International Journal of Emerging Technology and Innovative Engineering
Volume 2, Issue 1, January 2016 (ISSN: 2394 – 6598)

NODES ROUTING MECHANISM FOR MANET IN ADVERSARIAL ENVIRONMENT

DHAKSHINA MOORTHI P
Assistant Professor, Muthayammal Engineering College
Namakkal, India. Email: dhakshinamoorthitp@gmail.com

BOSELIN PRABHU S R, RAJKUMAR R
Assistant Professor, Department of Electronics and Communication Engineering
SVS College of Engineering, Coimbatore, India.

S. SOPHIA
Assistant Professor, Department of Electronics and Communication Engineering
Sri Krishna College of Engineering and Technology, Coimbatore, India.

***Abstract*—The Mobile Ad-hoc Networks (MANETs) is wired freely and dynamic self-organize into arbitrary and temporary network topologies. MANETs operates in different propagation and network operating conditions. For security purpose MANET operates on many security protocols, power/energy-efficient protocol. Many of an existing routing protocol for security enhancement is based on location based routing and some gets attack from the attacker and also provide delay in packet transmission. In this paper proposal routing protocol method is Trust model Authenticated Anonymous Secure Routing (TAASR). Group Signature and Onion Routing with the trust model increases the efficiency of routing in MANET. Group signature in this secure routing provides an managing keys for group node. TAASR protocol concept is to defend the neighbor nodes attack by the way of key-encryption and decryption in route-request and route-reply in group nodes. The calculating trust value of the nodes in MANET routing can helps to reduce the end to end packet transfer delay between nodes and TAASR provides better result when compared to an existing protocol.**

Keywords*— *Group Signature, Trust Model, Onion Routing, Mobile Ad hoc Networks

I. INTRODUCTION

The mobile communication is wireless communication; it is fully based on MANETs. Ad hoc network is wired free network, which makes connection between host embedded devices. MANET is a wireless and dynamic configuration for transferring the data between source and destination, it has no infrastructure and temporary established mobile communication. The nodes acts as a sender, receiver and intermediate nodes in data transferring channel. Because of dynamic connection MANETs are applicable to many wireless applications like battlefields, industrial conference, and co-operative industries. MANET has many security issues in data transmission such as unreliability, collision, energy-constraint in mobile nodes. An ad hoc network can be attacked from any direction at any node which is different from the fixed hardwired networks with physical protection at firewall and gateways. Each node in an MANET is to forward the packets and there is specific cooperation mechanism to forward from hop to hop, to reach the destination. Altogether it denotes that every node should be equipped to meet, both inside or outside attacker directly or indirectly. This paper is topology based MANETs, it has chance to get attack in its routing path for this consideration need authenticated based topology routing. Our anonymous communications in MANETs has unidentifiability and unlinkability [1]. Unindentifiability is the source and destination node cannot be identifying by the other nodes. Unlinkability is the route between the source and destination node cannot be linked directly together. The nodes in a MANETs are group together using Group Signature. Group Signature provides both public and private key for the nodes in routing. The public key provides the authentication for nodes involves in routing and private key provides the nodes identity for involving in routing process. Both public and private key to selects the authenticated mobile nodes in adversarial environment [2]. The trusted nodes are identifying group nodes by calculating trust value. The trust value is calculated from rate of success and rate of failure of the packet transfer between source and destination. The trust nodes are reliable node in security routing, efficient in reducing the data transfer delay and increase the throughput.

Trusted nodes send the secure data in routing path by the way of onion routing, it provides a vital role in the security enhancement in packet transfer. The onion routing makes the data encryption, while forwarding the packet from source to destination and decryption of data when the reversing from destination to source in adversarial environment [3]. The forward packet is Route Request (RREQ) from source to destination and backward the packet is Route Response (RREP) from destination to source.

II. RELATED WORK

Some of the related works for this paper are as follows. Nodes can be punished or rewarded by decreasing or increasing the trust counter or threshold value. The protocol provides link-layer security using Cipher Block Chaining (CBC) mode of authentication and encryption [4]. The trust value can be favor packet forwarding by maintaining a trust counter. In the trust model, packet forward end to end delay can be decrease.

Anonymous routing protocols that hide node identities and routes from outside observers in order to provide an anonymity protection[5]. This protocol supports either hop-by-hop encryption or redundant traffic; either generates high cost or cannot provide full anonymity protection to data sources, destinations and routes. This protocol is not provides full security for all the attack. It avoids the passive attacks and it supports notify mechanism and it produce high delay when packet sending.

Operates in hostile or suspicious setting requires communication security and privacy, especially in routing protocols [6]. It achieves privacy and security against both outsider and insider adversaries. The protocol resists the node tracking by degree of topology exposure in link-state based approaches. The security, privacy and performance of PRISM and PRISM is more efficient, it offers better privacy than prior work.

Nodes are identities must not be exposed and node movements should be untraceable and need to communicate on the basis of their current locations [7]. This protocol evaluates the scalability of nodes and reduces the traffic control. This protocol of MANET occurs in high security and privacy guarantees and ALARM offers performance tradeoffs in the context of link state MANET routing.

Mostly the routing process supports peer to peer communication, this mechanism misbehaving of nodes are isolate and trusted based reliable nodes are involves in routing [8]. The reliability using trust value of nodes and its energy constraints will better for MANET routing. This protocol gives better performance in PDR, decrease in delay and throughput.

MANET is self-organizing and no fixed topology connection between source and destination [9]. So it has chance for getting attack from the attacker in way of modifying and hacking the data in routing path. The trust based protocol gives the trusted routing path for secure communication by understanding the routing protocols.

MANET gets many attacks due to dynamic connection, the performance of this protocol against malicious nodes [10]. The protocol can avoid the selfish nodes in both cases forwarding and reversing. The malicious nodes can be avoided by secure routing protocol.

This survey gives various trust approaches to detect the trusted node [11]. The trusted nodes provide secure and good performance in routing for both dynamic location-based and topology based connection.

III. METHODOLOGY

Some of the techniques in anonymous communications to makes routing path.

A. Group Signature

Group Signature is a method for allowing members of a group to sign anonymously in a MANET routing protocol. Group Signatures can be viewed as traditional public key signatures with additional privacy features. This approach is to run a group key agreement protocol at the beginning of every time slot and use the resulting group key as the common parameter and scalable. The more efficient approach is to use a group key agreement protocol in order to agree on the common parameter and group manager to generate and distribute this starting value. Group Signature scheme has group manager, who is response for adding new members and revoking signature of individual nodes in anonymity are given to a group manager.

Public Key: key this is common to all the members of a group

Private Key: key which gives privacy for the data of individual members in a group.

B. Trust based

The trust is the authenticated as the degree of subjective belief about the behaviors of a sufficient entity. Trust node is the probability by which an individual node performance of anonymous routing in adversarial environment. Trust node is related to performances of nodes in the data reputation and recommendation. Trust nodes of anonymous communication in adversarial environment responses for reducing delay in data packet transmissions.

C. Onion Routing

Onion routing protocol is a technique for connection establishment and keying for anonymous communication. Messages are repeatedly encrypted the information when sent source to destination nodes in Route-Request of onion routers [7]. In Route-Request has each onion router nodes removes a layer of encryption and uncover routing information when sends the message from destination node to the source node. This prevents these intermediary nodes from knowing the origin, destination and contents of the message. A routing onion is a data structure formed hide layer (encrypted) for forwarding a text message with successive layers of encryption [12]. In such a way each node formed unhide layer (decrypted) for backward a text message with successive layer of decryption, the original plaintext message only being viewable to sender and recipient. It is end to end encryption and decryption process between the source and the destination in adversarial environment.

D. Trapdoor

Trapdoor is widely used in cryptography and gives a one-way communication and difficult to use in the opposite direction without special information between two sets. A

padlock and its key , it is trivial to change the padlock from open to closed without using the key, by pushing the shackle into the lock mechanism. Opening the padlock easily to source – destination by accessing pre- established key to be used [8]. A trapdoor in cryptography has the very specific aforementioned meaning and it is not to be confused with a backdoor.

Trust in MANETs is a degree of the belief that a node in a network or an agent in a distributed system will carry out tasks. In direction observation trust, an observer estimates the trust of his one-hop neighbor based on its own opinion. Therefore, the trust value (T) is the expectaction of a subjective probability that a trustor uses to decide whether or not a trustee is reliable. In the direct observation, we assume that each observer can overhear packets forward by an observed node and compare them with original packets, so that the observer can identify the malicious behaviors of the observed node. Therefore, the observer node can calculate trust values of its neighbors. In order to obtain less biased trust value (T), we also consider other observers opinions in our project. If the trust value (T) is less than the threshold value (λ), the node will be fixed as untrusted node and will not be considered for further transmission.

IV. OBJECTIVES AND OVERVIEW OF THE PROTOCOL

A. Objectives

In this paper, trust-based protocol carries the secure data between source and destination. This protocol increases the performance of MANETs in both cases RREQ and RREP, having following objectives:

Privacy: Nodes in group having public factor which cannot access specific node, so private keys are used for accessing the node.

*Network security***:** Facility to resist the attack, the network itself detecting and eliminating the source of attacks.

Trust based: Trust nodes with minimum threshold value nodes are involves in data transmission, so it provide high security.

Performance: Privacy and network security is goal, which cannot reduce the performance of MANET.

B. Overview of protocol

This protocol forwards the packets in trusted nodes, which provide security in data transmission. The group signature and provides key for obtaining authenticate node. The trust based nodes are obtained from authenticated node in a group, by evaluating the threshold level [13] – [15]. Onion routing provides key-encryption and decryption of data in both forward and reverse transmission. The source and destination nodes are accessing the data shared key mechanism using trapdoor during transmission as shown in figure.1. This protocol dynamically calculating the nodes trust value, the source node can select the intermediate for transmitting the packet to the destination node. The trusted mechanism provide the reducing end to end packet transfer delay, increase throughput and steady state energy consumption.

V. TRUST MODEL IN MANET

A. *Definition*

In adversarial environment, an ad hoc network can get the attacker from any direction by any node in fixed network. This attack can be protected by making security firewall and gateways. Malicious nodes are formed by attacker; these nodes are initiated from both inside and outside of the network. A specific node is difficult in large ad hoc networks; it is more dangerous and much difficult to detect the attacks from an affected node. It denotes that every node should be prepared to work in a way that it should not trust on any node immediately. The trust model in ad-hoc networks is important as a result high security and improves efficiency within the network.

B. *Trust based scheme*

In trust based authenticated anonymous secure routing a dynamic ways of calculating trusted nodes to make routing path in MANET. This routing protocol identifies the malicious node in the network by the way of given threshold value in group nodes. The routing protocol calculates dynamic way of trust nodes in routing path and gives topology based communication in adversarial environment.

The trust counters of the values T_1, T_2, T_3… for the nodes n_1, n_2, n_3… in routing path for source and destination connection. When normal routing path from source to destination the nodes are both trusted and untrusted, so it makes routing delay and high packet loss ratio.

During routing request (RREQ) packets are forwarding from source to destination is said to be forward counter. If the forward counter value is greater than threshold value, then it is forward trust nodes,

$$F_n \geq \text{Threshold value}$$

F_n – number of forward counter trust nodes

When forwarding the data from source to destination gives trust forwarding node by threshold value.

During routing reply (RREP) packets are reversing from destination to source is said to be reply counter.

The destination D receives a packet from source node through RREQ message and the packet received is measured in throughput.

The number of success ratio in packet received is calculated by,

$$S = P_{Forward} / P_{Received}$$

$P_{forward}$ – Number of packets forward from source.

$P_{received}$ – Number of packets received to destination.

The destination D sends the data packet forward in between source S and destination D through intermediate node. If the node receives the packet successfully through trust node, it gives

$$T_{Fn} = T_{Rn}$$

T_{Fn} – trust forward nodes

T_{Rn} – trust reverse nodes

VI. Attacker in Adversarial Environment

In adversarial environment, attacker affected nodes in both insider and outsider manner. Attack can be performed either from outside of the group entity is outside attack and from within the group by an insider that already has certain access to the network is inside attack [16]. The attacker initiates the malicious node to make modify, access the data in a network.

Passive attacker: Monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active attacker: The attacker tries to bypass or break into secured systems. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave and attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, Denial of Service (DoS), and modification of data.

Insider attacker: The attacker inside the group nodes has resulted both malicious and no malicious node. The malicious node provides unsecure data transmission in a group and it can access the data from authorized user.

External attacker: The attacker hacks the data from outside the group. It is unauthorized node from outside and access the data in a group.

Hijack attacker: The attacker hacks the data during communication between two nodes in particular session. It acts as an authorized node or actor node for hacking the data.

Close in attacker: The attacker involves in modifying, access of information in communication network. This attacker attacks a personal communication like mobile call accessing in network.

VII. Performance Evaluation

A. Simulation Parameter

The simulation parameters are shown in the table.1

B. Performance Metrics

The performance of the system can be calculated for measuring an efficiency of the system.

End to End Delay: Transferring packets from the source to the destination.

Packet Delivery Ratio: Ratio of the number of packets received to destination and number of packets transmitted from source.

Throughput: Number of packets received successfully to the destination at particular time.

Energy Consumption: Trust based model achieves nodes require steady state energy.

C. Result

In TAASR four groups of simulation result can be graphed for exposing the efficiency that as follows. The comparison of two protocols AASR and TAASR are given in graphical representation from simulation result. TAASR provides better result than AASR in increasing throughput, decreasing end to end delay, packet delivery ratio and steady state energy consumption.

TAASR gives better throughput result than AASR. The ratio of TAASR has 15% increasing packet throughput than AASR in figure.2. The ratio of TAASR has 20% increasing packet delivery ratio than AASR in figure.3. TAASR reduce 55% of delay than AASR in figure.4, and steady state power consumption as shown in figure.5.

VIII. Conclusion

In this paper, the design of trust based authenticated anonymous routing protocol design for MANETs in anonymous condition. It uses trust values to favor packet forwarding by maintaining a trust counter for each node. If the trust counter value falls below a threshold, the corresponding intermediate node is malicious node. In this proposed scheme, authorized node has high throughput and packet delivery ratio can be improved significantly with decreasing average end to end delay by increasing trust value.

Parameter	Value
Network Simulator	NS 2.34
Traffic Source	CBR
Number of nodes	50
Transport Protocol	UDP
Area Size	1250x1250
MAC Protocol	802.11
Packet Size	512 Bytes
Mobility Model	Random
Transmission Power	1.5 Joule
Receiving Power	1 Joule
CBR Transmission Interval	0.05ms

Table.1 Simulation Parameter

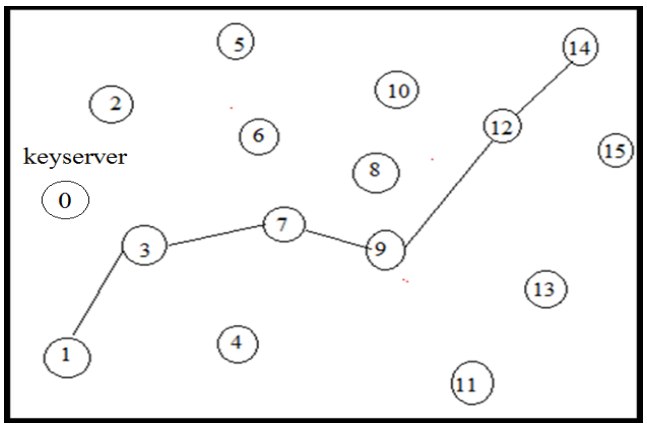

Figure.1 Trust based MANET Routing

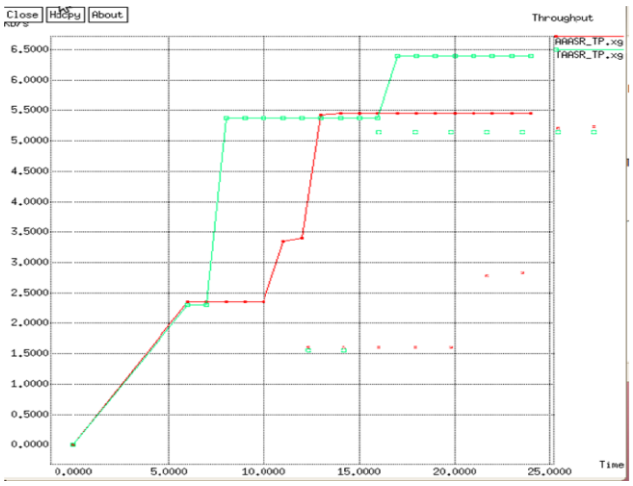

Figure.2 Comparison of TAASR Throughput and AASR Throughput

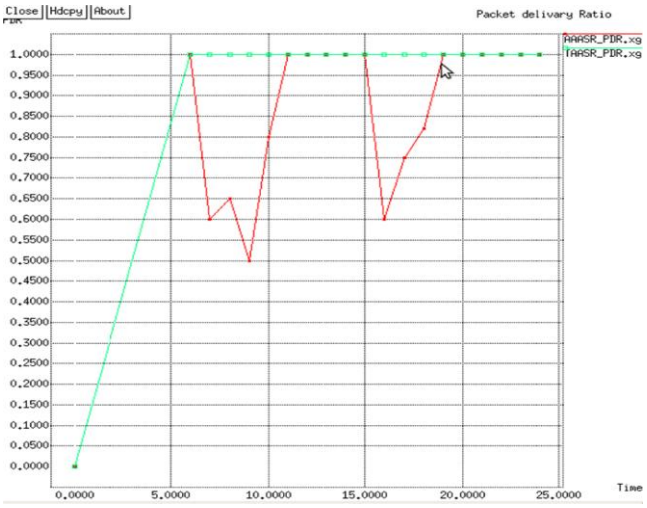

Figure.3 Comparison of TAASR PDR and AASR PDR

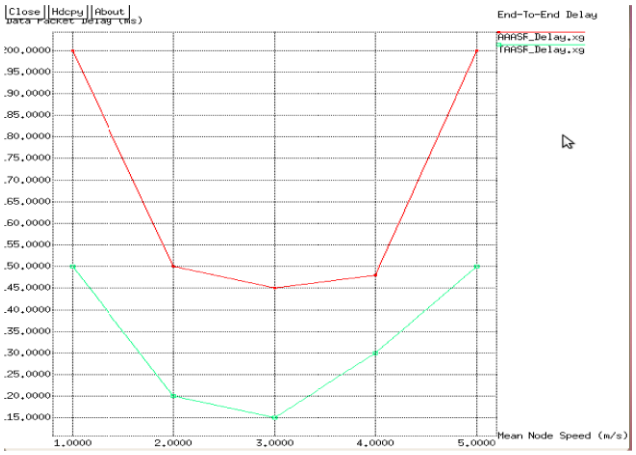

Figure.4 Comparison of TAASR Delay and AASR Delay

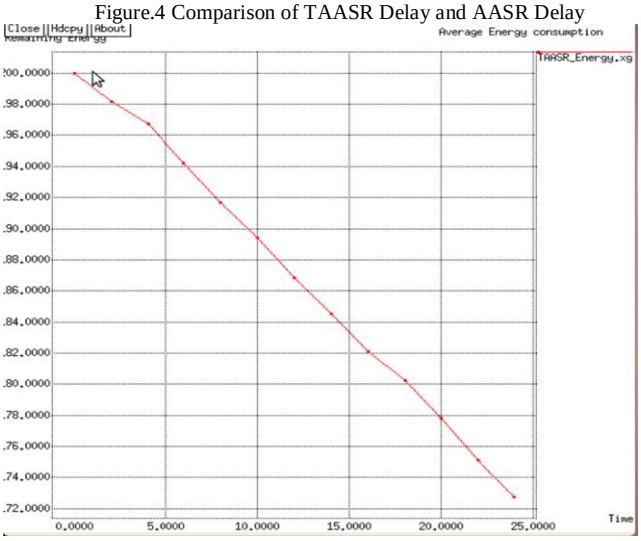

Figure.5 Steady State TAASR

REFERENCES

[1] Wei Liu and Ming Yu, "AASR:Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments," *IEEE Transaction On Vehicular Technology*., vol. X, no. Y, May 2014.

[2] Yanchao Zhang, Wei Liu, and Wenjing Lou, " Anonymous Communications in Mobile Ad hoc Networks, " in *Proc. IEEE INFOCOM* 2005, vol. 3, pp. 1940-1951, Mar.2005.

[3] Zheiong Wei, Helen Tang, F.Richard Yu, Maoyu Wang and Peter Mason, " Security Enhancements for Mobile Ad hoc Networks with Trust Management Using Uncertain Reasoning, " *IEEE Transaction On Vehicular Technology*, vol. X, no. Y pp. 1-12, 2013.

[4] A.Rajaram and Dr.S.Palaniswami, " Detecting Malicious Node in MANET Using Trust Based Cross-Layer Security Protocol, " *International Journal of Computer Science and Information Technologies*, vol. 1(2), pp. 130-137, 2010.

[5] H.Shen and L.Zhao, " ALERT:An Anonymous Location-based Efficient Routing Protocol in MANETs, " *IEEE Trans. on Mobile Computing*, vol. 12, no. 10, pp. 1079-1093, 2013.

[6] K.E.Defraway and G.Tsudik, " Privacy-Preserving Location-based On-Demand Routing in MANETs, " *IEEE Journal on Selecting Areas in Communications*, vol. 29, no. 10, pp. 1926-1934, Dec.2011.

[7] K.E.Defraway and G.Tsudik, " ALARM: Anonymous Location-Aided Routing in Suspicious MANETs, " *IEEE Trans. on Mobile Computing*, vol. 10, no. 9, pp. 1345-1358, Sept.2011.

[8] Sridhar Subramaniam and Basakaran Ramachandran, " Trust Based Scheme for QoS Assurance in Mobile Ad hoc Networks, " 2013.

[9] S.Geetha and G.Geetha Ramani, " Survey of Trust Based Routing Protocols in MANET, " *International Journal of Advanced Research in Computer Science and Software Engineering*, vol.4, Issue.10, pp.604-608, Oct.2014.

[10] Yaser Khamayseh, Ruba Al-Salah and Muneer Bani Yassein, " Malicious Nodes Detection in MANETs:Behavioral Analysis Appoach, " *Journal of Networks*, vol. 7, no. 1, pp. 116-125, Jan.2012.

[11] Kannan Govindhan and Prasant Mohapatra, " Trust Computations and Trust Dynamics in Mobile Ad hoc Networks: A survey, " 2014.

[12] G.Reed and Paul F.Syverson and David M.Goldschlag, " Anonymous Connection and Onion Routing, " *IEEE Journal on Selecting Areas in Communications*, vol. 16, no. 4, pp. 482-494, May.1998.

[13] Hui Xia, Zhiping Jia, Lei Ju, Xin Li, and Youqin Zhu, " A Subjective Trust Management Model with Multiple Decision Factors for MANET based on AHP and Fuzzy Logic Rules, " IEEE/ACM I*nternational Conference on Green Computing and Communications*, 2011.

[14] Philip England, Dr.Qi Shi, Dr.Bob Askwith, and Dr.Faycal Bouhafs, " A Survey of Trust Management in Mobile Ad-Hoc Networks, " 2012.

[15] Renu Dalal, Manju Khari and Yudhvir Singh, " Different Ways to Achieve Trust in MANET, " *International Journal on Adhoc Networking Systems*, vol. 2, no. 2, Apr.2012.

[16] Vidya N.Patil and S.A.Thorat, " Cross Layer Approach to Detect Malicious Node in MANET, " International Journal of Current Engineering and Technology,Issue.1, pp. 244-248, sep.2013.

AUTHOR'S PROFILE

Dhakshina moorthi.P obtained his bachelor's degree in electronics and communication engineering from Anna University and currently pursuing master of engineering in embedded system technologies from Anna University, Chennai, India. He was worked as a network engineer in industries. His research areas of interest include Wireless Sensor Networks, Mobile Ad-Hoc Networks and real time applications. He has published records of papers in International Journals and Conference Proceedings. He is currently a member of IAENG, IAETSD, CSTA, SDIWC and IACSIT.

Boselin Prabhu.S.R obtained his bachelor's degree in electronics and communication engineering and master's degree in network engineering. He is currently working towards doctorate in wireless sensor networks, with the department of information and communication engineering, Anna University, Chennai, India. He is currently working as an Assistant Professor with 6 years of experience in teaching and research. His research areas of interest include Wireless Sensor Networks, Mobile Networks and Ad-Hoc Networks. He has published more than 36 papers in International Journals and Conference Proceedings. He is currently a member of ISTE, IETE, PASS, CIR, ISOC, SSRG, SCIEI, IAENG, IAENG SOC, IRED, CSTA, OSPE, IAOE, UACSE, IACSIT, ASET, SDIWC, UACEE and ICST. He is an editorial board member, advisory board member and reviewer of AJCRR, JOHRE, JOHRM, JAP, IJACT, IJMCN, IJICS, SSRG, IJIMRA, IJR, IJTEL, SciEP, Pubicon, IJCTT, AJEEE, AJCSES, AJCSIT, IJCSBI, IJRECE, IJERT, IJRCAR, GJESR, JISCT, JOHRAS and IJCSCN. He is elected as a fellow member of ISECE (Malaysia) and UAAMP (USA), associate member of UACEE (USA) and senior member of UACSE (USA). He has reviewed more than 32 research articles for leading International Journals. He has attained Google scholar citations-44, h-index-04 and i10-index-01. As a young researcher, he is a biographical world record holder of Marquis Who's Who in the World (32nd Edition) for his outstanding contribution towards research community. He has written one book (electronic circuits-II) for engineering students.