checks or security certificates at the enterprise level and the use of modern versions of web browsers provides a greater degree of safety. You must modify the settings to suit the security policies in the enterprise. You must make sure not to enter into official websites, but through the means of secure communication. The devices Security Administration is critical of the security structure of the whole enterprise, the risks related devices threaten as well as desktop computers, databases and e-mail devices and servers, networks, and may cause the arrival of unauthorized persons to sensitive data, or it may cause slow systems. Moreover, because of the mobile nature, the smart devices are prone to loss or theft of data

IV. Recommendations

- Data encryption in all communication process to reduce risk wherever possible application of it. However, the encryption method must be compatible with the Federal Information Processing Standard System (FIPS) which does not possess a lot of hardware at the moment. For devices not compliant with FIPS system, institutions must use FIPS 140-2 sandbox security mechanism.
- Provide and encourage the use of formal communication network via virtual private networks (VPN) in high-risk situations, where the authentication and encryption, confidentiality and integrity of secure data across these networks operations.
- must be trained users to be very careful for their effective control on the devices, and that is to give them instructions about the potential for the loss of hardware hazards.
- Ensure that the smart devices do not allow the transaction if we're not connected to the Internet (offline) or to store transaction data for later use. Applications should require it relates to the Internet to complete the transaction.
- For secure smart devices and applications, make sure you download versions concerning the types of new threats and risks updates.
- Do not have to deal with payment applications other than authorized or can exchange data with applications.

References Références Referencias

1. United Nations Department of Economic and Social Affairs. "United Nations E-Government Survey 2014" (PDF). UN. Retrieved 2014-09-16.
2. Jump up ^ OECD. The e-government imperative: main findings, Policy Brief, Public Affairs Division, Public Affairs and Communications Directorate, OECD, 2003 .
3. Jump up ^ Grima-Izquierdo, C. (2010). A generic architecture for e-Government and E-Democracy: requirements, design and security risk analysis. Ed. LAP Publishing.
4. China: The Next, Science Superpower, (2006.).
5. Essam Abdel Fattah rain, e-government between theory and practice, the new University House, Alozartih 2008.
6. Abdel-Fattah Bayoumi Hijazi, e-government and legal system, the university thought Dar,..

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Energy Efficient Elliptical Curve based Spherical Grid Routing Protocol for Wireless Sensor Networks

By Jai Prakash Prasad & Dr. Suresh Chandra Mohan
Visvesvaraya Technological University, India

Abstract- The Wireless Sensor Network (WSN) is a collection of no. of mobile nodes which communicate through wireless channel without any existing network infrastructure. Because the resource constrained nature of WSN a data packet routing requires multiple hops to exchange data across the network. In order to facilitate communication within the network, a secure energy efficient routing protocol is used to discover routes between nodes. The proposed energy efficient elliptical curve based spherical grid routing protocol for WSN provides correct and efficient route establishment between a pair of nodes so that data packets can be delivered in time to the destination. Secure route construction can be done with optimized WSN performance matrices such as packet delivery ratio, throughput, minimum energy consumptions, communication overheads & end to end delay. This proposed algorithm evaluates Spherical grid routing protocols for wireless sensor networks protocol while varying no. of nodes and pause time and results are compared with few existing routing protocols using network simulator.

Keywords: wireless sensor network, spherical GRID routing, energy efficient, packet delivery ratio, throughput. multi-tier spherical GRID, elliptical curve cryptography, scalability, routing.

GJCST-E Classification : C.2.2, I.2.9, C.2.1

Strictly as per the compliance and regulations of:

Energy Efficient Elliptical Curve based Spherical Grid Routing Protocol for Wireless Sensor Networks

Jai Prakash Prasad [α] & Dr. Suresh Chandra Mohan [σ]

Abstract- The Wireless Sensor Network (WSN) is a collection of no. of mobile nodes which communicate through wireless channel without any existing network infrastructure. Because the resource constrained nature of WSN a data packet routing requires multiple hops to exchange data across the network. In order to facilitate communication within the network, a secure energy efficient routing protocol is used to discover routes between nodes. The proposed energy efficient elliptical curve based spherical grid routing protocol for WSN provides correct and efficient route establishment between a pair of nodes so that data packets can be delivered in time to the destination. Secure route construction can be done with optimized WSN performance matrices such as packet delivery ratio, throughput, minimum energy consumptions, communication overheads & end to end delay. This proposed algorithm evaluates Spherical grid routing protocols for wireless sensor networks protocol while varying no. of nodes and pause time and results are compared with few existing routing protocols using network simulator.

Keywords: wireless sensor network, spherical GRID routing, energy efficient, packet delivery ratio, throughput. multi-tier spherical GRID, elliptical curve cryptography, scalability, routing.

I. Introduction

Wireless Sensor Network consists of no. of sensor nodes where nodes are deployed in a region to monitor its environment. Each sensor nodes consists of Microcontroller, internal & external memory, antennas, sensor and batteries as its main components to perform a specific task. Each sensor node senses its input attributes process the raw data & converts it into digital data format and then forward the data through chain of network using optimized routing scheme till the data reaches to its correct destination.

When the data is travelling through optimized routing path then there are chances of data packet to compromise from its authenticity, confidentiality, and integrity before it reaches to the destination. Therefore to overcome such threats which may exist in WSN depending on its application, there is requirement of strong cryptographic technique to counter. Wireless sensor nodes resources have its own constrained in terms of limited computational speed & battery backup. There exist plenty of energy efficient secure & routing algorithms such as LEACH, PEGASIS, TEEN, APTEEN, GBDD, TTDD, DES, AES, RSA, DSA, Elgamal encryption etc has achieved appreciable popularity for improved performance efficiency. However all the existing protocol has its own limitations and their drawbacks which has been studied & analyzed in detail for further research improvement & development in the field of wireless sensor networks.

Wireless Data Communication poses some kind of threats due to its open environment communication. To avoid compromise of data security it is required to maintain the authenticity, confidentiality and integrity of data. The elliptical curve cryptosystem provide speedy security mechanism compare to other type of public key cryptosystem and used in constrained environment conditions. Elliptical Curve Cryptography provides advantage of smaller key size that result in to faster computations, lower power consumption with savings of memory and bandwidth that makes ECC a fast, flexible, low cost security algorithm suitable for constrained environment.

Wireless Sensor Network can be deployed for Tele communication connectivity between various regions of all over the world. The modeling and placement of Wireless sensor nodes across various parts of world region for the coverage of whole world forms a cluster of networks which appears into spherical shape as shown in figure-1.

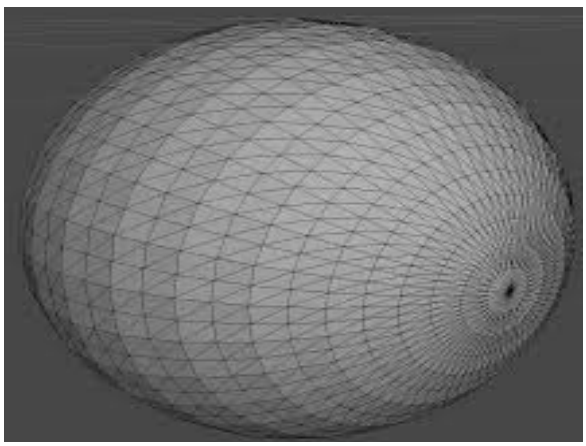


Fig.1 : Globe coverage structure using WSN's

Author α: Research Scholar, Visvesvaraya Technological University, Research Resource Centre, Belgaum, Karnataka, India.
e-mail: jaiaasu@gmail.com
Author σ: Professor, Dept. of ECE, BIET, Davangere, Karnataka, India.

The WSN find applications in,

- To monitor

Environment, parking & garden area, animals & birds, forest area, border area, Patient Health, Weather & Temp

- To Track

Nuclear mission, army movements, Production, Business, enemy

II. WSN Security & Routing: A Review

In cryptography the plaintext message content before it is sent out over the infrastructure network is encrypted, which becomes the cipher-text. At the destination side in order to read the plaintext, the cipher-text has to be decrypted. The application of wireless sensor network is wide spreading. The WSN are having limited power source, which required an ultimate power efficient routing and security protocol. There are several asymmetric cryptography schemes that are used to provide the security services. The Elliptic Curve Cryptography (ECC) performance is better for low power implementation applications. To ensure the communication network function correctly and safely, there are mainly four security requirements of WSN i.e. Authenticity, Integrity, Confidentiality, Availability.

In Wireless communication routing path is set up by establishing in either of three ways namely reactive, proactive and hybrid. Reactive protocols decide the routing path when they are ready with information to transmit. Proactive protocols calculate all the routes in advance and maintain the records in a routing table of each sensor node. If there is change in the route, the changes is updated throughout the network and due to this region proactive protocol are not suitable for WSN. Hybrid protocols join the idea of proactive and reactive protocols. Some of the routing protocols are discussed below.

Hierarchical protocols: Such protocols are suitable for higher scalability. Hierarchical protocols functions in two tier, first tier is used to decide about cluster-heads and the other tier is used for data routing. This protocol is more energy efficient and improves network scalability, lifetime and quality of service.

Location based Protocols: This protocol used nodes location information to decide the closeness among two or more nodes to estimate the energy consumptions. Two methods are used to determine the sensor node location, first one which calculates the coordinates of the neighbouring node and second one uses the global positioning system.

Ad-hoc on demand distance vector (AODV) Protocol: AODV is the energy efficient and shortest path routing algorithm widely being used for wireless network. It uses methods of path discovery and maintenance. AODV form routes between sensor nodes only when they are needed.

III. Elliptical Curve Cryptography

Elliptical Curve Cryptography (ECC) is suited for WSN applications. The benefit of this technique is that they uses smaller size key which need less storage, less bandwidth and less energy, thereby reducing processing and communication overhead, which is ideal for energy-constrained sensor nodes. An elliptic curve is the points in the *x-y* plane that satisfy an algebraic equation $y^2 = x^3 + bx + c$ of the form. The selection of values of *b* and *c* result different elliptic curves. The value of *x*, *y*, *b* and c are over the finite fields of F_P are commonly used in practice. An example of elliptic curve for Point addition and Point doubling is as shown below in Figure 2&3.

The equation of the elliptic curve over Prime field F_p is defined as:

$y^2 \bmod p = (x^3 + ax + b) \bmod p$; Where: $(4a^3 + 27b^2) \bmod p \neq 0$

$x, y, a, b \in [0, p-1]$

Point addition for EC over F_p

$x_R = (\lambda^2 - x_P - x_Q) \bmod p$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$

Where: $\lambda = ((y_Q - y_P)/(x_Q - x_P)) \bmod p$

Point doubling for EC over F_P

$x_R = (\lambda^2 - 2x_P) \bmod p$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$

Where: $\lambda = ((3x^2_P + a)/ (2y_P)) \bmod p$

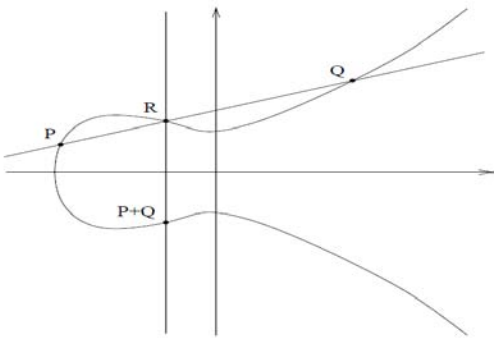


Fig.2 : Adding two points on elliptic curve

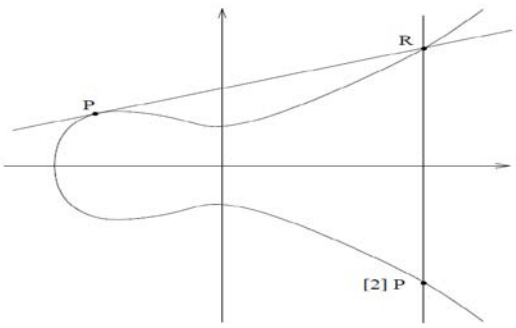


Fig.3 : Doubling a point on an elliptic curve

Elliptic Curve Cryptography technique consists of three parts: Key Generation, Encryption and Decryption. The following required inputs parameters are listed below,

1. Finite Prime Range
2. Parameters of elliptic curve equation
3. Generator Point
4. Random Numbers
5. Receiver's Public Key
6. Receiver's Private Key
7. Plain text File
8. Cipher text File

Example of an Elliptic Curve Group over F_p

As a very small example, an elliptic curve over the field F_{23} has been considered. With a = 9 and b =17, the elliptic curve equation is: $y^2 = x^3 + 9x + 17$.

For example the point (3, 5) satisfies this equation since:

$$5^2 \bmod 23 = 3^3 + 9*3 + 17 \bmod 23$$

$$25 \bmod 23 = 71 \bmod 23$$

$$2 = 2$$

The points which satisfy this equation are:
(1, 2), (1, 21), (3, 5), (3, 18), (4, 5), (4, 18), (5, 7), (5 ,16), (7, 3), (7 ,20), (8, 7), (8, 16), (10, 7), (10, 16), (12, 6), (12, 17), (13, 10), (13, 13), (14, 9), (14, 14), (15, 10), (15, 13), (16, 5), (16, 18), (17, 23), (18, 10), (18, 13), (19, 3), (19, 20), (20, 3), (20, 20).
The points are plotted in figure 4.

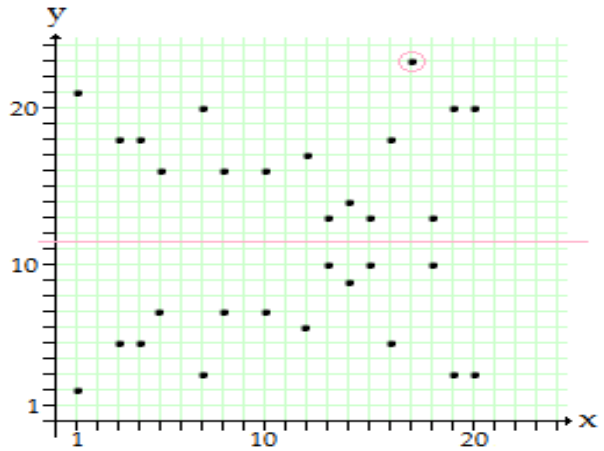


Fig. 4 : A plot on $y^2 \bmod 23 = x^3 + 9x + 17 \bmod 23$

IV. Spherical Coordinates for Ecmsgr

The proposed ECMSGR protocol is based on the concept of Cartesian Coordinates system which is consists of four basic elements: a) Choice of origin b) Choice of axes c) Choice of positive direction for each axis d) Choice of unit vectors for each axis.

Spherical Coordinates:

In the spherical coordinate system, as shown in figure 5 a point P(x, y, z) whose Cartesian coordinates are (x, y, z), is described by an ordered triple (ρ, θ, φ), where

$$\rho > 0, 0 \leq \theta \leq 2\pi, 0 \leq \varphi \leq \pi$$

are defined as follows.

- ρ = dist(P, O)
- θ is defined as the angle from zx-plane, counter-clockwise, to the half-plane originating from z-axis and containing P.
- φ = angle from positive z – axis to vector $\overrightarrow{OP}$

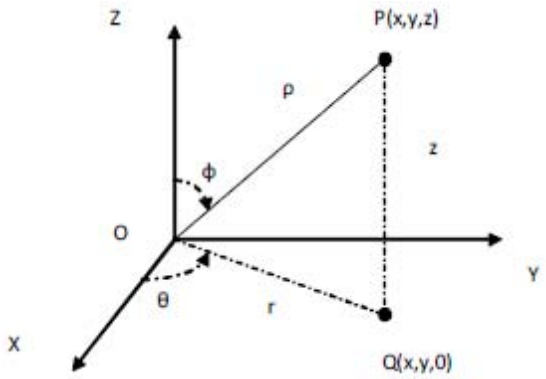


Fig. 5 : Spherical Cartesian System

Note that when P is on z – axis, φ = 0, and φ increases from 0 to $\frac{\pi}{2}$ as P moves closer to xy – plane, and φ keeps increasing as P moves below xy – plane, and φ reaches the maximum valueπ when P is on the negative z – axis.

Conversion formula (rectangular ↔ cylindrical ↔ spherical)

$$x = r\cos\theta = \rho\sin\varphi\cos\theta$$

$$y = r\sin\theta = \rho\sin\varphi\sin\theta$$

$$z = r\cot\varphi = \rho\cos\varphi$$

$$\rho = \sqrt{x^2 + y^2 + z^2}$$

$$\tan\theta = \frac{y}{z}$$

$$\cos\varphi = \frac{z}{\sqrt{x^2+y^2+z^2}}$$

To determine θ, we need to consider which quadrant the point is in. θ can be more precisely determined as,

$$\theta = \begin{cases} \arctan\frac{y}{x}, & \text{if } x > 0 \\ \arctan\frac{y}{x} + \pi, & \text{if } x > 0 \\ \frac{\pi}{2}, & \text{if } x = 0, y > 0 \\ -\frac{\pi}{2}, & \text{if } x = 0, y < 0 \end{cases}$$

φ can be uniquely determined as,

$$\varphi = \arccos\left(\frac{z}{\sqrt{x^2+y^2+z^2}}\right)$$

The coordinate system formation of the spherical grids is shown in figure 6.

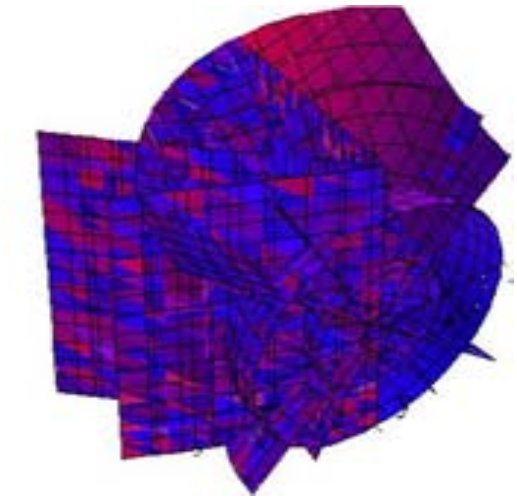


Fig.6 : A Spherical Grid

V. Elliptical Curve based Multi-tier Spherical Grid Routing (ECMSGR): A Proposed Method

The several sensor nodes are uniformly distributed across a field to form wireless sensor network for the secure routing of data packet between source and destination. Each sensor node senses its input attribute and before its send the data packet to its neighbor node it forms a routing path in spherical grid fashion with proper coordination among no. of sensor nodes. For the uniform utilization of sensor nodes, each sensor node is checked for remains energy level and no. of times used for path formation by the neighbouring sensor node as shown in figure.

In WSN multi-tier spherical grid routing path formation between two or more sensor node is calculated by determining previous and next sensor node angular position such that path formation will be in spherical fashion between starting node and destination node as shown in figure 7. Source as indication in figure 7 is sensed by a sensor node near to it. The sensed node now decides about choosing second next node with required angle and second node select third node such that the routing path formation between source and destination takes spherical shape. The red dot represent one tier spherical grid and blue dot represent second tier and so on routing path formation takes place.

The required angular position between nodes formation is shown in figure 8. The elliptical curve based multi-tier formation of spherical grid routing to cover very large area with effective & optimized utilization of sensor node is represented by figure 9.

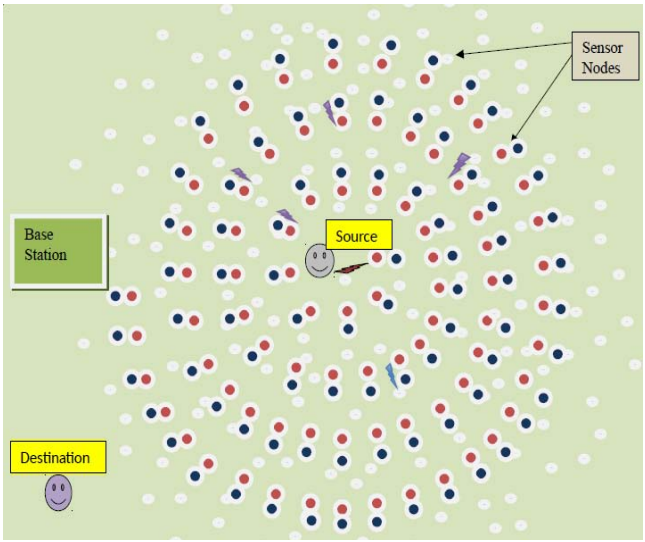


Fig.7 : Elliptical curve based Multi Tier Spherical Grid

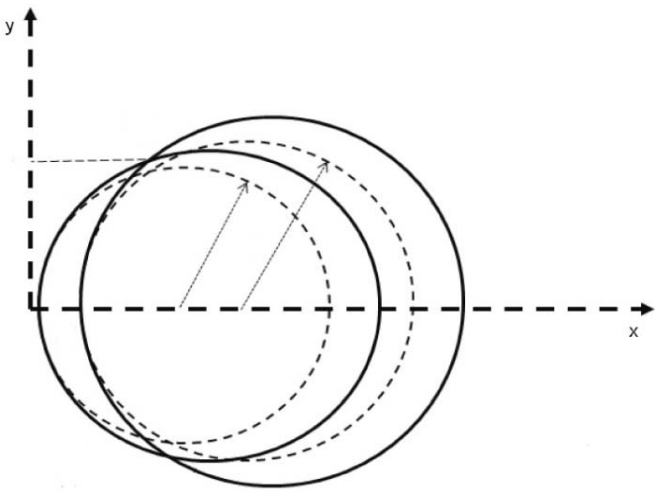


Fig. 8 : Formation of angular position between two nodes

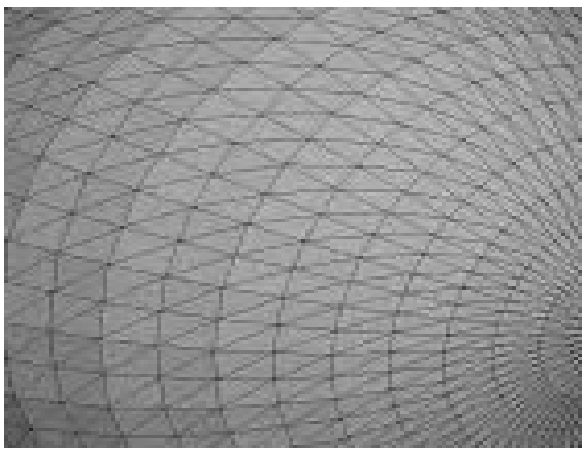


Fig. 9 : Spherical Grid formation over wide area

VI. Results & Discussions

The Proposed protocol ECMSGR is compared with LEACH and GRID protocol in network simulator 2 environment to evaluate the performance metric such packet delivery ratio, throughput, communication overhead, end-end delay and power consumption. The table I represent simulation parameter set up for NS2.

Table I : Simulation parameters for WSN

Simulation Parameters	Value
Channel type	Wireless Channel
Radio-propagation model	Propagation/Two Ray Ground
Network interface type	Phy /WirelessPhy
MAC type	Mac/802_11
Interface queue type	Queue/DropTail /PriQueue
Link layer type	LL
Antenna model	Antenna/Omni Antenna
Max packet in IFQ	50
Number of mobile nodes	16/25/36/49/98/196
Routing protocol	AODV/DSR/DSDV
X dimension of topography	4000
Y dimension of topography	4000
Time of simulation end	20/40/60/80/100
Initial energy in Joules	100
Network Type	Mobile
Connection Pattern	Random
Packet Size	512 bytes
Connection type	CBR/UDP/TCP

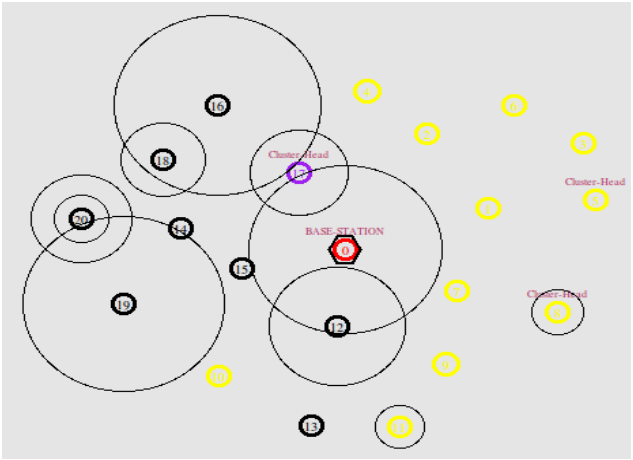


Fig.10 : M-LEACH Protocol

Figure 10 represent the M-LEACH protocol in which whole network is divided into no. of group of network. Each group of network selects their local cluster head for communication. Cluster heads are responsible for collection of data from their local sensor nodes and transmit to destination with the help of other cluster heads.

A large area is covered by a large number of sensor nodes which communicate with each other through short-range radios. Long-range data delivery is achieved by forwarding data across multiple hops. Each sensor is aware of its own location. However, mobile sinks may or may not know their own locations. When a stimulus appears, the sensors surrounding it collectively process the signal and one of them becomes the source to generate data reports. Sinks (users) query the network to collect sensing data. There can be multiple sinks moving around in the sensor field and the number of sinks may vary over time as shown in figure 11.

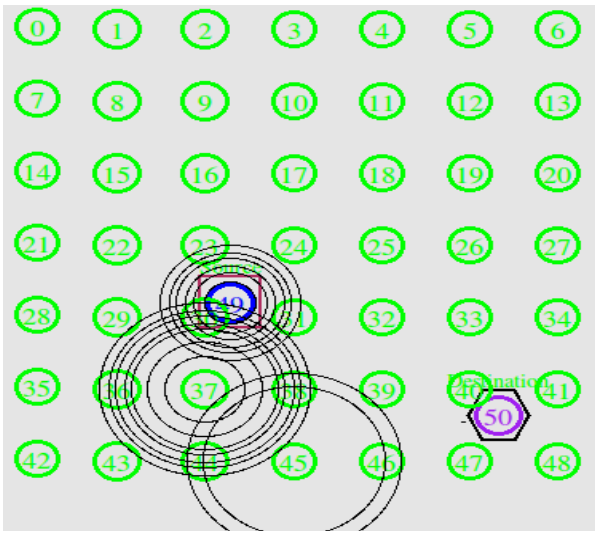


Fig.11 : 7 * 7 GBDD based Protocol

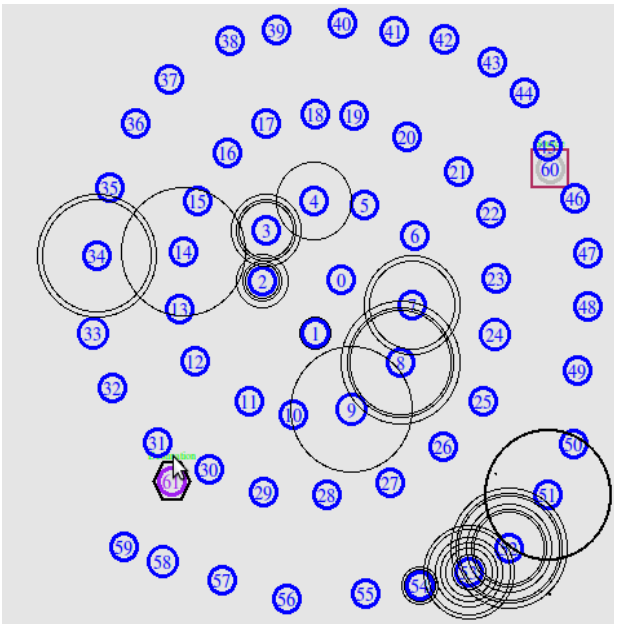


Fig.12 : ECMSGR Protocol

The ECMSGR Protocol as shown in figure 12 has been in discussed in section V. The experimental result of M-LEACH, 7*7 GBDD based protocol and ECMSGR for a network scenario as indicated in figure 10, 11& 12 and their result is compared for their transmitted packet, received packet, packet delivery ratio, average throughput and residual energy is shown in figure 13.

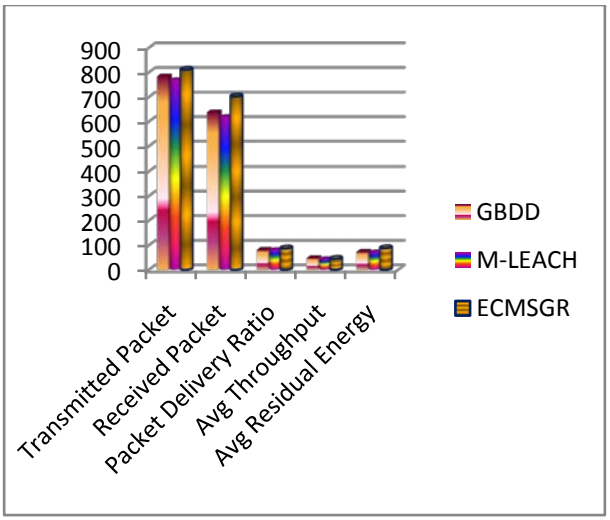


Fig.13 : A comparison between GBDD, M-LEACH & ECMSGR

VII. Conclusion

The proposed method ECMSGR provides a novel and an approach towards improvising potential WSN performance specially in terms of packet delivery ratio, throughput, communication overhead, end-end delay and power consumption. The network route formation as well as data transmission and its security are a major concern in the field of wireless sensor network. The ECMSGR protocol implementation and its performance compare to other related protocol is designed and analyzed to overcome some of the limitations of existing protocol using network simulator-2. The experimentation scenario and results shows that ECMSGR outperforms GBDD & M-LEACH. The ECMSGR protocol complexity increases when the network scalability increases at very large scale in the application of providing smart & secure gobal communication for data as well as voice communication to end users. ECC offer advantages of higher speeds, lower power consumption, and code size reductions. This concludes that ECC is best suited for wireless applications which demands speed, time and bandwidth. The results shows that optimal key generation time, encryption time and throughput using simulation. In this paper ECMSGR protocol gives an idea for researcher to explore further possible performance efficiency enhancement to offer better quality of services to provide communication coverage across globe.

References Références Referencias

1. W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocol for wireless micro sensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS)*, pp. 10–20, January 2000.
2. A. Manjeshwar, D.P. Agrawal, "TEEN: a protocol for enhanced efficiency in wireless sensor networks," in *Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing*, San Francisco, CA, April 2001.
3. S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in *Proceedings of the IEEE Aerospace*, vol. 3, pp. 1125–1130, 2002.
4. A. Manjeshwar and D. P. Agrawal, "APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in *Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing,* pp. 195–202, April 2002.
5. F. Ye, H. Luo, J. Cheng, S. Lu, and L. Zhang, "A two-tier data dissemination model for large-scale wireless sensor networks," in *MobiCom'02: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*, (Atlanta, USA), pp. 148–159, ACM, September 2002.
6. Ossama Younis and Sonia Fahmy, "HEED: A hybrid, Energy-efficient, Distributed Clustering Approach for Ad-hoc Networks," *in IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366-369, Oct-Dec 2004.
7. Ananthram Swami et al., "Wireless Sensor Networks: Signal Processing and Communication Perspectives", John Wiley, 2007.
8. T.P. Sharma, R.C. Joshi, Manoj Misra, "GBDD: Grid Based Data Dissemination in Wireless Sensor Networks," *In Proc. 16th International Conference on Advanced Computing and Communications (ADCOM 2008)*, Chennai, India, 2008, pp. 234-240.
9. Jamal N. Al-Karaki Raza Ul-Mustafa Ahmed E. Kamal, "Data Aggregation and Routing in Wireless Sensor Networks: Optimal And Heuristic Algorithms", *Computer Networks,* Volume 53, Issue 7, Pages 945–960, 13 May 2009.
10. Dragoş I. SĂcĂleanu, Dragoş M. Ofrim, Rodica Stoian, Vasile LĂzĂrescu, "Increasing lifetime in grid wireless sensor networks through routing algorithm and data aggregation techniques", *International Journal Of Communications*, Issue 4, Volume 5, 2011.
11. Neng-Chung Wang, Yung-Kuei Chiang, Chih-Hung Hsieh, and Young-Long Chen, "Grid-Based Data Aggregation for Wireless Sensor Networks", *Journal of Advances in Computer Networks*, Vol. 1, No. 4, December 2013.
12. Yung-Kuei Chiang, Neng-Chung Wang and Chih-Hung Hsieh, "A Cycle-Based Data Aggregation Scheme for Grid-Based Wireless Sensor Networks",

Sensors 2014, 14, 8447-8464; doi:10.3390/s140508447.
13. Hoffstein J, Pipher JC, Silverman JH. Elliptic curves and cryptography. An Introduction to Mathematical Cryptography. New York: Springer; 2014. p. 299–371.
14. Vigila SMC, Muneeswaran K. A new elliptic curve cryptosystem for securing sensitive data applications. International Journal of Electronic Security and Digital Forensics. 2013; 5(1):11–24.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Secure Elliptic Curve Digital Signature Algorithm for Internet of Things

By B. Sindhu & Dr. R. M. Noorullah
ABIT, JNTU Anantapur, India

Abstract- In the previous couple of years, the internet of things (IoT) is gaining additional and a lot of attention each within the academia and in the industrial worlds. A wide accepted notion of the internet of things (IoT) is stated the chance of militarization everyday objects with adequate technology to permit them to speak with alternative objects, identify themselves, or perhaps participate to distribute computing. These things are customarily stated as SO's (Smart Object), might be drawn as actual relics augmented with computing, communication, actuations and storing functionalities. Their importance resides within the capabilities they need to create physical environments "smart" therefore as to offer novel cyber physical service to individuals. smart Objects, that are vital elements of the IOT, are everyday objects that are equipped with hardware components like radio for communication, a CPU hardware to process tasks, sensors to be responsive to the globe within which they're located and to regulate it at a given instant. Even so, as sensible objects have restricted resource constraints to appoint sturdy protection mechanisms, they're at risk of subtle security attacks. For this reason, a smart authentication mechanism that considers every helpful resource constraints and safety is needed.

Keywords: elliptic curve digital signature algorithm, IOT, elliptic curve, ECDSA.

GJCST-E Classification : C.2.1, G.1.8, G.4

Strictly as per the compliance and regulations of:

Secure Elliptic Curve Digital Signature Algorithm for Internet of Things

B. Sindhu [α] & Dr. R. M. Noorullah [σ]

Abstract- In the previous couple of years, the internet of things (IoT) is gaining additional and a lot of attention each within the academia and in the industrial worlds. A wide accepted notion of the internet of things (IoT) is stated the chance of militarization everyday objects with adequate technology to permit them to speak with alternative objects, identify themselves, or perhaps participate to distribute computing. These things are customarily stated as SO's (Smart Object), might be drawn as actual relics augmented with computing, communication, actuations and storing functionalities. Their importance resides within the capabilities they need to create physical environments "smart" therefore as to offer novel cyber physical service to individuals. smart Objects, that are vital elements of the IOT, are everyday objects that are equipped with hardware components like radio for communication, a CPU hardware to process tasks, sensors to be responsive to the globe within which they're located and to regulate it at a given instant. Even so, as sensible objects have restricted resource constraints to appoint sturdy protection mechanisms, they're at risk of subtle security attacks. For this reason, a smart authentication mechanism that considers every helpful resource constraints and safety is needed. Our projected scheme uses the standards of Elliptic Curve digital signature scheme and evaluates consistently the potency of our scheme and observes that our scheme with a smaller key size and lesser infrastructure performs on par with the prevailing schemes while not compromising the security level.

Keywords: elliptic curve digital signature algorithm, IOT, elliptic curve, ECDSA.

I. Introduction

Digital signature algorithm is a public key cryptology algorithm designed to shield the genuineness of a digital document. A document is signed by a secret key to provide a sign and therefore the sign is verified against the message by a public key. Therefore any party can verify the signature with signer's public key. A legitimate digital signature offers a recipient reason to believe that the message was created by a identified sender who possesses the secret key, which it absolutely was not altered in transit.

Digital signatures are used wide in e-commerce applications, in banking applications, in software system distribution, and in different cases wherever jurisdiction is concerned and it's necessary to notice forgery or meddling. Thus it's crucial to use algorithms that are standardized by government organizations. Despite the fact that there are a varied range of digital signature algorithms in analysis literature, only three algorithms are standardized by the National Institute of Standards and Technology (NIST) and are wide employed in most industrial applications. These are the RSA, the DSA and therefore the ECDSA [7] [9]. The security of the DSA relies on the hardness of the discrete log problem on the multiplicative group of units on the finite field FP. The ECDSA is that the elliptic curve analogous of the DSA and its security is predicated on the distinct log drawback on the group of points on elliptic curve over a finite field. DSA and ECDSA are standardized and wide utilized in universe applications. Their securities are authenticated by the cryptology community for pretty much 20 years. It's affordable to believe that projected new DSA primarily based Elliptic Curve is secure. We have a tendency to confer the correctness of the projected algorithm and show that the security of the algorithm relies on the hardness of the discrete log problem within the underlined group.

II. Internet of Things

Internet of Things (IoT) was initially utilized in 1999 by British technology pioneer Kevin Ashton to explain a system within which objects in the physical world can be connected to the net by sensors. Ashton coined the term as an instance the ability of connecting Radio-Frequency Identification (RFID)tags utilized in corporate supply chains to the web so as to count and track product while not the necessity for human intervention [8]. Today, the net of Things has become a preferred term for describing situations during which internet connectivity and computing capability extend to a range of objects, devices, sensors, and everyday things. Whereas the term "Internet of Things" is comparatively new, the construct of mixing computers and networks to observe and control devices has been around for many years. The internet of Things (IoT) is what happens once every day normal objects have inter-connected microchips within them. These microchips facilitate not solely keep track of alternative objects, however several of those devices sense their

Author α: M.Tech Scholar, Department of CSE, ABIT, Kadapa. e-mail: basettysindhu2016@gmail.com
Author σ: principal & Professor, Department of CSE, ABIT, Kadapa, India. e-mail: noorullahrm@gmail.com

encompassing and report it to alternative machines likewise on the humans. Additionally known as M2M, standing for Machine to Machine, Machine to individual, individual to Machine or Machine to individual, the IoT showing intelligence connects humans, devices and systems. Experts term two divergent kinds of communication within the IoT: thing to individuals and individuals-to-individuals communication. Thing-to-individuals and individuals-to-thing communications cover variety of technologies and applications, whereby individuals act with things and contrariwise, as well as remote access to things by humans, and objects that endlessly report their standing, whereabouts and device information. Thing-to thing communications encompasses technologies and applications wherever in everyday objects and infrastructure act with the human. Objects will monitor alternative objects, take corrective actions and apprise or prompt humans as needed.

III. Elliptic Curve Arithmetic

ECC makes use of elliptic curves in which the variables and coefficients are restricted to elements of a finite field. There are two families of elliptic curves defined for use in cryptography: prime curves defined over odd prime field F_P and binary curves defined over Galois field $GF(2^m)$[1].

In Elliptic Curve Cryptography uses the following curve equation.

$y^2 = x^3 + ax + b$ where a and b are the constant with $4a^3 + 27b^2 \neq 0$

Cryptographic operations on elliptic curve over finite field are done using the coordinate points of the elliptic curve. Elliptic curve over finite field equation is given by:

$$y^2 = \{x^3 + ax + b\} \bmod p$$

Certain formula is defined for operation with the points [6]

a) Point Addition

The two point $P(x_1, y_1)$ and $Q(x_2, y_2)$ are distinct.

$P + Q = R(x_3, y_3)$ is given by the following calculation

$x_3 = \{\lambda^2 - x_1 - x_2\} \bmod p$

$y_3 = \{\lambda(x_1 - x_3) - y_1\} \bmod p$ where

$\lambda = \{(y_2-y_1)/(x_2-x_1)\} \bmod p$

b) Point Doubling

The two point $P(x_1, y_1)$ and $Q(x_2, y_2)$ overlap.

$P + Q = R(x_3, y_3)$ is given by the following calculation.

$x_3 = \{\lambda^2 - 2x_1\} \bmod p$

$y_3 = \{\lambda(x_1 - x_3) - y_1\} \bmod p$ where

$\lambda = \{(3x_1^2 + a)/2y_1\} \bmod p$

c) Point Multiplication

Let P be any point on the elliptic curve. Multiplication operation over P is defined by the repeated addition. $kP = P + P + P + \ldots +$ k times.

d) Elliptic Curve Cryptography

The use of Elliptic Curve Cryptography was initially suggested by Neal Koblitz [2] and Victor S. Miller [4]. Elliptic curve cryptosystems over finite field have some advantages like the key size can be much smaller compared to other cryptosystems like RSA. We have used Fixed and Variable Size Text Based Message Mapping Techniques [5] for message Encryption and decryption.

IV. Existing System

The scheme [3] is apt for a signer who has limited computing capability like, a signer using his smart Card which stocks his secret key.

a) Key-Pair Generation

Using random integer number d and generating point G, public key Q is computed as follows.

1) Select a random integer d in the interval [0, n-1]. 2) Compute $Q = d \times G$, obtained by point Multiplication. Q, G are points on the elliptic curve. 3) Now key-pair is (G, Q) where G is the Private Key and Q is the Public key.

b) Signature Generation

Signer uses parameters q, a, b, p, n, d and private key G, to sign a document or message M where a, b, p and q are constants in elliptic curve equation. To sign a message signer does the following:

1. Chooses a random integer k with $1 \leq k \leq n-1$.
2. Compute $k \times G = (x_1, y_1)$.
3. Compute hash value z of message M, $z = h^{-1}(M)^2$.
4. Compute $s = (z \times d) \times k^{-1} \bmod n$. If $s = 0$ then return to step 1.
5. Signature for the message M is (s, x_1).

c) Signature Verification

Authenticity of the received message can be verified by receiver exploiting the following steps:

1. First verify that s is integer in the interval $[1, n-1]$
2. Calculate hash z of the message/document M
3. Calculate the number $w = s^{-1} z \pmod n$
4. Using this number compute the point $(x, y) = w \times Q$ on the curve, and, finally, authenticate the signature by checking whether the equivalence x=x1 holds.

d) Possible Attack

The intruder can easily modify the message and append hash value of the modified message to the signature element. This modification cannot identify by the receiver.

The attack is described as follows.

1. Calculate hash z of the message m
2. Calculate z^{-1}
3. Calculate $s_1 = s \times (z^{-1})$
4. New/modified message m_1
5. Calculate hash z_1 of the message m_1
6. $s' = s_1 \times (Z_1)$
7. Signature for the message m1 is (s', x1).

V. Proposed System

Proposed scheme is secure when compare with existing system. This scheme is developed without modular inversion process in Signature Verification algorithms.

Notations:

To be appropriate in explanation of our work the elements are defined as

d: random integer number

T: private key

Q: Public key

m: message

k: Random number

H() : a secure one-way hash function

r, S_1, s_2: Signature elements

q: field order

FR: field representation

a, b: coefficients

G: Base point

n: Order of G

h: co-factor

a) Key Pair Generation

Key pair d and Q made by the Signer as follows

INPUT: D= (q, FR, a, b, G, n, h)

1. Choose a distinctive random number, j, within the interval [1, n-1]
2. Compute T ←(j×G) Choose a distinctive random number, d, within the interval [1, n-1]
3. Compute Q ←(d×T)
4. Return (Q, T, d)

OUTPUT: Q, T, d

b) Signature Generation

The signer can sign message m as follows

INPUT: D= (q, FR, a, b, G, n, h), d, m, T, Q

Begin

repeat

k = Random [1, 2,…, n-1]

P = k×T

c=X-Co-ordinate (P)

z = H (m) mod n

$S_1 = c \times k \times d \times T \bmod n$

$s_2 = (c + d^{-1}) z \times k \bmod n$

R = z×P

r = X-Co-ordinate(R)

until $r \neq 0$ and $s_1 \neq 0$ and $s_2 \neq 0$ return (r, S_1, s_2)

End

OUTPUT: Signature (r, S_1, s_2)

c) Signature Verification

To verify the signature (r,S_1, s_2) on message m, receiver does the following:

INPUT: D= (q, FR, a, b, G, n, h), Q, m, Signature (r, S_1, s_2)

Begin

If r, S1, s2 doesn't belongs to [1,2…, n-1] then

Return ("Reject the signature")

end if

z= H(m)

$U_1 = s_2 \times Q$

$U_2 = z \times S_1$

$W = U_1 - U_2$

v= X-Co-ordinate (W)

if v = r then

Return ("Accept the signature")

else

Return ("Reject the signature")

end if

end

OUTPUT: Acceptance or rejection of the signature.

d) Proof of Signature Verification

$S_1 = c \times k \times d \times T \bmod n$

$s_2 = (c + d^{-1}) z \times k \bmod n$

$W = U_1 - U_2$

$= s2Q - zS_1$

$= (c + d^{-1}) z \times k \times d \times T - z \times c \times k \times d \times T$

$= c \times z \times k \times d \times T + d^{-1} \times z \times k \times d \times T - z \times c \times k \times d \times T$

$= z \times k \times T$

$= R$

VI. Conclusion

The intruder can easily alter the message or document and replace the existing message hash value with modified message hash value. But in proposed scheme attacker may modify the message but attacker cannot substitute hash value of existing message with hash value of new message. If the message modified without appending the hash value then it rejects the Signature. Considering the above, our proposed digital signature scheme is more secure when compared to the existing scheme.

References Références Referencias

1. Hankerson Darrel, Alfred Menezes and Scott Vanstone,"Guide to Elliptic Curve Cryptography".

2. Koblitz N, "EllipticCurve Cryptosystems", Mathematics of Computation, 48, 1987, pp. 203-209.
3. Lamba Shweta,Monika Sharma, "An Efficient Elliptic Curve Digital Signature Algorithm (ECDSA),2013 International Conference on Machine Intelligence Research and Advancement(ICMIRA),2013,PP.179-183.
4. Miller V, "Uses of Elliptic Curve in Cryptography", Advances in Cryptography, Proceedings of Crypto'85, Lectures notes on Computer Sciences, 218, Springer-Verlag, 1986, pp. 417-426.
5. Muthukuru Jayabhaskar, Prof. Bachala Sathyanarayana, "Fixed and Variable Size Text Based Message Mapping Techniques Using ECC", Global Journal of Computer Science and Technology, Vol-12, Issue-3, Feb-2012, pp. 13-18.
6. Muthukuru Jayabhaskar, Prof. Bachala Sathyanarayana,"A Survey of Elliptic Curve Cryptography Implementation Approaches for Efficient Smart Card Processing", Global Journal of Computer Science and Technology, Vol-12, Issue-1, Jan-2012, pp. 7-12.
7. Seberry Jennifer, Vinhbuu To, Dongvu Tonien, "A new generic digital signature algorithm", 3(2),Apr-2011, pp.221-237.
8. Shelkikar Ravindra P, Nitin S.Wagh,"Review Paper Based On Women Tracking Device Using Concept Of Internet Of Things",IJAIEM, Vol-5,Issue-2, Feb-16,pp.63-73.
9. Tao LONG, Xiaoxia LIU, "Two Improvements to Digital Signature Scheme Based on the Elliptic Curve Cryptosystem", Proceedings of the 2009 International Workshop on Information Security and Application, Nov-2009.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 3 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

The Encryption Algorithms GOST-IDEA16-2 and GOST-RFWKIDEA16-2

By Gulom Tuychiev
National University of Uzbekistan, Uzbekistan

Abstract- In the paper created a block encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16- 2 based on networks IDEA16-2 and RFWKIDEA16-2, with the use the round function of the encryption algorithm GOST 28147-89. The block length of created block encryption algorithm is 128 bits, the number of rounds is 8, 12 and 16.

Keywords: GOST 28147-89, Lai-Massey scheme, round function, round keys, output transformation

GJCST-E Classification : G.4, E.3

Strictly as per the compliance and regulations of:

The Encryption Algorithms GOST-IDEA16-2 and GOST-RFWKIDEA16-2

Gulom Tuychiev

Abstract- **In the paper created a block encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 based on networks IDEA16-2 and RFWKIDEA16-2, with the use the round function of the encryption algorithm GOST 28147-89. The block length of created block encryption algorithm is 128 bits, the number of rounds is 8, 12 and 16**

Keywords: GOST 28147-89, Lai-Massey scheme, round function, round keys, output transformation.

I. Introduction

The encryption algorithm GOST 28147-89 is a standard encryption algorithm of the Russian Federation. It is based on a Feistel network. This encryption algorithm is suitable for hardware and software implementation, meets the necessary cryptographic requirements for resistance and, therefore, does not impose restrictions on the degree of secrecy of the information being protected. The algorithm implements the encryption of 64-bit blocks of data using the 256 bit key. In round functions used eight S-box of size 4x4 and operation of the cyclic shift by 11 bits. To date GOST 28147-89 is resistant to cryptographic attacks.

On the basis of encryption algorithm IDEA and scheme Lai-Massey developed the networks IDEA16-2 and RFWKIDEA16-2, consisting from two round function. In the networks IDEA16-2 and RFWKIDEA16-2, similarly as in the Feistel network, when it encryption and decryption using the same algorithm. In the networks used two round function having four input and output blocks and as the round function can use any transformation.

As the round function networks IDEA4-2 [1], RFWKIDEA4-2 [5], PES4-2 [6], RFWKPES4-2 [7], PES8-4 [2], RFWKPES8-4 [8] using the round function of the encryption algorithm GOST 28147-89 [4] created the encryption algorithm GOST28147-89-IDEA4-2 [9], GOST28147-89-RFWKIDEA4-2 [10], GOST28147-89-PES4-2 [11], GOST28147-89-RFWKPES4-2 [12], GOST28147-89-PES8-4 [13] and GOST28147-89-RFWKPES8-4 [13].

Author: Candidate technical science (Ph.d), the teacher of National University of Uzbekistan, Uzbekistan, Tashkent.
e- mail: blasterjon@gmail.com

In this paper, applying the round function of the encryption algorithm GOST 28147-89 as round functions of the networks IDEA16-2 [14] and RFWKIDEA16-2 [15], developed new encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2.

In the encryption algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 block length is 256 bits, the key length is changed from 256 bits to 1024 bits in increments of 128 bits and a number of rounds equal to 8, 12, 16, allowing the user depending on the degree of secrecy of information and speed of encryption to choose the number of rounds and key length. Below is the structure of the proposed encryption algorithm.

II. The Structure of the Encryption Algorithm Gost28147-89-Idea16-2

In the encryption algorithm GOST28147-89-IDEA16-2 the length of subblocks X^0, X^1, X^2,..., X^{15}, length of round keys $K_{24(i-1)}$, $K_{24(i-1)+1}$, $K_{24(i-1)+2}$, …, $K_{18(i-1)+15}$, $i=\overline{1...n+1}$, $K_{24(i-1)+16}$, $K_{24(i-1)+17}$, $K_{24(i-1)+18}$, …, $K_{24(i-1)+23}$ $i=\overline{1...n}$, K_{24n+16}, K_{24n+17}, K_{24n+18}, …, K_{24n+47} are equal to 8-bits. The length of the input and output blocks of round functions is 32 bits. This encryption algorithm round function GOST 28147-89 is applied twice and in each round function employed eight S-boxes, i.e. the total number of S-boxes is 16. The structure of the encryption algorithm GOST28147-89-PES16-2 is shown in Figure 1 and the S-boxes shown in Table 1.

Consider the round function block encryption algorithm GOST28147-89-IDEA16-2. First the 8-bit subblocks T^0, T^1, …, T^7 combined from 32-bit subblocks, i.e. $T_0 = T^0 \| T^1 \| T^2 \| T^3$, $T_1 = T^4 \| T^5 \| T^6 \| T^7$. Subblocks T_0, T_1 are summed round keys $K_{24(i-1)+16} \| K_{24(i-1)+17} \| K_{24(i-1)+18} \| K_{24(i-1)+19}$, $K_{24(i-1)+20} \| K_{24(i-1)+21} \| K_{24(i-1)+22} \| K_{24(i-1)+23}$ i.e.

$$S^0 = T_0 + (K_{24(i-1)+16} \| K_{24(i-1)+17} \| K_{24(i-1)+18} \| K_{24(i-1)+19}),$$

$$S^1 = T_1 + (K_{24(i-1)+20} \| K_{24(i-1)+21} \| K_{24(i-1)+22} \| K_{24(i-1)+23}).$$

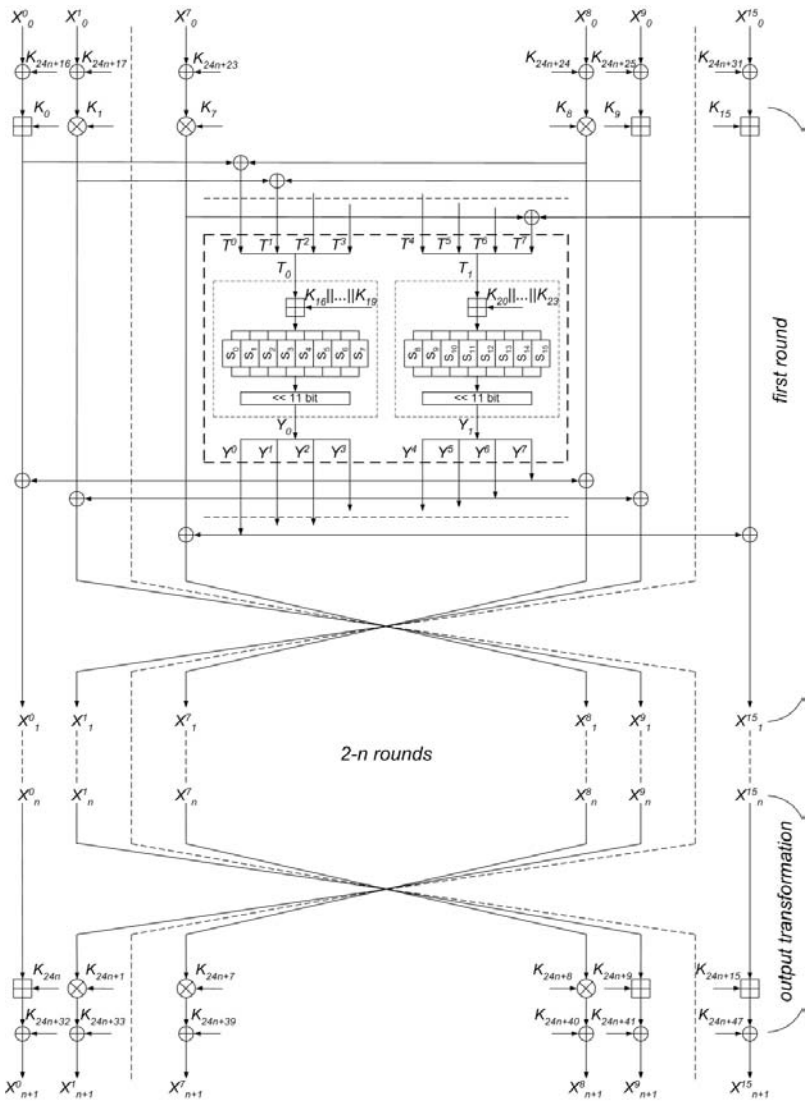


Figure 1 : The scheme n-rounded encryption algorithm GOST28147-89-IDEA16-2

Table 1 : The S-boxes of encryption algorithm GOST28147-89-RFWKPES4-2

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
S0	0x4	0x5	0xB	0x9	0xE	0x8	0xD	0x0	0x6	0xC	0xF	0x7	0x2	0x1	0x3	0xA
S1	0x5	0x4	0xA	0x8	0xF	0x9	0xC	0x1	0x7	0xD	0xE	0x6	0x3	0x0	0x2	0xB
S2	0xE	0xB	0x4	0x2	0xF	0x7	0xC	0x0	0x8	0x9	0xA	0xD	0x6	0x5	0x3	0x1
S3	0xF	0xA	0x5	0x3	0xE	0x6	0xD	0x1	0x9	0x8	0xB	0xC	0x7	0x4	0x2	0x0
S4	0xD	0xC	0xB	0x1	0x4	0x0	0xF	0x3	0x7	0xE	0x5	0x6	0x9	0x2	0x8	0xA
S5	0xA	0x3	0x4	0x6	0xB	0xF	0x0	0xC	0x8	0x9	0x2	0x1	0xE	0x5	0x7	0xD
S6	0xB	0x2	0x5	0x7	0xA	0xE	0x1	0xD	0x9	0x8	0x3	0x0	0xF	0x4	0x6	0xC
S7	0xC	0x5	0x2	0x0	0xD	0x9	0x6	0xA	0xE	0xF	0x4	0x7	0x8	0x3	0x1	0xB
S8	0xD	0x4	0x3	0x1	0xC	0x8	0x7	0xB	0xF	0xE	0x5	0x6	0x9	0x2	0x0	0xA
S9	0xE	0x7	0x0	0x2	0xF	0xB	0x4	0x8	0xC	0xD	0x6	0x5	0xA	0x1	0x3	0x9
S10	0xF	0x6	0x1	0x3	0xE	0xA	0x5	0x9	0xD	0xC	0x7	0x4	0xB	0x0	0x2	0x8
S11	0x1	0x0	0x7	0x5	0x8	0x4	0xB	0xF	0x3	0xA	0x9	0x2	0xD	0xE	0xC	0x6
S12	0x2	0x3	0x4	0x6	0xB	0x7	0x8	0xC	0x0	0x9	0xA	0x1	0xE	0xD	0xF	0x5
S13	0x3	0x2	0x5	0x7	0xA	0x6	0x9	0xD	0x1	0x8	0xB	0x0	0xF	0xC	0xE	0x4
S14	0x4	0x5	0x2	0x0	0xD	0x1	0xE	0xA	0x6	0xF	0xC	0x7	0x8	0xB	0x9	0x3
S15	0x5	0x4	0x3	0x1	0xC	0x0	0xF	0xB	0x7	0xE	0xD	0x6	0x9	0xA	0x8	0x2

32-bit subblocks S^0, S^1 divided into eight four bit subblocks $S^0 = s_0^0 \| s_1^0 \| s_2^0 \| s_3^0 \| s_4^0 \| s_5^0 \| s_6^0 \| s_7^0$, $S^1 = s_0^1 \| s_1^1 \| s_2^1 \| s_3^1 \| s_4^1 \| s_5^1 \| s_6^1 \| s_7^1$. Four bit subblocks s_i^0, s_i^1, $i = \overline{0...7}$ transformed into the S-boxes: $R^0 = S_0(s_0^0) \| S_1(s_1^0) \| S_2(s_2^0) \| S_3(s_3^0) \| S_4(s_4^0) \| S_5(s_5^0) \| S_6(s_6^0) \| S_7(s_7^0)$, $R^1 = S_8(s_0^1) \| S_9(s_1^1) \| S_{10}(s_2^1) \| S_{11}(s_3^1) \| S_{12}(s_4^1) \| S_{13}(s_5^1) \| S_{14}(s_6^1) \| S_{15}(s_7^1)$. The resulting 32-bit subblocks R^0, R^1 cyclically shifted left by 11 bits and we obtain subblocks Y_0, Y_1: $Y_0 = R^0 << 11$, $Y_1 = R^1 << 11$. Thereafter 32-bit subblocks Y_0, Y_1 divided into four 8-bit subblocks Y^0, Y^1, ..., Y^7 i.e., $Y_0 = Y^0 \| Y^1 \| Y^2 \| Y^3$, $Y_1 = Y^4 \| Y^5 \| Y^6 \| Y^7$.

Consider the encryption process of encryption algorithm GOST28147-89-IDEA16-2. Initially the 128-bit plaintext *X* partitioned into subblocks of 8-bits X_0^0, X_0^1, X_0^2, ..., X_0^{15}, and performs the following steps:

1. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} summed by XOR respectively with round key K_{24n+16}, K_{24n+17}, K_{24n+18}, ..., K_{24n+31}: $X_0^j = X_0^j \oplus K_{24n+16+j}$, $j = \overline{0...15}$.

2. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} multiplied and summed respectively with the round keys $K_{24(i-1)}$, $K_{24(i-1)+1}$, $K_{24(i-1)+2}$, ..., $K_{24(i-1)+15}$, $i = \overline{1...n+1}$ and calculated 8-bit subblocks T^0, T^1, T^2, ..., T^7. This step can be represented as follows:

$$T_0 = (X_{i-1}^0 + K_{24(i-1)}) \oplus (X_{i-1}^8 \cdot K_{24(i-1)+8}),$$
$$T_1 = (X_{i-1}^1 \cdot K_{24(i-1)+1}) \oplus (X_{i-1}^9 + K_{24(i-1)+9}),$$
$$T_2 = (X_{i-1}^2 + K_{24(i-1)+2}) \oplus (X_{i-1}^{10} \cdot K_{24(i-1)+10}),$$
$$T_3 = (X_{i-1}^3 \cdot K_{24(i-1)+3}) \oplus (X_{i-1}^{11} + K_{24(i-1)+11}),$$
$$T_4 = (X_{i-1}^4 + K_{24(i-1)+4}) \oplus (X_{i-1}^{12} \cdot K_{24(i-1)+12}),$$
$$T_5 = (X_{i-1}^5 \cdot K_{24(i-1)+5}) \oplus (X_{i-1}^{13} + K_{24(i-1)+13}),$$
$$T_6 = (X_{i-1}^6 + K_{24(i-1)+6}) \oplus (X_{i-1}^{14} \cdot K_{24(i-1)+14}),$$
$$T_7 = (X_{i-1}^7 \cdot K_{24(i-1)+7}) \oplus (X_{i-1}^{15} + K_{24(i-1)+15}),\ i = 1.$$

3. to 8-bit subblocks T^0, T^1, T^2, ..., T^7 applied round functions and get 8-bit subblocks Y^0, Y^1, Y^2, ..., Y^7.

4. subblocks Y^0, Y^1, Y^2, ..., Y^7 are summed to XOR with subblocks X_{i-1}^0, X_{i-1}^1, X_{i-1}^2, ..., X_{i-1}^{15}, i.e. $X_{i-1}^j = X_{i-1}^j \oplus Y^{7-j}$, $X_{i-1}^{j+8} = X_{i-1}^{j+8} \oplus Y^{7-j}$, $j = \overline{0...7}$, $i = 1$.

5. at the end of the round subblocks swapped, i.e. $X_i^j = X_{i-1}^{15-j}$, $j = \overline{1...14}$, $i = 1$

6. repeating steps 2-5 *n* times, i.e., $i = \overline{2...n}$ obtain subblocks X_n^0, X_n^1, X_n^2, ..., X_n^{15}.

7. in output transformation round keys K_{24n}, K_{24n+1}, K_{24n+2}, ..., K_{24n+15} are multiplied and summed into subblocks, i.e.

$$X_{n+1}^0 = X_n^0 + K_{24n},$$
$$X_{n+1}^1 = X_n^{14} \cdot K_{24n+1},$$
$$X_{n+1}^2 = X_n^{13} + K_{24n+2},$$
$$X_{n+1}^3 = X_n^{12} \cdot K_{24n+3},$$
$$X_{n+1}^4 = X_n^{11} + K_{24n+4},$$
$$X_{n+1}^5 = X_n^{10} \cdot K_{24n+5},$$
$$X_{n+1}^6 = X_n^9 + K_{24n+6},$$
$$X_{n+1}^7 = X_n^8 \cdot K_{24n+7},$$
$$X_{n+1}^8 = X_n^7 \cdot K_{24n+8},$$
$$X_{n+1}^9 = X_n^6 + K_{24n+9},$$
$$X_{n+1}^{10} = X_n^5 \cdot K_{24n+10},$$
$$X_{n+1}^{11} = X_n^4 + K_{24n+11},$$
$$X_{n+1}^{12} = X_n^3 \cdot K_{24n+12},$$
$$X_{n+1}^{13} = X_n^2 + K_{24n+13},$$
$$X_{n+1}^{14} = X_n^1 \cdot K_{24n+14},$$
$$X_{n+1}^{15} = X_n^{15} + K_{24n+15}$$

8. subblocks X_{n+1}^0, X_{n+1}^1, X_{n+1}^2, ..., X_{n+1}^{15} are summed to XOR with the round K_{24n+32}, K_{24n+33}, K_{24n+34}, .., K_{24n+47}: $X_{n+1}^j = X_{n+1}^j \oplus K_{24n+32+j}$, $j = \overline{0...7}$.

As ciphertext plaintext X receives the combined 8-bit subblocks $X_{n+1}^0 \| X_{n+1}^1 \| X_{n+1}^2 \| ... \| X_{n+1}^{15}$.

III. Key Generation of the Encryption Algorithm Gost28147-89-Idea16-2

In *n*-round encryption algorithm GOST28147-89-IDEA16-2 in each round used twenty four round keys of the 8-bit and output transformation sixteen round keys of the 8-bit. In addition, before the first round and after the output transformation we used sixteen round keys of 8-bits. Total number of 8-bit round keys is equal to $24n+48$. In Figure 4 encryption used encryption round keys K_i^c instead of K_i^c, while decryption used decryption round keys K_i^d. If n=8 then need 240 to generate round keys, if n=12, you need to generate 336 round keys and if n=16 need 432 to generate round keys.

The key encryption algorithm *K* of length l ($256 \le l \le 1024$) bits is divided into 8-bit round keys K_0^c, K_1^c,..., $K_{Lenght-1}^c$, $Lenght = l/8$, here $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_7\}$, $K_1^c = \{k_8, k_9, ..., k_{15}\}$,..., $K_{Lenght-1}^c = \{k_{l-8}, k_{l-7}, ..., k_{l-1}\}$ and $K = K_0^c \| K_1^c \| ... \| K_{Lenght-1}^c$. Then we calculate $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$. If $K_L = 0$ then K_L is chosen as 0xC5, i.e. K_L =0xC5. Round keys K_i^c, $i = \overline{Lenght...24n+47}$ are computed as follows

$K_i^c = Sbox0(K_{i-Lenght}^c) \oplus Sbox1(RotWord(K_{i-Lenght+1}^c)) \oplus K_L$. After each round key generation the value K_L is cyclic shift to the left by 1 bit. Here, RotWord8()-cyclic shift to the left of 1 bit of the 11-bit subblock, Sbox-transformation a 8-bit subblock in the S-boxes, $Sbox0(S) = S_0(t^0) \| S_1(t^1)$, $Sbox1(S) = S_8(t^0) \| S_9(t^1)$ and t^0, t^1-four bit subblock, $T = t^0 \| t^1$-eight bit subblock.

Decryption round keys K_i^d are computed on the basis of encryption round keys K_i^c and decryption round keys of the output transformation associate with of encryption round keys as follows:

$$(K_{24n}^d, K_{24n+1}^d, K_{24n+2}^d, K_{24n+3}^d, K_{24n+4}^d, K_{24n+5}^d, K_{24n+6}^d, K_{24n+7}^d, K_{24n+8}^d, K_{24n+9}^d, K_{24n+10}^d, K_{24n+11}^d, K_{24n+12}^d, K_{24n+13}^d, K_{24n+14}^d, K_{24n+15}^d) = (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, (K_8^c)^{-1}, -K_9^c, (K_{10}^c)^{-1}, -K_{11}^c, (K_{12}^c)^{-1}, -K_{13}^c, (K_{14}^c)^{-1}, -K_{15}^c).$$

Decryption round keys of the first round associate with of encryption round keys as follows:

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d, K_{16}^d, K_{17}^d, K_{18}^d, K_{19}^d, K_{20}^d, K_{21}^d, K_{22}^d, K_{23}^d) = (-K_{24n}^c, (K_{24n+1}^c)^{-1}, -K_{24n+2}^c, (K_{24n+3}^c)^{-1}, -K_{24n+4}^c, (K_{24n+5}^c)^{-1}, -K_{24n+6}^c, (K_{24n+7}^c)^{-1}, (K_{24n+8}^c)^{-1}, -K_{24n+9}^c, (K_{24n+10}^c)^{-1}, -K_{24n+11}^c, (K_{24n+12}^c)^{-1}, -K_{24n+13}^c, (K_{24n+14}^c)^{-1}, -K_{24n+15}^c, K_{24(n-1)+16}^c, K_{24(n-1)+17}^c, K_{24(n-1)+18}^c, K_{24(n-1)+19}^c, K_{24(n-1)+20}^c, K_{24(n-1)+21}^c, K_{24(n-1)+22}^c, K_{24(n-1)+23}^c).$$

Decryption round keys of the second, third and n-round associates with the encryption round keys as follows:

$$(K_{24(i-1)}^d, K_{24(i-1)+1}^d, K_{24(i-1)+2}^d, K_{24(i-1)+3}^d, K_{24(i-1)+4}^d, K_{24(i-1)+5}^d, K_{24(i-1)+6}^d, K_{24(i-1)+7}^d, K_{24(i-1)+8}^d, K_{24(i-1)+9}^d, K_{24(i-1)+10}^d, K_{24(i-1)+11}^d, K_{24(i-1)+12}^d, K_{24(i-1)+13}^d, K_{24(i-1)+14}^d, K_{24(i-1)+15}^d, K_{24(i-1)+16}^d, K_{24(i-1)+17}^d, K_{24(i-1)+18}^d, K_{24(i-1)+19}^d, K_{24(i-1)+20}^d, K_{24(i-1)+21}^d, K_{24(i-1)+22}^d, K_{24(i-1)+23}^d) = (-K_{24(n-i+1)}^c, (K_{24(n-i+1)+14}^c)^{-1}, -K_{24(n-i+1)+13}^c, (K_{24(n-i+1)+12}^c)^{-1}, -K_{24(n-i+1)+11}^c, (K_{24(n-i+1)+10}^c)^{-1}, -K_{24(n-i+1)+9}^c, (K_{24(n-i+1)+8}^c)^{-1}, (K_{24(n-i+1)+7}^c)^{-1}, -K_{24(n-i+1)+6}^c, (K_{24(n-i+1)+5}^c)^{-1}, -K_{24(n-i+1)+4}^c, (K_{24(n-i+1)+3}^c)^{-1}, -K_{24(n-i+1)+2}^c, (K_{24(n-i+1)+1}^c)^{-1}, -K_{24(n-i+1)+15}^c, K_{24(n-i)+16}^c, K_{24(n-i)+17}^c, K_{24(n-i)+18}^c, K_{24(n-i)+19}^c, K_{24(n-i)+20}^c, K_{24(n-i)+21}^c, K_{24(n-i)+22}^c, K_{24(n-i)+23}^c), i = \overline{2...n}.$$

Decryption round keys applied to the first round and after the output transformation associated with the encryption round keys as follows: $K_{24n+16+j}^d = K_{24n+32+j}^c$, $K_{24n+32+j}^d = K_{24n+16+j}^c$, $j = \overline{0...7}$.

IV. The Structure of the Encryption Algorithm GOST28147-89-RFWKIDEA16-2

In the encryption algorithm GOST28147-89-RFWKIDEA16-2 the length of subblocks X^0, X^1, X^2,..., X^{15}, length of round keys $K_{16(i-1)}$, $K_{16(i-1)+1}$, $K_{16(i-1)+2}$, ..., $K_{16(i-1)+15}$, $i = \overline{1...n+1}$, K_{16n+16}, K_{16n+17}, K_{16n+18}, ..., K_{16n+47} are equal to 8-bits. The length of the input and output blocks of round functions is 32 bits. This encryption algorithm round function GOST 28147-89 is applied twice and in each round function employed eight S-boxes, i.e. the total number of S-boxes is 16. The structure of the encryption algorithm GOST28147-89-PES16-2 is shown in Figure 2 and the S-boxes shown in Table 1.

Consider the round function block encryption algorithm GOST28147-89-RFWKIDEA16-2. First the 8-bit subblocks T^0, T^1, ..., T^7 combined from 32-bit subblocks, i.e. $T_0 = T^0 \| T^1 \| T^2 \| T^3$, $T_1 = T^4 \| T^5 \| T^6 \| T^7$. 32-bit subblocks T_0, T_1 divided into eight four bit subblocks $T_0 = t_0^0 \| t_1^0 \| t_2^0 \| t_3^0 \| t_4^0 \| t_5^0 \| t_6^0 \| t_7^0$, $T_1 = t_0^1 \| t_1^1 \| t_2^1 \| t_3^1 \| t_4^1 \| t_5^1 \| t_6^1 \| t_7^1$. Four bit subblocks t_i^0, t_i^1, $i = \overline{0...7}$ transformed into the S-boxes: $R^0 = S_0(t_0^0) \| S_1(t_1^0) \| S_2(t_2^0) \| S_3(t_3^0) \| S_4(t_4^0) \| S_5(t_5^0) \| S_6(t_6^0) \| S_7(t_7^0)$, $R^1 = S_8(t_0^1) \| S_9(t_1^1) \| S_{10}(t_2^1) \| S_{11}(t_3^1) \| S_{12}(t_4^1) \| S_{13}(t_5^1) \| S_{14}(t_6^1) \| S_{15}(t_7^1)$.

The resulting 32-bit subblocks R^0, R^1 cyclically shifted left by 11 bits and we obtain subblocks Y_0, Y_1: $Y_0 = R^0 << 11$, $Y_1 = R^1 << 11$. Thereafter 32-bit subblocks Y_0, Y_1 divided into four 8-bit subblocks Y^0, Y^1, ..., Y^7 i.e., $Y_0 = Y^0 \| Y^1 \| Y^2 \| Y^3$, $Y_1 = Y^4 \| Y^5 \| Y^6 \| Y^7$.

Consider the encryption process of encryption algorithm GOST28147-89-IDEA16-2. Initially the 128-bit plaintext \$X\$ partitioned into subblocks of 8-bits X_0^0, X_0^1, X_0^2, ..., X_0^{15}, and performs the following steps:

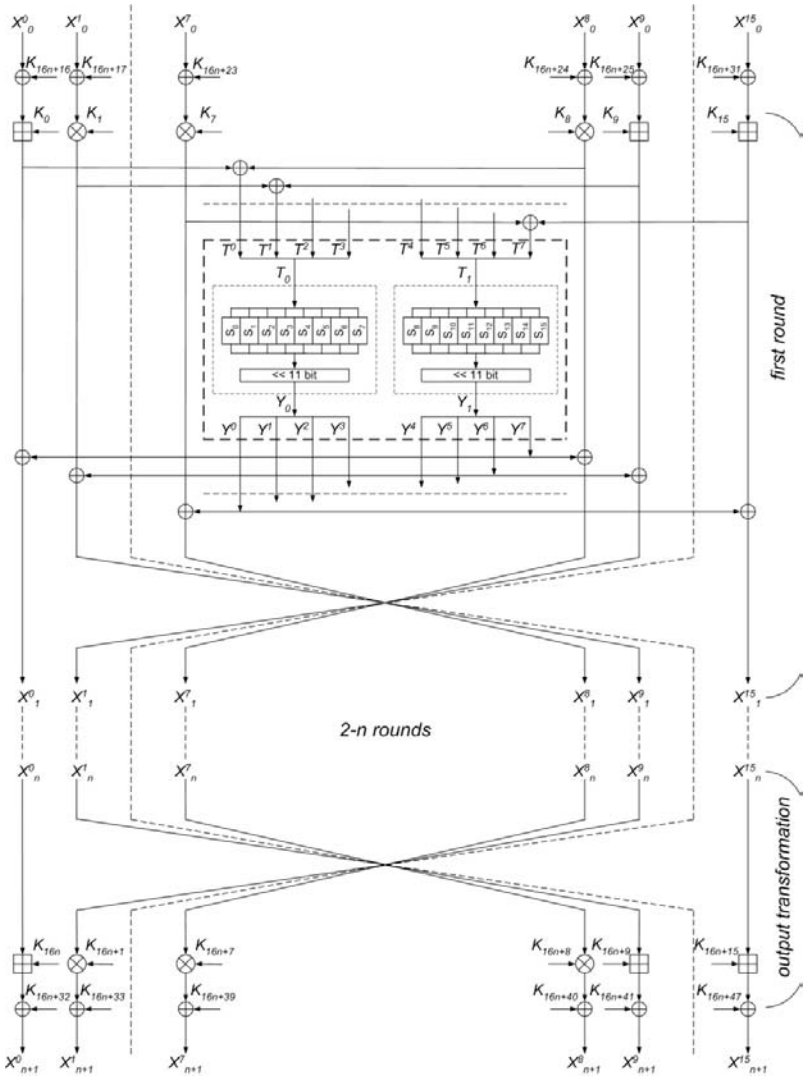


Figure 2 : The scheme n-rounded encryption algorithm GOST28147-89-RFWKIDEA16-2

1. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} summed by XOR respectively with round key K_{16n+16}, K_{16n+17}, K_{16n+18}, ..., K_{16n+31} i.e $X_0^j = X_0^j \oplus K_{16n+16+j}$, $j = \overline{0...7}$.
2. subblocks X_0^0, X_0^1, X_0^2, ..., X_0^{15} multiplied and summed respectively with the round keys $K_{16(i-1)}$, $K_{16(i-1)+1}$, $K_{16(i-1)+2}$, ..., $K_{16(i-1)+15}$ and calculated 8-bit subblocks T^0, T^1, T^2, ..., T^7. This step can be represented as follows:

$$T_0 = (X_{i-1}^0 + K_{16(i-1)}) \oplus (X_{i-1}^8 \cdot K_{16(i-1)+8}),$$
$$T_1 = (X_{i-1}^1 \cdot K_{16(i-1)+1}) \oplus (X_{i-1}^9 + K_{16(i-1)+9}),$$
$$T_2 = (X_{i-1}^2 + K_{16(i-1)+2}) \oplus (X_{i-1}^{10} \cdot K_{16(i-1)+10}),$$
$$T_3 = (X_{i-1}^3 \cdot K_{16(i-1)+3}) \oplus (X_{i-1}^{11} + K_{16(i-1)+11}),$$
$$T_4 = (X_{i-1}^4 + K_{16(i-1)+4}) \oplus (X_{i-1}^{12} \cdot K_{16(i-1)+12}),$$
$$T_5 = (X_{i-1}^5 \cdot K_{16(i-1)+5}) \oplus (X_{i-1}^{13} + K_{16(i-1)+13}),$$
$$T_6 = (X_{i-1}^6 + K_{16(i-1)+6}) \oplus (X_{i-1}^{14} \cdot K_{16(i-1)+14}),$$
$$T_7 = (X_{i-1}^7 \cdot K_{16(i-1)+7}) \oplus (X_{i-1}^{15} + K_{16(i-1)+15}), \; i = 1.$$

3. to 8-bit subblocks T^0, T^1, T^2, ..., T^7 applied round functions and get 8-bit subblocks Y^0, Y^1, Y^2, ..., Y^7.
4. subblocks Y^0, Y^1, Y^2, ..., Y^7 are summed to XOR with subblocks X_{i-1}^0, X_{i-1}^1, X_{i-1}^2, ..., X_{i-1}^{15} i.e. $X_{i-1}^j = X_{i-1}^j \oplus Y^{7-j}$, $X_{i-1}^{j+8} = X_{i-1}^{j+8} \oplus Y^{7-j}$, $j = \overline{0...7}$, $i = 1$.
5. at the end of the round subblocks swapped, i.e., $X_i^j = X_{i-1}^{15-j}$, $j = \overline{1...14}$, $i = 1$.
6. repeating steps 2-5 *n* times, i.e., $i = \overline{2...n}$ obtain subblocks X_n^0, X_n^1, X_n^2, ..., X_n^{15}.

7. in output transformation round keys K_{16n}, K_{16n+1}, K_{16n+2}, ..., K_{16n+15} are multiplied and summed into subblocks X_n^0, X_n^1, X_n^2, ..., X_n^{15}, i.e.

$$X_{n+1}^0 = X_n^0 + K_{16n}, \quad X_{n+1}^1 = X_n^{14} \cdot K_{16n+1},$$
$$X_{n+1}^2 = X_n^{13} + K_{16n+2}, \quad X_{n+1}^3 = X_n^{12} \cdot K_{16n+3},$$
$$X_{n+1}^4 = X_n^{11} + K_{16n+4}, \quad X_{n+1}^5 = X_n^{10} \cdot K_{16n+5},$$
$$X_{n+1}^6 = X_n^9 + K_{16n+6}, \quad X_{n+1}^7 = X_n^8 \cdot K_{16n+7},$$
$$X_{n+1}^8 = X_n^7 \cdot K_{16n+8}, \quad X_{n+1}^9 = X_n^6 + K_{16n+9},$$
$$X_{n+1}^{10} = X_n^5 \cdot K_{16n+10}, \quad X_{n+1}^{11} = X_n^4 + K_{16n+11},$$
$$X_{n+1}^{12} = X_n^3 \cdot K_{16n+12}, \quad X_{n+1}^{13} = X_n^2 + K_{16n+13},$$
$$X_{n+1}^{14} = X_n^1 \cdot K_{16n+14}, \quad X_{n+1}^{15} = X_n^{15} + K_{16n+15}.$$

8. subblocks X_{n+1}^0, X_{n+1}^1, X_{n+1}^2, ..., X_{n+1}^{15} are summed to XOR with the round key K_{16n+32}, K_{16n+33}, K_{16n+34}, .., K_{16n+47}: $X_{n+1}^j = X_{n+1}^j \oplus K_{16n+32+j}$, $j = \overline{0...7}$.

As ciphertext plaintext X receives the combined 8-bit subblocks $X_{n+1}^0 \| X_{n+1}^1 \| X_{n+1}^2 \| ... \| X_{n+1}^{15}$.

V. Key Generation of the Encryption Algorithm Gost28147-89-Rfwkidea16-2

In n-round encryption algorithm GOST28147-89-IDEA16-2 in each round used sixteen round keys of the 8-bit and output transformation sixteen round keys of the 8-bit. In addition, before the first round and after the output transformation we used sixteen round keys of 8-bits. Total number of 8-bit round keys is equal to 16n+48. In Figure 4 encryption used encryption round keys K_i^c instead of K_i, while decryption used decryption round keys K_i^d.

The key encryption algorithm K of length l ($256 \le l \le 1024$) bits is divided into 8-bit round keys K_0^c, K_1^c,..., $K_{Lenght-1}^c$, $Lenght = l/8$, here $K = \{k_0, k_1, ..., k_{l-1}\}$, $K_0^c = \{k_0, k_1, ..., k_7\}$, $K_1^c = \{k_8, k_9, ..., k_{15}\}$, ..., $K_{Lenght-1}^c = \{k_{l-8}, k_{l-7}, ..., k_{l-1}\}$ and $K = K_0^c \| K_1^c \| ... \| K_{Lenght-1}^c$.

Then we calculate $K_L = K_0^c \oplus K_1^c \oplus ... \oplus K_{Lenght-1}^c$.

If $K_L = 0$ then K_L is chosen as 0xC5, i.e. K_L =0xC5. Round keys K_i^c, $i = \overline{Lenght...16n+47}$ are computed as follows $K_i^c = Sbox0(K_{i-Lenght}^c) \oplus Sbox1(RotWord(K_{i-Lenght+1}^c)) \oplus K_L$. After each round key generation the value K_L is cyclic shift to the left by 1 bit. Here, RotWord8()-cyclic shift to the left of 1 bit of the 11-bit subblock, Sbox-transformation a 8-bit subblock in the S-boxes, $Sbox0(T) = S_2(t^0) \| S_3(t^1)$, $Sbox1(T) = S_{10}(t^0) \| S_{11}(t^1)$, $T = t^0 \| t^1$ and t^0, t^1-four bit subblock, T-eight bit subblock.

Decryption round keys K_i^d are computed on the basis of encryption round keys K_i^c and decryption round keys of the output transformation associate with of encryption round keys as follows:

$$(K_{16n}^d, K_{16n+1}^d, K_{16n+2}^d, K_{16n+3}^d, K_{16n+4}^d, K_{16n+5}^d, K_{16n+6}^d, K_{16n+7}^d, K_{16n+8}^d, K_{16n+9}^d, K_{16n+10}^d, K_{16n+11}^d, K_{16n+12}^d, K_{16n+13}^d, K_{16n+14}^d, K_{16n+15}^d) = (-K_0^c, (K_1^c)^{-1}, -K_2^c, (K_3^c)^{-1}, -K_4^c, (K_5^c)^{-1}, -K_6^c, (K_7^c)^{-1}, (K_8^c)^{-1}, -K_9^c, (K_{10}^c)^{-1}, -K_{11}^c, (K_{12}^c)^{-1}, -K_{13}^c, (K_{14}^c)^{-1}, -K_{15}^c).$$

Decryption round keys of the first round associate with of encryption round keys as follows:

$$(K_0^d, K_1^d, K_2^d, K_3^d, K_4^d, K_5^d, K_6^d, K_7^d, K_8^d, K_9^d, K_{10}^d, K_{11}^d, K_{12}^d, K_{13}^d, K_{14}^d, K_{15}^d) = (-K_{16n}^c, (K_{16n+1}^c)^{-1}, -K_{16n+2}^c, (K_{16n+3}^c)^{-1}, -K_{16n+4}^c, (K_{16n+5}^c)^{-1}, -K_{16n+6}^c, (K_{16n+7}^c)^{-1}, (K_{16n+8}^c)^{-1}, -K_{16n+9}^c, (K_{16n+10}^c)^{-1}, -K_{16n+11}^c, (K_{16n+12}^c)^{-1}, -K_{16n+13}^c, (K_{16n+14}^c)^{-1}, -K_{16n+15}^c).$$

Decryption round keys of the second, third and n-round associates with the encryption round keys as follows:

$$(K_{16(i-1)}^d, K_{16(i-1)+1}^d, K_{16(i-1)+2}^d, K_{16(i-1)+3}^d, K_{16(i-1)+4}^d, K_{16(i-1)+5}^d, K_{16(i-1)+6}^d, K_{16(i-1)+7}^d, K_{16(i-1)+8}^d, K_{16(i-1)+9}^d, K_{16(i-1)+10}^d, K_{16(i-1)+11}^d, K_{16(i-1)+12}^d, K_{16(i-1)+13}^d, K_{16(i-1)+14}^d, K_{16(i-1)+15}^d) = (-K_{16(n-i+1)}^c, (K_{16(n-i+1)+14}^c)^{-1}, -K_{16(n-i+1)+13}^c, (K_{16(n-i+1)+12}^c)^{-1}, -K_{16(n-i+1)+11}^c, (K_{16(n-i+1)+10}^c)^{-1}, -K_{16(n-i+1)+9}^c, (K_{16(n-i+1)+8}^c)^{-1}, (K_{16(n-i+1)+7}^c)^{-1}, -K_{16(n-i+1)+6}^c, (K_{16(n-i+1)+5}^c)^{-1}, -K_{16(n-i+1)+4}^c, (K_{16(n-i+1)+3}^c)^{-1}, -K_{16(n-i+1)+2}^c, (K_{16(n-i+1)+1}^c)^{-1}, -K_{16(n-i+1)+15}^c), i = \overline{2...n}.$$

Decryption round keys applied to the first round and after the output transformation associated with the encryption round keys as follows: $K_{16n+16+j}^d = K_{16n+32+j}^c$, $K_{16n+32+j}^d = K_{16n+16+j}^c$, $j = \overline{0...7}$

VI. Results

As a result of this study built a new block encryption algorithms called GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2. This algorithm is based on a networks IDEA16-2 and RFWKIDEA16-2 using the round function of GOST 28147-89. Length of block encryption algorithm is 128 bits, the number of rounds and key lengths is variable. Wherein the user depending on the degree of secrecy of the information and speed of encryption can select the number of rounds and key length.

It is known, that the S-box encryption algorithm GOST 28147-89 are secret and used as a long-term key.

following Table 2 summarizes options openly declared S-box such as: $\deg$ -degree of algebraic nonlinearity; NL -nonlinearity; λ -resistance to linear cryptanalysis; δ -resistance to differential cryptanalysis; SAC-strict avalanche criterion; BIC-bit independence criterion.To S-box was resistant to cryptanalysis it is necessary that the values $\deg$ and NL were large, and the values λ, δ, SAC and BIC small. In block cipher algorithms GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 for all S-boxes, the following equation: $\deg = 3$, $NL = 4$, $\lambda = 0.5$, $\delta = 3/8$, $SAC \le 2$, $BIC \le 4$, i.e. resistance is not lower than the algorithm GOST 28147-89. These S-boxes are created based on Nyberg construction [3].

Table 2 : Parameters of the S-boxes encryption algorithm GOST 28147-89

№	Parameters	S1	S2	S3	S4	S5	S6	S7	S8
1	$\deg$	2	3	3	2	3	3	2	2
2	NL	4	2	2	2	2	2	2	2
3	λ	0.5	3/4	3/4	3/4	3/4	3/4	3/4	3/4
4	δ	3/8	3/8	3/8	3/8	1/4	3/8	0.5	0.5
5	SAC	2	2	2	4	2	4	2	2
6	BIC	4	2	4	4	4	4	2	4

IV. Conclusions

In this way, built a new block encryption algorithms called GOST28147-89-IDEA16-2 and GOST28147-89-RFWKIDEA16-2 based on networks IDEA16-2 and RFWKIDEA16-2 using the round function of GOST 28147-89. Installed that the resistance offered by the author block cipher algorithm not lower than the resistance of the algorithm GOST 28147-89.

References Références Referencias

1. Aripov M.M. Tuychiev G.N. The network IDEA4–2, consists from two round functions // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2012, №4 (24), pp. 5559.
2. Aripov M.M. Tuychiev G.N. The network PES8–4, consists from four round functions // Materials of the international scientific conference конференции «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012», Volume №I, –Tashkent, 2012, pp. 16–19.
3. Bakhtiyorov U., Tuychiev G. About Generation Resistance S Box And Boolean Function On The Basis Of Nyberg Construction // Materials scientific-technical conference «Applied mathematics and information security», Tashkent, 2014, 28–30 april, - pp. 317–324
4. GOST 28147–89. National Standard of the USSR. Information processing systems. Cryptographic protection. Algorithm cryptographic transformation.
5. Tuychiev G.N. The networks RFWKIDEA4–2, IDEA4–1 and RFWKIDEA4–1 // Acta of Turin polytechnic university in Tashkent, 2013, №3pp. 71-77
6. Tuychiev G.N. The network PES4–2, consists from two round functions // Uzbek journal of the problems of informatics and energetics. –Tashkent, 2013, №56, pp. 107–111
7. Tuychiev G.N. About networks PES4–1 and RFWKPES4–2, RFWKPES4–1 developed on the basis of network PES4–2 // Uzbek journal of the problems of informatics and energetics. –Tashkent, 2015, №12, pp. 100-105.
8. Tuychiev G.N. About networks RFWKPES8–4, RFWKPES8–2, RFWKPES8–1, developed on the basis of network PES8–4 // Transactions of the international scientific conference «Modern problems of applied mathematics and information technologies–Al–Khorezmiy 2012», Volume№ 2, –Samarkand, 2014, pp. 32–36
9. Tuychiev G. Creating a data encryption algorithm based on network IDEA4-2, with the use the round function of the encryption algorithm GOST 28147-89 // Infocommunications: Networks–Technologies–Solutions. –Tashkent, 2014, №4 (32), pp. 4954
10. Tuychiev G. Creating a encryption algorithm based on network RFWKIDEA4–2 with the use the round function of the GOST 28147-89 // International Conference on Emerging Trends in Technology, Science and Upcoming Research in Computer Science (ICDAVIM-2015), //printed in International Journal of Advanced Technology in Engineering and Science, 2015, vol. 3, №1pp. 427-432
11. Tuychiev G. Creating a encryption algorithm based on network PES4-2 with the use the round function of the GOST 28147-89 // TUIT Bulleten, -Tashkent, 2015, №2(34)pp. 132-136
12. Tuychiev G. Creating a encryption algorithm based on network RFWKPES4–2 with the use the round function of the GOST 28147–89 // International Journal of Multidisciplinary in Cryptology and Information Security, 2015, vol.4., №, pp. 14-17
13. Tuychiev G. The encryption algorithms GOST28147–89–PES8–4 and GOST28147–89–RFWKPES8–4 // «Information Security in the light of the Strategy Kazakhstan-2050»: proceedings III International scientific-practical conference (15-16 October 2015, Astana). - Astana, 2015. pp. 355-371
14. Tuychiev G.N. About networks IDEA16–4, IDEA16–2, IDEA16–1, created on the basis of network IDEA16–8 // Compilation of theses and reports republican seminar «Information security in the sphere communication and information. Problems and their solutions» –Tashkent, 2014

15. Tuychiev G.N. About networks RFWKIDEA16–8, RFWKIDEA16–4, RFWKIDEA16–2, RFWKIDEA16–1, created on the basis network IDEA16–8 // Ukrainian Scientific Journal of Information Security, –Kyev, 2014, vol. 20, issue 3, pp. 259–263

Global Journals Inc. (US) Guidelines Handbook 2016

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards "FARSC" title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

AUXILIARY MEMBERSHIPS

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.

The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

After nomination of your institution as "Institutional Fellow" and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

Process of submission of Research Paper

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

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

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

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

(II) Choose corresponding Journal.

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

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

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

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

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

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

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

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

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

Scope

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

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

2. ETHICAL GUIDELINES

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

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

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

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

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

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

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

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

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

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

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

Please mention proper reference and appropriate acknowledgements wherever expected.

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

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

3. SUBMISSION OF MANUSCRIPTS

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

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

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

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

4. MANUSCRIPT'S CATEGORY

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

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

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

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

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

5. STRUCTURE AND FORMAT OF MANUSCRIPT

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

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

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

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

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

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

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

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

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

(h) Brief Acknowledgements.

(i) References in the proper form.

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

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

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

Format

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

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

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

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

Structure

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

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

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

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

Key Words

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

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

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

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

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

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

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

Acknowledgements: Please make these as concise as possible.

References

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

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

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

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

Tables, Figures and Figure Legends

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

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

Preparation of Electronic Figures for Publication

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

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

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

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

6. AFTER ACCEPTANCE

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

6.1 Proof Corrections

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

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

(Free of charge) from the following website:

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

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

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

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

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

6.3 Author Services

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

6.4 Author Material Archive Policy

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

6.5 Offprint and Extra Copies

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

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

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

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Informal Guidelines of Research Paper Writing

Key points to remember:

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

Final Points:

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

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

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

General style:

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

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

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

In every sections of your document

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

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

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

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

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

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

Title Page:

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

Abstract:

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

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

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

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

Approach:

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

Introduction:

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

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

Approach:

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

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

Procedures (Methods and Materials):

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

Materials:

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

Methods:

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

Approach:

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

What to keep away from

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

Results:

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

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

Content

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

What to stay away from

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

Approach

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

Figures and tables

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

Discussion:

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

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

Approach:

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

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

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