IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-9 E-ISSN: 2347-2693

Comparison of Static and Dynamic Watchdog Technique to Provide Secure Data Transfer

Gayathri C.[1], Vadivel R.[2*]

1. Dept. of IT, School of Computer Science and Engineering, Bharathiar University, Coimbatore, India
2. Dept. of IT, School of Computer Science and Engineering, Bharathiar University, Coimbatore, India

*Corresponding Author: gayathricheran93@gmail.com

Available online at: www.ijcseonline.org

Received: 23/Aug/2017, Revised: 07/Sep/2017, Accepted: 12/Sep/2017, Published: 30/Sep/2017

Abstract: Wireless network is one of the significant aspects for the roaming users while they travel across the networks transfer of data may done. It provide issues like data attackers were catch the files and they used by their way. Hence user of the network faces the security problems. For this issues watchdog mechanism were provide to monitor the attackers. The watchdog technique is a trust based attacker detection technique which identifies the malicious nodes and its activity in the network is to monitor the nodes within its communication range. The nodes selected as the watchdog nodes are the most trustworthy nodes due to its inherent features like highly stable. For this aspect static and dynamic watchdog techniques were followed, this article provides the comparison between static and dynamic watchdog mechanism to shows which technique provide the best.

Keywords: MANET, Security, Watchdog, Comparison, Static and Dynamic.

I. INTRODUCTION

Technology is expanding every day, forcing a change in communication trends. Mobile Ad-hoc networks are a new paradigm of wireless communication, for mobile hosts.

Unlike traditional networks, Mobile Ad-hoc networks do not rely on any fixed infrastructure, or any centralized control, such as base stations, or mobile switching centres. The mobile nodes communicate using a wireless network [1]. Mobile Ad-hoc network hosts are mobile and flexible, and they communicate with each other within radio range, through direct wireless links, or multi hop routing.

Due to its mobility and portability in wireless communication, it introduces data security threats, and security attacks. The routing protocols in Mobile Ad-hoc networks are there to set up the most suitable path, between the source and destination, with minimum overhead and minimum bandwidth consumption. So that packets are delivered in a timely manner.

In MANET routes are enabled in between the mobile hosts, using multi hop, as the transmission range of wireless radio is limited. The hosts are responsible for passing through packets over Mobile Ad-hoc networks, and they are not aware of the topology of the network. Routing plays an important role in the security of the entire network. The mobility and portability in Mobile Ad-Hoc networks introduces security threats and security attacks.

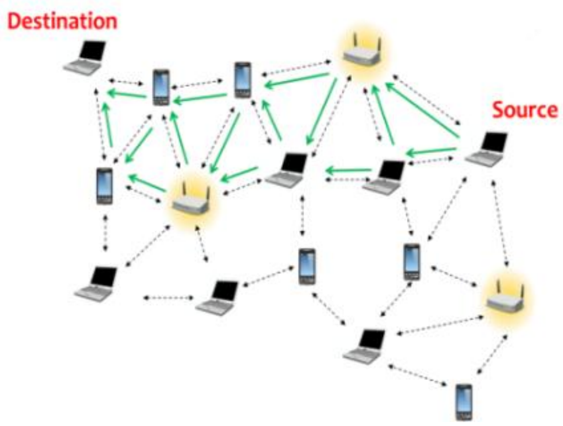

Fig 1: MANET mechanism

A change in topology means that security will have to be accessible, as nodes may be mobile, entering and leaving the network [2]. Mobile Ad-hoc networks are vulnerable to attacks that can be categorized into two types: Passive attacks and Active attacks, where active attacks can further be subdivided into internal and external attacks. Mobile Ad-hoc networks routing protocols are exposed to different types of attacks, Black-hole attacks, being the most serious type. Basically MANETs is self-forming, self-maintained, and self-healing, allowing for extreme network flexibility. MANET can be implemented as self-contained networks, or linked up to the internet, or private networks.

Security always implies the identification of potential attacks, threats, and vulnerabilities of a certain system. In information systems, security is often defined in the context of being able to ensure confidentiality, integrity, and availability of network resources. The watchdog scheme works in two parts-in the first part the watchdog detects the malicious node by promiscuously listening to its next neighbour's transmission. If a node doesn't forward the packet after a threshold, then watchdog declares that node as malicious [3]. And then the pathrater finds the new route to the destination excluding that malicious node. The watchdog occurs in every node in the network. When a node forwards a packet, the nodes watchdog component verifies that the next node in the path also forward the packet. The only way a watchdog can do this, is by listening in a promiscuous mode, to the next node's transmission. If the next node does not forward the packet, it is said to be a malicious (mischievous) node, and has to be reported [4]. This is done by sending an alarm message to the other nodes on its friends list. When the nodes accept the alarm message, they check it, and change the status of the accused node, only if the alarm source is trusted, or a number of trusted nodes accused the same node. The watchdog technique is a trust based attacker detection technique which identifies the malicious nodes and its activity in the network is to monitor the nodes within its communication range. The nodes selected as the watchdog nodes are the most trustworthy nodes due to its inherent features like highly stable [5]. For this aspect static and dynamic watchdog techniques were followed, this article paper provides the comparison between static and dynamic watchdog mechanism to shows which technique provide the best.

II. LITERATURE REVIEW

Mobile Ad-Hoc Network (MANET) has become more popular in recent years because of its features like mobility and deployed nature. But, few natures like wireless and dynamic changes of topology launch different types of attack than the wired network. Hence, security is one of the major concerns should be considered to prevent MANET services from vulnerable attacks due to the presence of malicious nodes. This section shows the various researches approaches advantages and disadvantages

Indhu Lekha, S.J., Kathiroli, R [6] A Joint Routing and Medium Access Control (MAC) Algorithm is proposed for lifetime maximization of distributed wireless sensor networks. By adopting the flow contention graph model and the resulting MAC constraints, the problem can be formulated into a linear program (LP) with separable structure, which can be solved distributive using dual decomposition. However, the message passing overhead of such a solution is still high, since the information exchange must occur among the interfering links as well as the communicating links. In this research work, the MAC layer constraints are relaxed in the form of a penalty function, which facilitates distributed optimization using only the collision statistic that each node can accumulate essentially at no extra cost. The resulting algorithm solves a convex optimization problem by a distributed primal-dual approach, where the network layer problem is solved in the dual domain, and the MAC layer problem is solved in the primal domain.

Zuckerman, M., Faliszewski, P, [7] Traditional trust management schemes developed for wired and wireless ad hoc networks are not well suited for sensor networks due to their higher consumption of resources such as memory and power. In this work propose a new lightweight Group-based Trust Management Scheme (GTMS) for wireless sensor networks, which employs clustering. Our approach reduces the cost of trust evaluation. Also, theoretical as well as simulation results show that our scheme demands less memory, energy, and communication overheads as compared to the current state-of-the-art trust management schemes and it is more suitable for large-scale sensor networks. Furthermore, GTMS also enables us to detect and prevent malicious, selfish, and faulty nodes.

Liu,W., Nishiyama, H., Ansari, N., et al. [8] The resource efficiency and dependability of a trust system are the most fundamental requirements for any Wireless Sensor Network (WSN). However, existing trust systems developed for WSNs are incapable of satisfying these requirements because of their high overhead and low dependability. In this work proposed a Lightweight and Dependable Trust System (LDTS) for WSNs, which employ clustering algorithms. First, a lightweight trust decision-making scheme is proposed based on the nodes' identities (roles) in the clustered WSNs, which is suitable for such WSNs because it facilitates energy-saving. Due to cancelling feedback between Cluster Members (CMs) or between Cluster Heads (CHs), this approach can significantly improve system efficiency while reducing the effect of malicious nodes. More importantly, considering that CHs take on large amounts of data forwarding and communication tasks, a dependability-enhanced trust evaluating approach is defined for co-operations between CHs.

This approach can effectively reduce networking consumption while malicious, selfish, and faulty CHs. Moreover, a self-adaptive weighted method is defined for trust aggregation at CH level. This approach surpasses the limitations of traditional weighting methods for trust factors, in which weights are assigned subjectively. Theory as well as simulation results shows that LDTS demands less memory and communication overhead compared with the current typical trust systems for WSNs.

Izquierdo, L.R., Izquierdo, [9], The multi-hop routing in wireless sensor networks (WSNs) offers little protection against identity theft through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols, including sinkhole attacks, wormhole attacks and Sybil attacks. The situation is further aggravated by mobile and harsh network conditions. Traditional cryptographic techniques or efforts at developing trust-aware routing protocols do not effectively address this severe problem.

To secure the WSNs against adversaries misdirecting the multi-hop routing, the proposed technique is designed and implemented TARF, a robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. Most importantly, TARF proves effective against those harmful attacks developed out of identity deception; the resilience of TARF is verified through extensive evaluation with both simulation and empirical experiments on large-scale WSNs under various scenarios including mobile and RF-shielding network conditions.

Kim, S. [10], un-attended Wireless Sensor Networks (UWSNs) are characterized by long periods of disconnected operation and fixed or irregular intervals between sink visits. The absence of an online trusted third party implies that existing WSN trust management schemes are not applicable to UWSNs. In this paper, propose a trust management scheme for UWSNs to provide efficient and robust trust data storage and trust generation. For trust data storage, employ a geographic hash table to identify storage nodes and to significantly decrease storage cost.

In this subjective logic based consensus techniques used to mitigate trust fluctuations caused by environmental factors. In this research work exploit a set of trust similarity functions to detect trust outliers and to sustain trust pollution attacks and demonstrate, through extensive analyses and simulations, that the proposed scheme is efficient, robust and scalable.

III. PROBLEM FACING

A watchdog task consists of a bidirectional communication between the watchdog node and the target node. But this technique required large amount of energy. The inefficient use of watchdog technique provides security issues. It increases security issues in MANET.

Construction trust system is not simple task. This scheme takes additional time to identify malicious node. Devour high energy while identify and rescind malicious node [13, 14]. If deduce the CA is not accessible the CH unable to send malicious information, it guide to hindrance in network. There is no word for CH switch in case of low energy.

- This kind of technique provide data loss
- They not give correct solution for energy consumption.
- This technique is not efficiently identified and blocks the attacking nodes.
- Decrease the network lifetime.

IV. COMPARISON OF STATIC AND DYNAMIC WATCHDOG

The use of attacker's node as watchdogs will impede the security maximization goal in since those sensor nodes can report fake watchdog results to drop the trust robustness. So find the optimal watchdog here compare the static and dynamic watchdog approaches.

A. Static watchdog

The Watchdog is used to improve throughput in a MANET, by identifying misbehaving nodes, which trick other nodes, by agreeing to forward the packets without ever doing so. While the watchdog is used to identify misbehaving (malicious) nodes, initiated by a Replica server, static method helps routing protocols avoid these nodes, by removing them, and creating a new path. The watchdog occurs in every node in the network. When a node forwards a packet, the nodes watchdog component verifies that the next node in the path also forward the packet. The only way a watchdog can do this, is by listening in a promiscuous mode, to the next node’s transmission. If the next node does not forward the packet, it is said to be a malicious (mischievous) node, and has to be reported. This is done by sending an alarm message to the other nodes on its friends list. When the nodes accept the alarm message, they check it, and change the status of the accused node, only if the alarm source is trusted, or a number of trusted nodes accused the same node. By this static node selection of watchdog method it only find the attackers in the one path only, it does not concentrated on other paths.

Disadvantages

- This method has lot of time to detect the malicious node.
- It reduce with the more energy
- This watchdog technique is costly

B. Dynamic watchdog

By using Dynamic watchdog technique is used to create shortest path between intermediate nodes to target node dynamically. Watchdog Location Optimization is to identify the nodes location. The dynamic watchdog optimization can improve the efficiency in a significant manner throughout the MANET. This technique is used to balance energy efficiency and security in terms of trust accuracy and robustness. While sending information from source to destination, in the path there will be many intermediate nodes. In this dynamic watchdog optimization method, the neighbour or nearest node will be changed as the watchdog node for the purpose of reducing the energy requirement. This watchdog is called as a dynamic watchdog. And also the watchdog frequency is optimized. Ultimate goal is to reduce the energy cost induced by watchdog tasks as much as possible, while keeping trust accuracy and robustness in a sufficient level. All the active nodes in MANET, Once the correct destination router is found, an end-to-end connection is established to carry end-system. This connection remains active as long as the file requested transferred and it is dynamically shut down when not in use.

Advantages

- This method has shortest time to find malicious node.
- Not require more cost.
- Increasing network lifetime
- Maintaining the security in sufficient level

C. Data Transfer

Intermediate nodes are computing or networking is a distributed application that partitions watchdog's task between source and target nodes.

These nodes are connected and communicate by using IP address and host name. Often Inheritor nodes operate over a network on separate functionalities.

A server machine is a high-performance host that is running one or more tasks which share its resources with nodes.

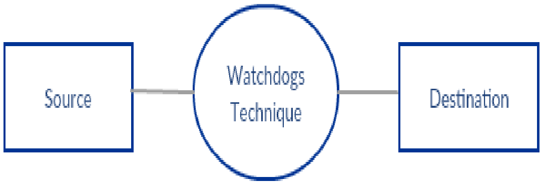

Fig 2: Watchdog Mechanism

In this paper the model of the trust of a sensor node as this node's expected behavior distribution over time. The behavior could be data sensing or routing behavior etc. This trust model can allow our analysis to be focused on WSNTS's foundation, and will not be affected by higher level's trust update and aggregation processes. In Fig. 2 shows the three concepts. One is trustworthiness that can be used to estimate a sensor node's behavior. The other two are trust accuracy and trust robustness, which can be used to measure how accurate the target nodes trustworthiness can be recovered in the presence of WSN attacks and WSNTS attacks respectively. Unlike the trustworthiness that the trust systems need to calculate at run time, the trust accuracy and trust robustness are two performance indices that to evaluate and compare different trust systems security levels. Trust systems do not need to compute the trust accuracy and robustness at run time.

D. Target Nodes

Choose the target node from the intermediate nodes. Then the number of connections to establish between each pair of target node and established between each and every nodes for network communication. From the source node to the destination node and intermediates node must have connection between source nodes after communicate between combinations of multi node each and every node must be link to each other.

After to choose the neighbor nodes and communicate with each other and also set the priority queue in the network communications. In multipath data transmission, send the data from source node that means which type of file size and file extension.

E. Energy Consumption Model

Energy-efficient trust model by applying a geographic target nodes to identify trust managers (may save energy due to low storage usage), while implemented an energy watcher to help sensor nodes estimate their neighbor nodes' energy cost for each packet forwarding and thus enable the selection of the most efficient node as their next hop in the route.

Watchdog Frequency Optimization techniques are used to estimate energy consumption of each node. The source node sends all type of file, and then enters the data send from source node to destination node over the network.

As well as data must be send from source node to intermediate node automatically in this module. The data's are successfully transfer from source to destination without attacks. Watchdog frequency is adjusted adoptively by referencing trust worthiness.

V. RESULT AND DISCUSSION

Simulation Configuration

The Simulation is carried out using the tool Network simulator 2 (NS-2) shown in the given below Table.

S.NO	Parameter	Value
1	Simulator	NS-2
2	Channel Type	Wireless channel
3	Routing protocol	AODV
4	Type of Traffic	CBR
5	MAC Layer	802_11
6	Grid size	500*500
7	No.of.Nodes	50 nodes

Comparison Results

In this work, the Dynamic Watchdog Optimization Technique is used to show the performance is better than the Static Watchdog method.

This is done by metrics like Throughput, Energy Level and Packet Ratio. The metrics are calculated for 50 nodes using Dynamic Watchdog Optimization Technique and the graph given below shows the proposed work compared to Static Watchdog technique.

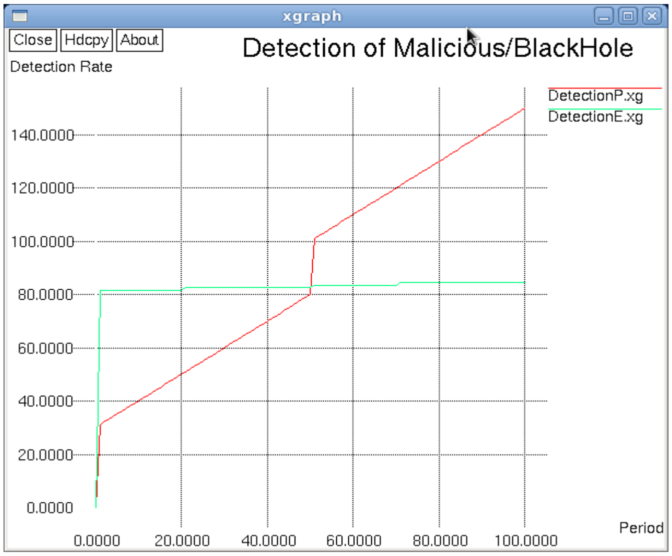

Fig 5.1 Comparison Result of Static and Dynamic atchdog Technique for Malicious Node Detection

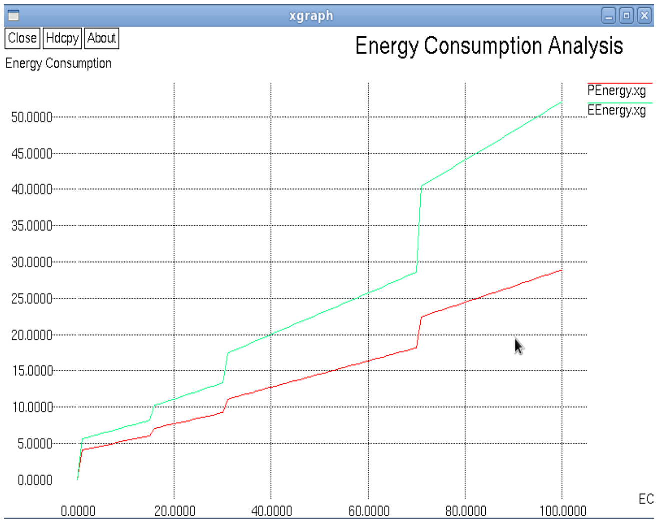

Fig 5.2 Comparison Result of Static and Dynamic Watchdog Technique for Energy Level Analysis

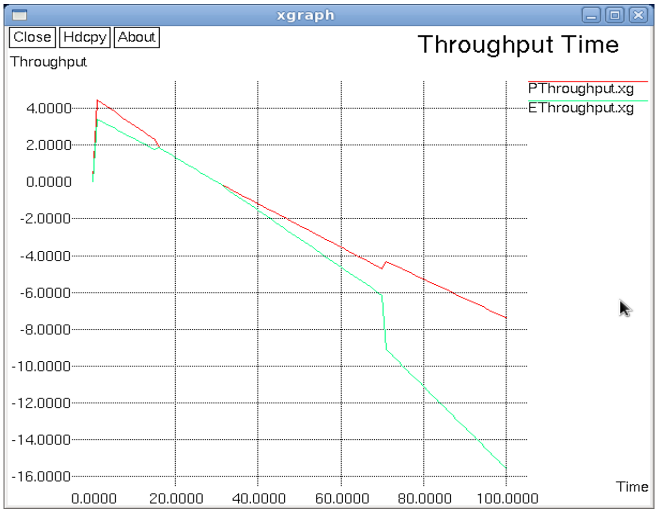

Fig 5.3 Comparison Result of Static and Dynamic atchdog Technique for Throughput

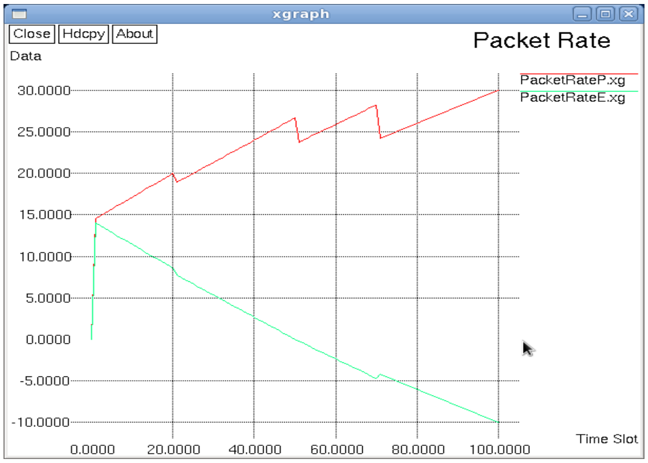

Fig 5.4 Comparison Result of Static and Dynamic Watchdog Technique for Packet Ratio

VI. CONCLUSION

MANET faces the security issues while sending the data through the wireless network. MANET user wants the secure data transfer of data. For this issues watchdog mechanism were provide to monitor the attackers.

The watchdog technique is a trust based attacker detection technique which identifies the malicious nodes and its activity in the network is to monitor the nodes within its communication range.

In existing static watchdog mechanism were used it provide lot of issues. It only find the attackers in the one path only, it does not concentrated on other paths.

The proposed Dynamic Watchdog algorithm can find a set of watchdog nodes by considering those nodes locations in a probabilistic manner and to create shortest path between source node and destination node. Then detect the malicious node and estimate energy units for each node. By using the dynamic approach it balances security issues hence it concentrate on each node in the network in terms of trust accuracy and robustness and increase network life time.

REFERENCES

[1] Singh UK, Mewada S, Iaddhani L, Bunkar K. "*An overview and study of security issues & challenges in mobile ad-hoc networks (manet)"*,International Journal of Computer Science and Information Security, Vol.9, Issue.4, pp.106-111, 2011.

[2] Amit Gupta and Dhananjay Bisen, "*Review of Different Routing Protocols in Mobile Ad-Hoc Networks*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.5, pp.105-112, 2015.

[3] Indhu Lekha, S.J., Kathiroli, R. "*Trust based certificate revocation of malicious nodes in MANET*", IEEE ICACCCT 2014, pp. 1185–1189.

[4] Pradeep Kumar Sharma, Shivlal Mewada and Pratiksha Nigam, "*Investigation Based Performance of Black and Gray Hole Attack in Mobile Ad-Hoc Network*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.4, pp.8-11, 2013.

[5] N.Soganile1 , T. Baletlwa , and B. Moyo "*Hybrid Watchdog and Pathrater algorithm for improved security in Mobile Ad Hoc Networks*", Int'I Conf.Wireless Networks ICWN'2015.

[6] SJI Lekha, S.J., Kathiroli, R., "*Trust based certificate revocation of malicious nodes in MANET"*, IEEE ICACCT ,pp 1185-1189, 2014.

[7] Zuckerman, M., Faliszewski, P., Bachrach, Y., et al. "*Manipulating the quota in weighted voting games"*. Conf. on Artificial Intelligence, pp. 215–220. 2008.

[8] Liu,W., Nishiyama, H, Ansari, N, Yang J, Kato N, "*Cluster-based certificate Revocation with Vindication Capability for Mobile Adhoc Networks*", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, Vol.24, No.2 pp 1 to 12, 2013.

[9] Izquierdo, L.R., Izquierdo, S.S. '*Dynamics of the Bush–Mosteller learning algorithm in 2 × 2 games*' (In Tech Publisher) 2008.

[10]Sungwook Kim "*Trust based dynamic bandwidth allocation scheme for Ethernet passive optical networks*", Wireless Personal Communications, Vol.83, No.4,pp. 2869–2882, 2015.

[11] Moretti Annoni M, Fernado Cruz, Goncalves Riso B, Westphall "*Wireless Communications : Security Management Against Cloned Cellular Phones*", Wireless Communications and Networking Conference-IEEE, pp 1412-1416, 1999.

[12] Pooja saini and Meenakshi Sharma, "*Impact of Multimedia Traffic on Routing Protocols in MANET*", International Journal of Scientific Research in Network Security and Communication, Vol.3, Issue.3, pp.1-5, 2015.

[13] J. Kaur, G.Singh, "*MANET Routing Protocols: A Review*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.3, pp.60-64, 2017.

Authors Profiles

R.Vadivel is a Assistant Professor in the Dept. of Info. Technology, School of CSE, Bharathiar University, Coimbatore, Tamil Nadu, India. He obtained his Diploma in Electronics and Communication Engineering from State Board of Technical Education in the year 1999, B.E., Degree in Computer Sci-ence and Engineering from Periyar University in the year 2002, M.E., degree in Computer Science and Engineering from Annamalai University in the year 2007 and Ph.D., degree in CSE from Manonmaniam Sundaranar University in the year 2013. He has published 20 papers in journals and 15 papers in Conferences both at National and International level. He is a life member of ISTE, ISCA, CSI and ACS, IAENG. Also he is an Associate Member of the Institution of Engineers (India) AMIE. His areas of interest include Computer Networks, Network Security, Information Security, etc.

Gayathri.c Pursing the M.Phil in Department of Info. Technology Bharathiar University, Coimbatore, Tamilnadu. And also she completed the M.sc., Degree in Information Technology from Bharathiar University during the 2015. Her Research interests include mobile ad-hoc networks.