International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 2, ISSN 2249 –071X

Performance Analysis of SAODV with DOS Attack

S.Madhavi **K.Duraiswamy** **B.Kalaavathi** **S.Vijayaragavan**

maha2002saro@yahoo.co.in

Abstract **- Protection against Denial of Service (DOS) attacks is critical component in any security system especially for wireless networks. Particularly Mobile Ad hoc Network (MANET) applications are deployed into battleground and its nature of the networking is also susceptible to attacks like DOS. Routing plays an important role when communication is established between the nodes in the network. Based on the nature of the communication and the importance of the transferring message between the nodes, the secure routing can be considered as an essential factor in the networking environment. This paper details about DOS attack and its impact based on the simulation results of SAODV with attacker scenario for DOS.**

Key Words **- Attacker, DOS, MANET, Routing.**

I. INTRODUCTION

MANET is a collection of mobile nodes with wireless network interface forms temporary network without any fixed infrastructure. Mobile nodes in this network dynamically set up paths among mobile nodes and transmit packets. In this network, routing involves various phases; they are route discovery, route maintenance and data forwarding. In this network, a node may be either a sender, or a receiver or a forwarder. If the sender and receiver mobile nodes are within one hop distance, they can transmit their packets directly; otherwise they transmit the packet with the help of forwarder nodes. This shows the dependency nature of this network. Since the most of the transmission takes place with the help of forwarders, they play a major role in this network environment. Based on the behaviour, a node can be classified as either an altruist, or an egotist or an introvert. This behaviour creates the non co-operation between the nodes and affects the performance of the whole network. The cooperation between the nodes is the major issue in MANET; hence security is needed to achieve authentication, confidentiality, integrity, non-repudiation and availability.

In general DOS attacks play active role in the two layers of protocol stack such as MAC and network layer. This attack is hard to detect but implementation of this attack is not so difficult. No hardware is required to launch this attack. This attack is one of the most dangerous attack affect the network layer. Presence of this attacker may lead to shutdown the network process. So nodes are unable to discover a route between the source and destination. The rest of the paper is organized as follows. The section 2 presents different types of DOS attacks and security attacks on protocol stacks. In section 3 the overview and security flaws of AODV is discussed. The section 4 explores overview of SAODV and which types of attacks are vulnerable to SAODV. Attacks scenarios and attacker free scenarios of SAODV are discussed in section 5. Conclusion of the work is shown in the section 6.

II. METHODS

Security can be achieved in a MANET in three different methods - providing security for basic infrastructure, secure routing and misbehaviour detection and response. The first method, secured infrastructure, provides security associations between the nodes. The second method, secure routing, provides security for both route discovery and data forwarding phases. The third method misbehaviour detection and removal, detects the attack if it is launched by any attacker and provides necessary steps to remove the attacker from that scenario. This paper explores the concepts of attacks and attacker actions and their impact, particularly DOS.

III. CLASSIFICATION OF ATTACKS

In general, attacks on wireless networks fall into four basic categories: passive attacks, active attacks, man-in-the middle attacks, and jamming attacks. A passive attack occurs when someone listens to or eavesdrops on network traffic. Wireless communication takes place on unlicensed public frequencies—anyone can use these frequencies.

A. Passive Attacks

Passive attacks are and by their nature very difficult to detect. Once an attacker has gained sufficient information from the passive attack, the hacker can then launch an active attack against the network. There are potentially large numbers of active attacks that a hacker can launch against a wireless network. Some general types of passive attacks are interruption, modification, fabrication and interception.

B. Active Attacks

Active attacks perform some modification either on data or on control packets or it creates a false control packet or data packet and send it to their neighbour. Active attack is of two types such as external and internal. An external attack is one caused by nodes that do not belong to the network. An internal attack is one from either compromised or hijacked nodes that belong to the network. These attacks replace, replay and modify the message and results in DOS. This paper explores only the concepts of DOS attack in MANET.

C. Man-in-the-Middle Attack

Man-in-the-middle attack refers to the type of attack where the attacker intrudes between the communication endpoints of a network to inject false information and

intercept the data transferred between them. Man-in-the-Middle attacks are usually selected by hackers against public-key cryptosystems. In a public key scenario, hackers may substitute the intercepted public key with their forged public keys. In such cases, the casualty parties are made to believe that they remain safe in communicating with each other.

D. Jamming Attack

In an open medium, jamming can be a huge problem for wireless networks. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless networks can no longer function.

IV. CATEGORIZATION OF ATTACKERS

Outsider and insider are the categories of attackers in MANET. Outsider attackers mean the nodes who are not a member in the active communication process. That outside member performs illegal actions to disrupt the networking operations, they will be considered as non-member attacker. The members who are actively participated in the communication process, if they are doing some wrong operations, it may collapse the communication process, they will be considered as member attacker. The insider attacker's attacks can be categorized into atomic and compound [13]. Atomic actions are performed manipulating single routing message. Some atomic misuses are drop, modify and forward, forge reply and active forge. Compound actions are composed of atomic actions; it can be divided into many single pieces of atomic actions.

V. ATTACKERS BEHAVIOUR

Behaviour of attacker nodes can be classified into two types such as selfish and malicious. Naturally selfish behaviour node motive is to improve performance and resource saving of its own. So it is not interested to play the forwarder role in an active manner, when it receives either the data or control packet, simply ignores the process of forwarding. This selfishness node intention is to save the battery power for future use of its own because all wireless devices are operated with the help of battery power. This activity partially affects the network operations. The malicious node tries either to disrupt the activities of the network or degrade the performance of the network. Disruption in the routing and forwarding process and more resource consumption in the participated networking environment are exhibited by poisonous nodes actions. The characteristics of these actions may be unnecessary dropping of packets, flooding the packets and misguiding the packets. Due to this lacking of cooperation, security plays a major role to achieve the flourishing communication process.

VI. TYPES OF DOS ATTACKS

Based on the node behaviour in different environment of MANET, new type attacks are identified. Here some identified attacks are discussed as follows.

Black Hole Attack: it is one type of DOS attack. Attacker node sends false RREP message to the source node with highest sequence number. Legitimate source node sends the data packets through the attacker node, that node simply drops the packet without forwarding the packets to the proper destination.

Wormhole Attack: In this attack, the attacker records all routing information. Two different end located attackers get connected, record the packets, and replay the packets at other end. This attack replays the valid information at different place.

Flooding Attack: This attack floods the false control packets such as RREQ, Hello, which creates congestion in the network. This type of attack prevents the transmission of route discovery packets between the nodes in the network. This kind of DOS attack may lead to network failure.

DOS attacks are very dangerous attack in the network. The Table I shows few examples of attacks at each layer in the protocol stack.

TABLE I - ATTACKS ON THE PROTOCOL STACK

Layer	Attacks
Application	Data Corruption, Viruses and Worms
Transport	TCP/UDP SYN Flood
Network	Hello flood, Blackhole, Wormhole
Data link	Monitoring, Traffic Analysis
Physical	Eavesdropping, Active interference

VII. OVERVIEW AND SECURITY FLAWS OF AODV

AODV is an on-demand MANET routing protocol. It consists of two phases - route discovery and route maintenance [14]. This on-demand routing protocol, facilitates a smooth adaptation to changes in the link conditions. In the case of link failure, notifications are sent only to the affected nodes. This information enables the affected nodes to invalidate all the routes through the failed link. It has low memory overhead, builds unicast routes from source to the destination and network utilization is minimal. There is minimal routing traffic in the network since routes are built on demand. It does not allow nodes to keep routes that are not in use. When two nodes in an ad hoc network wish to establish a connection between each other, AODV will enable them to build multihop routes between the mobile nodes involved. AODV is loop free. It uses Destination Sequence Numbers (DSN) to avoid counting to infinity. This is one of the

distinguishing feature of this algorithm. Requesting nodes in a network send DSNs together with all routing information to the destination. It also selects the optimal route based on the sequence number [8].

AODV defines three messages: Route Requests (RREQs), Route Errors (RERRs) and Route Replies (RREPs) [14]. These messages are used to discover and maintain routes across the network from source to destination by using UDP packets. Whenever there is need to create a new route to the destination, the requesting node broadcasts an RREQ. A route is determined when this message either reaches the next hop node (intermediate node with routing information to the destination) or the destination itself and the RREP has reached the originator of the request [10]. Routes from the originator of the RREQ to all the nodes that receive this message are cached in these nodes. Whenever there is a link failure, an RERR message is generated. This message contains information about the nodes that are not reachable because of this failure. It also contains IP addresses of all the nodes that were using it as their next hop to the destination.

To protect an ad-hoc network from attacks a routing protocol must fulfill a set of requirements [3] to ensure that the discovered path from source to destination functions properly in the presence of malicious nodes. These are:

- Authorized nodes should perform route computation and discovery,
- Minimal exposure of network topology,
- Detection of spoofed routing messages,
- Detection of fabricated routing messages,
- Detection of altered routing messages,
- Avoiding formation of routing loops, and
- Prevent redirection of routes from shortest paths.

Early stages of MANET routing protocol won't consider the security requirements of the network. Hence most of the initial routing protocols do not satisfy the above mentioned requirements.

This part analyzes the security threats and describes the requirements for AODV routing protocol to mitigate these threats. A node is malicious if it is an attacker that cannot authenticate itself as a legitimate node due to the lack of valid cryptographic information. A node is compromised if it is an inside attacker who is behaving maliciously but can be authenticated by the network as a legitimate node and is being trusted by other nodes. A node is selfish when it tends to deny providing services for the benefit of other nodes in order to save its own resources. Several attacks can be launched against the AODV routing protocol.

Message tampering attack: An attacker can alter the content of routing messages and forward them with falsified information. For example, by reducing the hop-count field in either an RREQ or RREP packet, an attacker can increase its chance to be an intermediate node of the route. A selfish node can relieve the burden of forwarding messages for others by setting the hop-count field of the RREQ to infinity. Simulation results in [13] show that a single attacker can drop up to 75% of packets by manipulating destination sequence numbers in some scenarios.

Message dropping attack: Both attackers and selfish nodes can intentionally drop some (or all) routing and data messages. Since all the mobile nodes within a MANET function as both end hosts and routers, this attack can paralyze the network completely as the number of message dropping increases.

Message replay (or wormhole) attack: Attackers can retransmit eavesdropped messages again later in a different place. One type of replay attacks is the wormhole attack. A wormhole attacker can tunnel an RREQ directly to a destination node. Since a wormhole attacker may not increase the hop-count field value, it prevents any other routes from being discovered. The wormhole attack can be combined with the message dropping attack to prevent the destination node from receiving packets. The security requirements for AODV routing protocol includes [15] as follows:

Source authentication: The receiver should be able to confirm that the identity of the source is indeed who or what it claims to be.

Neighbour authentication: The receiver should be able to confirm that the identity of the sender (i.e., one hop previous node) is indeed who or what it claims to be.

Message integrity: The receiver should be able to verify that the content of a message has not been altered either maliciously or accidentally in transit.

Access control: It is necessary to ensure that mobile nodes seeking to gain access to the network have the appropriate access rights.

VIII. Overview of SAODV and Security Flaws

Secure AODV (SAODV) [4,6,7] is a security extension of the AODV protocol, based on public key cryptography. SAODV routing messages (RREQs, RREPs, and RERRs) are digitally signed to guarantee their integrity and authenticity. Therefore, a node that generates a routing message signs it with its private key, and the nodes that receive this message verify the signature using the sender's public key. The hop count cannot be signed by the sender, because it must be incremented at every hop. Therefore, to protect it, a mechanism based on hash chains is used. In its basic form, this makes it impossible for intermediate nodes to reply to RREQs if they have a route towards the destination, because the RREP message must be signed by the destination node.

In order to preserve the collaboration mechanism of AODV, SAODV includes a kind of delegation feature that allows intermediate nodes to reply to RREQ messages. This is called the double signature. When a node 'A' generates a RREQ message, in addition to the regular

signature, it can include a second signature, which is computed on a fictitious RREP message towards 'A' itself. Intermediate nodes can store this second signature in their routing table, along with other routing information related to node 'A'. If one of these nodes then receives a RREQ towards node 'A', it can reply on behalf of 'A' with a RREP message, similarly to what happens with regular AODV. To do so, the intermediate node generates the RREP message, includes the signature of node 'A' that it has previously cached, and signs the message with its own private key.

SAODV does not require additional messages with respect to AODV. Nevertheless, SAODV messages are significantly bigger, mostly because of digital signatures. Moreover, SAODV requires heavyweight asymmetric cryptographic operations: every time a node generates a routing message, it must generate a signature, and every time it receives a routing message (also as an intermediate node), it must verify a signature. This gets worse when the double signature mechanism is used, because this may require the generation or verification of two signatures for a single message. In the SAODV operations, SAODV allows to authenticate the AODV routing data. Two mechanisms [9, 10] are used to achieve this: hash chains and signatures. They used signatures for authentication and hash chains for integrity of the routing messages.

The SAODV protocol has not designed to withstand DOS attacks [17]. SAODV provides a cryptographic solution to secure routing control messages. However, SAODV still has vulnerabilities to attacks by captured or subverted insider nodes and even to unauthenticated

dropping data packets while Jellyfish attacks[1] achieve this by manipulating the transport layer protocol. MAC

transmission by surrounding nodes. Wormholes and Rushing attacks [15] allow attraction of routes to increase the effectiveness of data interception or Black-hole/Jellyfish attacks. Hop count protection is not perfect because it does not prevent a malicious node from leaving the hop count unchanged [1].

IX. Scenario and Environment Settings

The scenario and the environment settings are fixed and dynamic. The routing protocol SAODV performance compared in a chosen free-attack and attacker. Table II details the parameters and values of the simulation environment.

II. Simulation Settings

Parameters	Values
Topology Size	800 × 800
Communication Traffic	CBR
Varying Number of Nodes	50,60,70,80,90,100
Varying Speed	0.5 to 3.0 m/sec
Mobility Model	Random Way point
varying pause time	0, 5,10,15,20,25 sec
data transfer rate	512 kbps
total simulation Time	200 seconds

This simulation is based on an 800 × 800 meter flat space, scattered with varying number of nodes from 50 to 100. Each simulation is executed for 200 seconds of simulation time. The random way point model is utilized as mobility model. In this network set up, the node speeds are varied from 0.50 m/sec to 3 m/sec. Pause time is varied from 0 seconds to 30 seconds. This set up is to analyze the performance metrics like Packet Delivery Ratio (PDR), delay, throughput, packet loss , control overhead and routing overhead with and without attacker scenario.

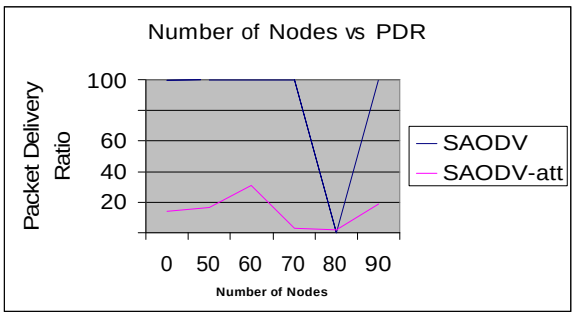

Fig.(a) PDR with varied number of nodes

The fig.(a),(c),(d) evaluated the PDR with varied number of nodes, Pause time and node speed. In the entire cases attacker free set up of SAODV perform better compared with SAODV with attacker set up. We observed from that simulations results presence of attacker in the network environment surely affects the performance of the routing protocol.

The fig.(b) evaluated packet losses compared with varying node speed. In an attacker free set up packet loss is 0.85% and an attacker set up packet losses are 57.05%.

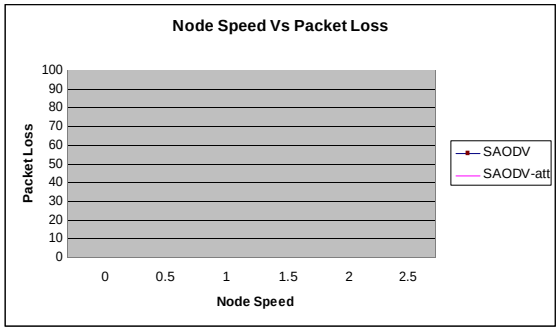

Fig.(b) Packet loss with varied node speed

In fig.c. shows varying mobility with packet delivery ratio. The results shows attacker free environment gives 83.15 % and attacker environment gives 32.33%.

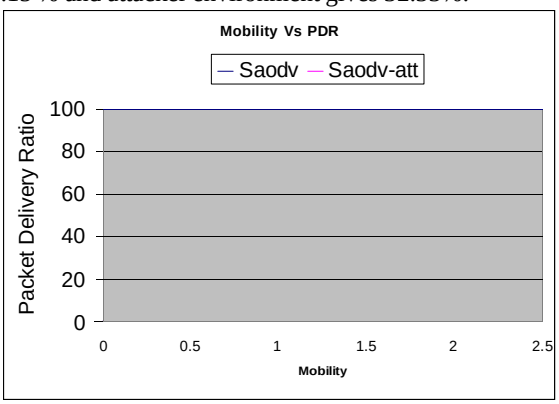

Fig.(c) PDR with varied mobility

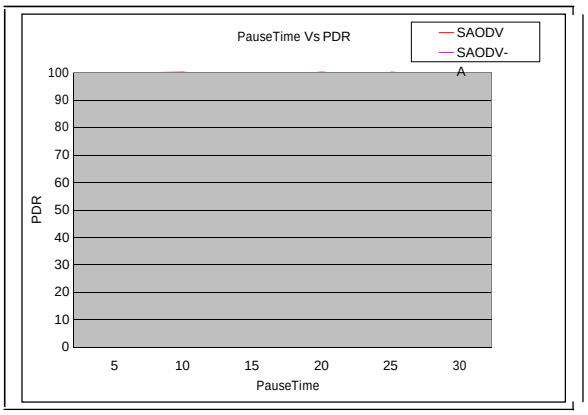

Fig.(d) PDR with varied Pause Time

In fig.(e) depict the control overhead of an attacker free and attacker environment is 1.41 % and 23.31 %.

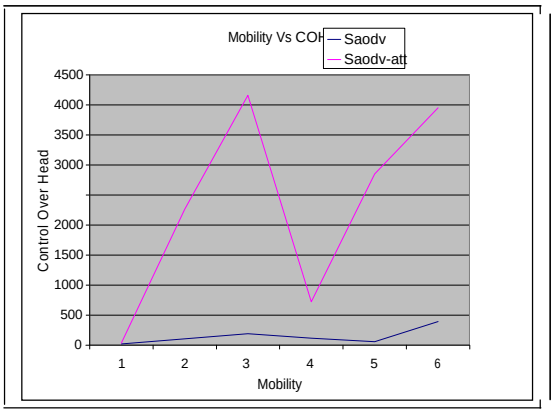

Fig.(e) Control OverHead with varied Mobility

The table III. Shows the results of various scenario and measuring factor of SAODV and SAODV-attacker environment.

III. Various Scenarios with Measuring Factors

Scenario	Measuring Factor	SAODV	SAODV-Attacker
Varying node speed	Packet Loss	0.85%	57.05%
Varying Mobility	PDR	83.15%	32.33%
Varying Number of nodes	PDR	83.21%	14.33%
Varying Pause Time	PDR	99.91%	44.55%
Varying Mobility	Control overhead	1.41%	23.31%

CONCLUSION

From this simulation study it is observed that the presence of attacker degrades the performance of the network. Even though the SAODV routing protocol has some cryptographic techniques to achieve security, still it needs more security features to safeguard from malicious nodes action during high mobility. This paper considered only DOS attack particularly packet dropping and it can be further enhanced to provide a solution to various DOS attacks by suggesting an effective detection and prevention methodology for insider's attacks.

REFERENCES

[1] Aad, J.-P. Hubaux, E. W. Knightly, Denial of service resilience in ad hoc networks, in: Proceedings of the 10th annual international conference on Mobile computing and networking (MobiCom), Philadelphia, PA, USA, 2004, pp. 202–215

[2] S. Capkun and J.P. Hubaux, "BISS: Building Secure Routing out of an Incomplete Set of Security Associations," in Proc. of

ACM Workshop on Wireless Security (WiSe'03), San Diego, CA, Sept. 2003.

[3] B. Dahill, B. N. Levine, E. Royer, and C. Shields, "A secure routing protocol for ad hoc networks," Proceedings of the International Conference on Network Protocols (ICNP), pp. 78–87, 2002

[4] Davide Cerri and Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", 0163-6804/08 © 2008 IEEE, IEEE Communications Magazine, February 2008E.

[5] Jan von Mulert, Ian Welch , Winston K.G. Seah, "Security Threats and Solutions in MANETs: A Case Study using AODV and SAODV",

[6] M. F. Juwad, and H. S. Al-Raweshidy, "Experimental Performance Comparisons betweenSAODV & AODV", IEEE Second Asia International Conference on Modelling & Simulation,

[7] Junaid Arshad and Mohammad Ajmal Azad, "Performance Evaluation of Secure on-DemandRouting Protocols for Mobile Ad-hoc Networks", 1-4244-0626-9/06 © 2006 IEEE

[8] Lijuan Cao, K. Sharif, Yu Wang, T. Dahlberg, "Adaptive Multiple Metrics Routing Protocols for Heterogeneous Multi-Hop Wireless Networks", proceedings for 5th CCNC Consumer Communications and Networking Conference, IEEE, 2008, pp. 13 – 17.

[9] M. Guerrero Zapata, "Key Management and Delayed Verification for Ad Hoc Networks", J.High Speed Networks, vol. 15, no. 1, Jan. 2006, pp. 93–109.

[10] Manel Guerrero Zapata, "Secure Ad hoc On Demand Distance Vector (SAODV) Routing",Technical University of Catalonia (UPC), Mobile Ad Hoc Networking Working Group, Internet Draft, 15 September 2005.

[11] Guerrero Zapata, N. Asokan, "Securing Ad Hoc Routing Protocols", WiSe'02,September 28, 2002, Atlanta, Georgia, USA, ACM 1-58113-585-8/02/0009 Copyright 2002.Available: http://www.atm.com

[12] M. Guerrero-Zapata, Re: [manet] one way hash in SAODV, IETF MANET Working Group Discussions (8 January 2003). URL http://www.ietf.org/mail-archive/web/manet/current

[13] P. Ning and K. Sun, "How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad hoc Routing Protocols," in Proc. IEEE Information Assurance Workshop, West Point, NY, June 2003.

[14] C. Perkins, E. M. Belding-Royer and S. Das. "Ad hoc On-Demand Distance Vector (AODV) Routing". Experimental RFC 3561.

[15] Yih-Chun Hu, Adrian Perrig, and Dave Johnson. "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols." In Proceedings of the ACM Workshop on Wireless Security (WiSe), San Diego, California, September 2003.

[16] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, Joo-Han Song "Experimental Comparisons between SAODV and AODV Routing Protocols ", WMuNeP'05, October 13, 2005, Montreal, Quebec, Canada.

[17] A. Zahary, A. Ayesh, "Analytical study to detect threshold number of efficient routes in multipath AODV extensions", proceedings of International Conference of Computer Engineering & Systems, ICCES, 2007, pp. 95 – 100

AUTHOR'S PROFILE

S.Madhavi

is working as Associate Professor in the Department of Computer science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode, Tamilnadu. She has done M.E(CSE) from J.J College of Engineering and Technology, Trichirappalli She is Lifetime Member of ISTE. Her research areas of interest include Mobile Computing, Network Security, and Information security. She has presented and published 7 research papers in national and international Journals and conferences.

Dr. K. Duraiswamy

B.E., M.Sc. (Engg.), Ph.D,, is currently working as Dean (Academic) in K.S. Rangasamy College of Technology, Tiruchengode, Tamilnadu, India. He has 42 years of teaching and research experience. He has guided 16 Ph.D.s in the area of Computer Science and Engineering in addition to 14 M.Phil students in Computer Science. He is currently guiding more than 12 students for Ph.D. He has also guided more than 100 M.E. students in the area of Computer Science and Engineering. He has published 51 papers in International Journals and 12 papers in National Journals in addition to participating more than 72 National and 43 International Conferences. His area of interest are : Image Processing, Network Security, Data Communication, Soft Computing, Computer Architecture, Character Recognition, Data mining etc.

Dr. B. Kalaavathi

is working as a Head &Professor in Computer Science and Engineering Department, K.S.Ranagasamy Institute of Engineering and Technology, Tiruchengode, Tamilnadu. She has 17 years of teaching experience. She has guided 15 M.E students and now guiding 12 Ph.D research scholars. She has published 15 number of papers in international and national journals and conferences. She is a life member of ISTE and CSI. Her research areas of interest include Mobile Computing, Mobile Ad Hoc networks, Network security and Data Mining.

Dr. S. Vijayaraghavan

is working as a Professor in Christ Engineering College Pondicherry. He has 10 years of Teaching experience. He is a life member of ISTE. He has published more papers in conference and journal of national and international. His area of research includes Mobile Ad hoc network, Network security, and Data Mining.