International Journal of Electrical and Computer Engineering (IJECE)
Vol. 5, No. 5, October 2015, pp. 1111~1118
ISSN: 2088-8708

Designing an Adversarial Model Against Reactive and Proactive Routing Protocols in MANETS: A Comparative Performance Study

A. Peda Gopi*, E. Suresh Babu*, C. Naga Raju, S. Ashok Kumar***
* Department of Computer Science and Engineering, K L University, India
** Department of Computer Science and Engineering, Yogi Vemana University, India

Article Info

Article history:

Received Apr 2, 2015
Revised Jun 15, 2015
Accepted Jun 29, 2015

Keyword:

MANETS
Routing protocols
Wormhole

ABSTRACT

Mobile ad-hoc networks are self-organized infrastructure less networks that consists of mobile nodes, which are capable of maintaining and forming the network by themselves. Recently, researchers are designed several routing protocols on these networks. However, these routing protocols are more vulnerable to attacks from the intruders, which can easily paralyze the operation of the network due to its inherited characteristics of MANETS. One such type of attack is wormhole attack. Because of its severity, the wormhole attack has attracted a great deal of attention in the research community. This paper compares reactive and proactive routing protocols in adversarial environment. Specifically, wormhole attack is applied to these routing protocols to evaluate its performance through simulation. Comprehensively the results shows the comparative performance of these protocols against wormhole attack is hard to detect and easy to implement.

Corresponding Author:

C. Naga Raju
Departement of Computer science and Engineering,
Yogi Vemana University,
Email: cnrcse@yahoo.com

S. Ashok Kumar
Departement of Computer science and Engineering,
K L University
Email: gopiarepalli2@gmail.com

1. INTRODUCTION

From the last few decades, there has been drastic development and deployment of wireless technology. This technologies is already witnessed with the revolutionary computing devices such as PDAs, smart phones, palmtops and notebooks etc., which creates interaction among each other. This habitat has created a new paradigm with extensive applications in ubiquitous computing. One such type of paradigm is mobile ad-hoc network. Particularly, mobile ad hoc networks have emerged in many forms where fixed infrastructure is not available or expensive to deploy the existing infrastructure. Moreover, mobile ad-hoc networks are self-organized infrastructure less networks that consists of mobile nodes, which are capable of maintaining and forming the network by themselves.

The unique features of these networks enables several applications such as government, military and health services etc., However, the MANET [1] applications pose a new routing and security challenges due to the open nature of the networks. Indeed, the nodes in MANET [2] move arbitrarily which may experience rapid and unpredictable changes in the network topology. Further, establishing the routing in such network is one of the challenge issue. Recently, researchers are designed several routing protocols such as AODV, DSR, DSDV, OLSR. However, these routing protocols are more vulnerable to attacks from the intruders, which

can easily paralyze the operation of the network due to its inherited characteristics of MANETS. Furthermore, the security in these networks is more challenging when it's comes to the wormhole intrusion. This wormhole intrusion is one of the severe attack that is hard to detect and defend due to its special properties [3], that can intercept the packets and quickly guide the Packets to another node with the help of tunnel as shown in figure-1. Many proposals [4] of this kind of attack are already proposed. Previously, existing work is mainly focused on individual routing protocols In this paper we compared two reactive (AODV, DSR) and two proactive (DSDV, OLSR) routing protocols [5] in adversarial environment. Specifically, wormhole attack is applied to these routing protocols to evaluate the performance through simulation. The rest of this paper is organized as follows. In section 2, describes various existing mechanisms of wormhole detection in various routing protocols. Section 3 we discuss the AODV, DSR, DSDV and OLSR routing protocol in detail. Section 4 provides the simulation environment and results. Finally we conclude in section 5.

2. RELATED WORK

The particulars of various existing wormhole detection mechanisms on different routing protocols are as follows:

S. Gupta [6] et al proposed a Wormhole Attack Detection Protocol using Hound packet called WHOP for detecting colliding attacks without using any exceptional hardware or watching systems. In this method after path discovery operation initiator node uses a hound message packet to spot wormhole attacks which reckonings hop variance between the neighbors of the one hop distance nodes in the path. After the process the target node detects the wormhole based on the hop, difference between neighbors of nodes exceeds the acceptance level.

Umesh Kumar chaurasia [7] et al proposes MAODV, a concept to detect wormhole attacks in the network by collecting both number of hops and delay per hop information for different routes from initiator to target, which offers a wide-ranging solution for both diversities of wormhole attacks. However, under genuine situation, the delay for each packet is similar along each hop in the path and it should be excessive for those nodes are involved in the colluding attack because there can be many nodes between them otherwise can be connected through a long link (wired or wireless).

Hu [8] et al proposed a packet leashes method to defend against colluding attacks. The main concept of this method is to bound the maximum tolerable communication distance. Two types of leashes data were used Geographical restraint and temporal restraint. Both Geographical and temporal leash methods require authentication of received packets. For Geographical leashes, each node must have its exact location information and requires a loosely clock harmonization. For temporal leashes, each node requires a precise clock synchronization and requires a roughly location information.

Zubair Ahmed Khan [9] et al proposes the use of the modified routing information table for recognition of the mistrustful links, authorization of colluding nodes existence, at the end segregating the dyed-in-the-wool wormhole nodes. Regarding at the other alternatives of the wormhole attack, that there is one thing common in all, which is. a path is advertised between the noxious nodes, and all the normal hosts are forced to make all their paths using this malicious path. Modified routing table that will help in the identification of malicious links. In this paper writer made changes to the paths and the full path from initiator to target node. By doing this we can straightaway detect a prospective wormhole link as quickly as it is created. By giving the hosts the ability to analyses/share one another's routing information tables we can also detect the latent wormholes.

Jain [10] et al Proposes wormhole detection using channel characteristics detecting a wormhole by exploiting the essential equilibrium of electromagnetic wave transmission in the wireless environment. It is hands-on economical method to detect colluding attack using the essential equilibrium in the wireless channel. We investigated two physical characteristics of the channel reaction, phase and magnitude that can be used as signs in our security scheme. We validated that channel quantities from IRIS sensor motes support our assumptions on channel characteristics.

Mahdi Nouri [11] et al proposes two techniques for to detecting the wormhole attack. The first practice is designed for detection of noxious nodes in a community of nodes in which individually pair of nodes in the neighborhood is surrounded by radio assortment of each other. The second method is deliberate for recognition of noxious nodes in a community of nodes, in which individually pair of nodes may not be in broadcasting range of each other but where there is a node among them which has all the other nodes in its one-hop surrounding area. Shortcoming of these practices is the impracticality of identifying wormhole attack in the usage of out of band attack.

3. ROUTING PROTOCOLS

Routing [12] is one of the essential and challenging issue in mobile ad-hoc networks, as mobile nodes comprises with battery power, low bandwidth capabilities, high error rates and unpredictable movement of the nodes. Recently, researchers proposed several routing protocols with different dimensions such as efficiency, quality of service, scalability, etc. However, these routing protocols [13] [14] are more vulnerable to attacks from the intruders, which can easily paralyze the operation of the network due to the inherited characteristics. Hence, there is a need to provide the security for these routing protocols against wormhole intrusion. In this paper, we compare various routing protocols in adverse environment. There are two major categories of routing protocols in Mobile Ad-hoc Networks which are proactive and reactive.

3.1 Proactive Routing Protocols

Proactive routing protocols are enclosed with routing information tables at each and every host. And all hosts continuously updates the routing information tables to maintain latest view on the network topology. The existing static routing protocols are: DSDV, OLSR and these are described briefly below.

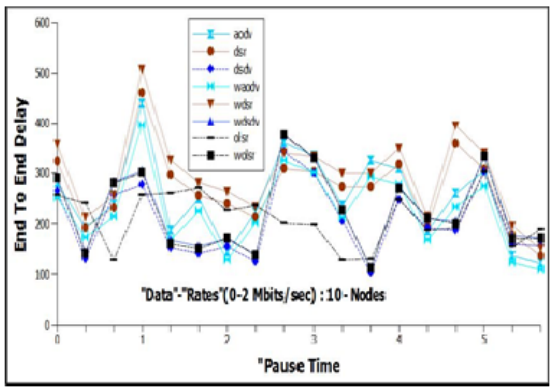

Figure-1: End to End Delay of 10-Nodes

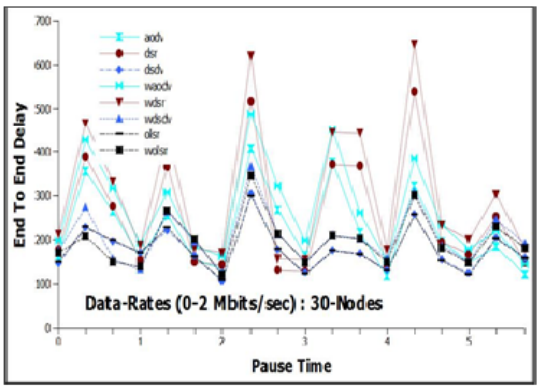

Figure-2: End to End Delay of 30-Nodes

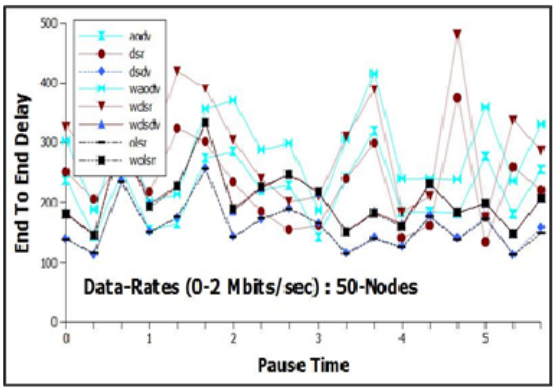

Figure-3: End to End Delay of 50-Nodes

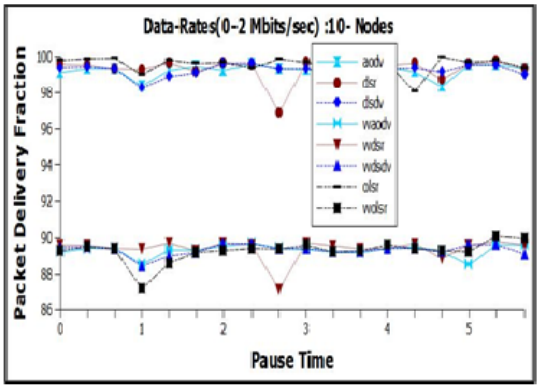

Figure-4: Packet Delivery Fraction of 10-Nodes

Destination Sequenced Distance Vector Routing (DSDV) Protocol

DSDV is a one of the earliest routing protocol proposed for wireless networks, particularly for mobile ad-hoc networks. The nature of the routing protocol is proactive, and the routes are pre-established from one to all in the network. Due to the proactive nature, all hosts maintain complete topology information as routing table. To know the freshness of a particular path it uses sequence numbers. All hosts are continuously in a timely manner updates the routing tables. However, this routing protocol is more vulnerable to wormhole intrusion due to its openness and lack of central authority. The adversary node exploits the weakness of this routing protocol to launch wormhole by simply forwarding the false link information to the routing tables. This will result the wormhole route between source and destination. Moreover, the data packets will be travel through the wormhole route, which may be fully or selectively discarded by the attacker that results denial of service attack.

Optimized Link State Routing (OLSR) Protocol

Optimized Link State Routing Protocol [15] is proactive in nature. The name optimized link state stands for reduce the number of links and reduce the size of control packets in the network. For to reduce the number of links it uses multipoint relays (MRPS). The reduction is done by stating a subset of links called multipoint relays to cover all nodes in the network. Functionally it works with two control messages one is HELLO and other is Topology Control (TC) message. OLSR is also vulnerable wormhole attack, it is launched during the transmission of routing control messages. Due to the wormhole attack the functioning of the protocol is altered and the performance of the OLSR is decreased. Due to wormhole attack QOS parameters are affected tremendously, those are throughput, jitter, packet delivery ratio and end to end delay.

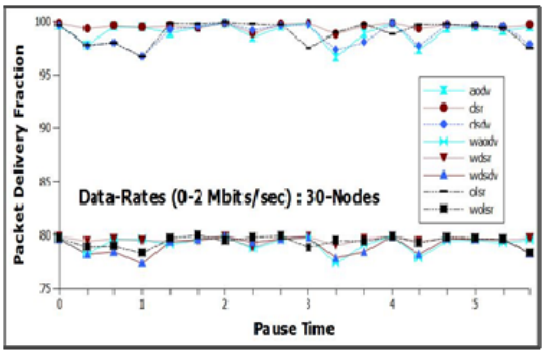

Figure-5: Packet Delivery Fraction of 30-Nodes

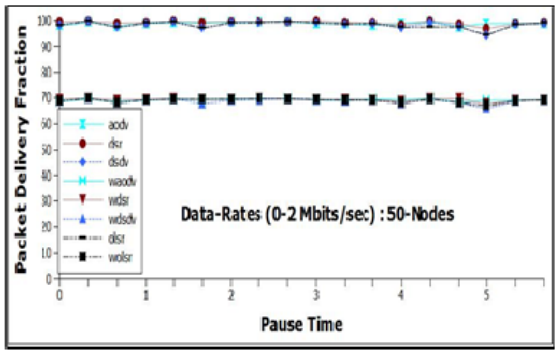

Figure-6: Packet Delivery Fraction of 50-Nodes

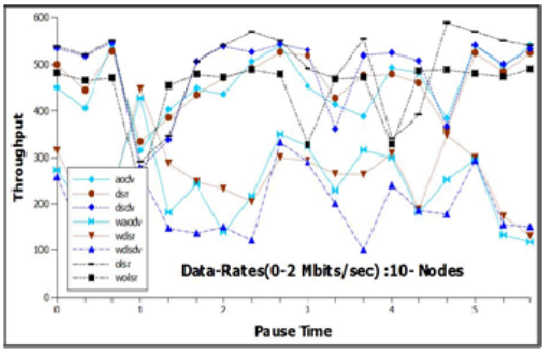

Figure-7: Throughput of 10-Nodes

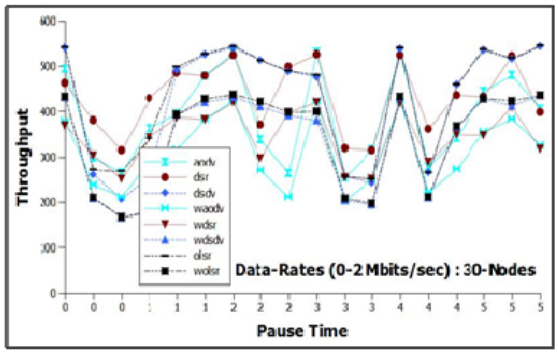

Figure-8: Throughput of 30-Nodes

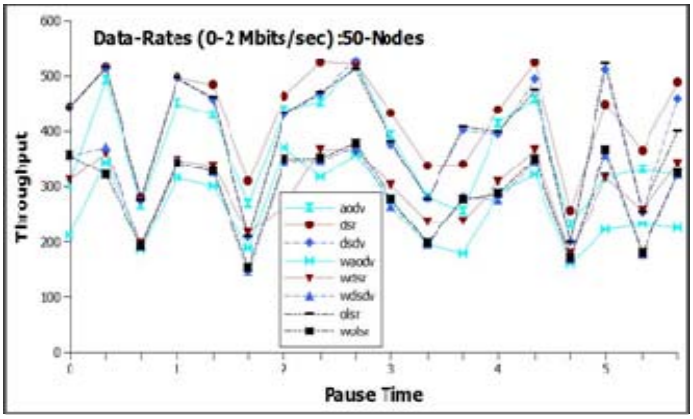

Figure-9: Throughput of 50-Nodes

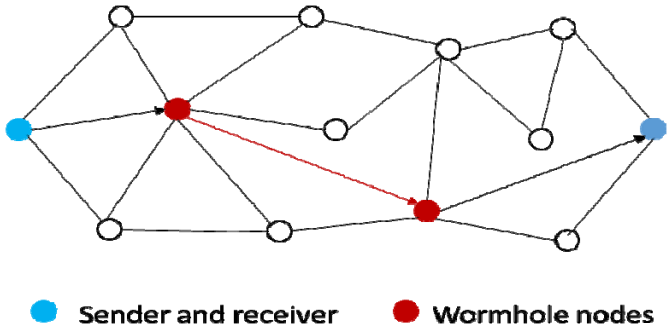

Figure 10. Wormhole attack

3.2 Reactive Routing Protocols

Reactive routing protocols are not maintain routs to other nodes in the network, they create the routes whenever required by originating the route discovery process. And the routes are maintained until the willing ness of the intermediate nodes and the completion of the communication between communicating parties. The existing dynamic routing protocols are: AODV, DSR.

Dynamic Source (DSR) Routing

Dynamic source routing protocol [16] is reactive one, the routs are builds based on sender perception, when sender wants to communicate with other nodes in the network routs are build. DSR [17], the name indicates it is a source routing protocol. DSR is mainly composed with two basic mechanisms route discovery and route maintenance. Route discovery is originated by sender, whenever it wants to communicates with the other node by broadcasting RREQ message globally. After reaching RREQ message receiver will replay with the RREP packet, then the route is well established, transmission of data is taken place between the both of the mobile nodes. Route maintenance is also one of the curtail operation, in this the status of the link is known to the communicating parties. And also presence of the communicating parties is also known to neighbors. However, this routing protocol is more vulnerable to wormhole intrusion due to its openness and lack of central authority. The adversary node exploits the weakness of this routing protocol to launch wormhole by just forwarding the first RREQ packet which is received from the neighbor node. Consequently, the adversary will forward the same RREQ message through fast channel to the colliding node, which intern reaches the same RREQ packet to the destination much faster than other RREQ packets from different neighbor nodes. This will result the wormhole route between source and target node. Moreover, the data packets will be travel through the wormhole route, which may be fully or selectively discarded by the attacker that results denial of service attack. Due to wormhole attack QOS parameters are affected tremendously, those are throughput, jitter, packet delivery ratio and end to end delay.

Ad Hoc On Demand Distance Vector (AODV) protocol

AODV [18] is a reactive routing protocol it will arranges routs on demand from sender to the receiver. AODV [19] mainly designed for to handle the problems of huge message header in on-demand protocols and huge packet overhead due to the periodic update messages in static routing protocols. Functioning of AODV is mainly composed with two level's one is route discovery and another is route maintenance. Primarily, it uses global route discovery process by broadcasting RREQ message over the network for to finding desired route to the destination. Whenever the receiver gets the RREQ message from the neighbor it replays back to the sender with RREP message. After getting RREP message form the receiver the route is well-established, and transmission of data takes place. Secondarily, route maintenance is composed with three operations route error, hello and time out messages. Route error message is fired when the route is not available or failed. Hello is used to check the connection condition and time out is used to identify the connection status, if a connection is inactive, it will be discorded after timeout completion. AODV routing is completely disturbed when there is a wormhole in the network. Worm hole [20] attack is launched during the route discovery process, a node (source) wants to communicate with other node (destination) normally this conversation is possible with shortest path which is provided by the AODV, that route is called as traditional route. If wormhole is present in the network two noxious nodes are located at two different locations and impersonates neighbors to the source and destination. So the source is establish the route through the noxious nodes to make communication with the destination, this path is called as wormhole path. It illuminates that wormhole attack is wholly aggravate AODV routing. Due to wormhole attack QOS performane parameters [21] are affected tremendously, those are throughput, jitter, packet delivery ratio and end to end delay.

4. PERFORMANCE EVALUTION AND SIMULATION ANALYSIS

The simulations were performed using Network Simulator 2 (NS-2.35). Random waypoint model is used to generate the mobility scenarios by varying 10 to 50 nodes moving in a territory area of 1000 X 1000 meters. Hear we uses moderate packet rate and varying pause times to simulation and we compare different ad-hoc routing protocols (DSDV, OLSR, DSR, AODV) with Wormhole attack and without wormhole attack by varying the number of wormhole nodes in the network. And we calculate various performance metrics of packet delivery fraction, throughput and end to end delay. The simulation parameters are summarized in Table 1.

Table1. Simulation parameters

Parameter	Values
Traffic type	CBR.
Number of nodes	10 to 50.
Simulation time	1000 sec.
Pause time	0, 1, 2, 3, 4 and 5.
Simulation area	1000 X 1000 meters.
Mobility	0 to 20 meter/sec.
Performance metrics	End to End Delay, Throughput and Packet delivery fraction.

4.1 Performance Metrics

This paper analyze the MANET routing protocols under the following three performance metrics.

1. *Packet delivery Fraction/Ratio:* Ratio between the amounts of data received by the target node to the amount of data send by the source host is called packet delivery fraction.
2. *End-to-end Delay:* The time interval between sender and target node to transmit a data packet over the network. It is the sum of all intervals which are source, intermediate nodes, route discovery delay and queuing interval is called as end to end delay.
3. *Throughput:* It is the portion of channel capacity used for successful data transmission.

Figure 1, 2 and 3 shows the graphs for end-to-end delay Vs pause time in 10, 30 and 50 nodes End to End delay in both legitimate and under wormhole situation. In legitimate situation proactive routing protocols has lesser end to end delay than compared to reactive protocols. In normal situation overall OLSR has minimum end to end delay and DSR having more end to end delay. But by increasing number of nodes and high mobility situation reactive protocols having less end to end delay.

Under wormhole attack also Proactive routing protocols (OLSR & DSDV) perform better then compared to the reactive routing protocol (AODV & DSR). AODV and DSR show deprived delay characteristics as their paths are habitually not the shortest. Due to node mobility the paths which are finds shorter under early route discovery process does not remain same over time goes on.

By increasing number of nodes AODV gives better end to end delay under wormhole but DSR having more end to end delay in both the situations.

Figure 4, 5 and 6 shows the graphs for PDF Vs pause time in 10, 30 and 50 nodes respectively under both legitimate and wormhole attack. Dynamic routing protocols (DSR and AODV) drop a major number of packets during the route discovery phase, as route acquirement takes time proportional to the distance between the source and target node. Packet drops are scarcer with static routing protocols (DSDV & OLSR) as substitute routing table entries can always be assigned in reaction to link failures. Static routing protocols also drop huge number of data packets when the number of nodes are more and high mobility situations. AODV has a slightly poorer packet delivery performance than DSR because of greater drop rates. AODV uses route expiration, dropping few packets when a route terminates and a new route must be originate. Under wormhole DSR having slight increase in Packet delivery ratio compared to AODV, DSDV and OLSR.

Figure 7, 8 and 9 shows the graphs for Throughput Vs pause time for 10, 30 and 50 nodes respectively under both legitimate and wormhole attack. Throughput is the measure of information exchanged over the time of time communicated in kilobits per every second (Kbps). Through put is dependent on PDF, more the PDF gives more throughput, under normal situation DSR having high throughput compared to all other routing protocols. AODV has slight decrease in throughput compared to DSR but proactive protocols (DSDV & OLSR) has low through put when the number of nodes are more. Under wormhole attack throughput of all routing protocols decrease drastically compared to normal situation. Compared to all other routing protocols DSR having better throughput and AODV is slightly lower. On other side Proactive routing protocols have lower throughput when increasing number of nodes.

5. CONCLUSION

Mobile ad hoc networks have emerged in many forms where fixed infrastructure is not available or expensive to deploy the existing infrastructure. The existing routing protocols on these networks are more vulnerable to wormhole attack. Because of its severity, the wormhole attack has attracted a great deal of attention in the research community. This papers compares two reactive and two proactive routing protocols in adversarial environment. Specifically, wormhole attack is applied to these routing protocols to evaluate the performance through simulation. Comprehensively the results shows the comparative performance of these protocols against wormhole attack is hard to detect and easy to implement. As a future work, it is necessary to design a mechanism to avoid the wormhole intrusion using some cryptographic methods.

REFERENCES

[1] C.E. Perkins. Ad Hoc Networking. Addison-Wesley Professional, first edition, 2000.

[2] S. Basagni, M.Conti, S. Giordano and I. Stojmenovic, "Mobile Ad Hoc Networking", A. John Wiley & Sons, Inc., Publication, 2004, ISBN 0- 471-37313-3.

[3] E.S. Babu, "An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks", vol. 4, no. 9, pp. 691–695, 2013.

[4] Thaier Hayajneh, Prashant Krishnamurthy, David Tipper, "DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks", 978-0-7695-3838-9/09 $26.00 © 2009 IEEE

[5] E.S. Babu and M.L.R. Chandra, "A comprehensive study of Routing protocols in Mobile Ad hoc Networks : Research Survey". vol. 7, no. 7, pp. 77–83, 2012.

[6] Saurabh Gupta, Subrat Kar and S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", 978-1-4577-0314-0/11/$26.00 ©2011 IEEE.

[7] Umesh kumar chaurasia, Mrs. Varsha singh, "MAODV: Modified Wormhole Detection AODV Protocol", 978-1-4799-0192-0/13/$31.00 ©2013 IEEE.

[8] Yih-Chun Hu, Adrian Perrig and David B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks".

[9] Zubair Ahmed Khan, M. Hasan Islam, "Wormhole Attack: A new detection technique", 978-1-4673-4451-7/12/$31.00 ©2012 IEEE.

[10] Shalabh Jain, Tuan Ta, John S. Baras, "Wormhole Detection Using Channel Characteristics", 978-1-4577-2053-6/12/$31.00 ©2012 IEEE.

[11] Mahdi Nouri, Somayeh Abazari Aghdam, Sajjad Abazari Aghdam, "Collaborative Techniques for Detecting Wormhole Attack in MANETs".

[12] Sunil Taneja, and Ashwani Kush, "A Survey of Routing Protocols in Mobile Ad Hoc Networks", *International Journal of Innovation, Management and Technology*, Vol. 1, No. 3, August 2010 ISSN: 2010-0248.

[13] E.S. Babu, C. Nagaraju, and M.H.M.K. Prasad, "A Comparative Study of Tree based Vs. Mesh based Multicast Routing Protocols in Mobile Ad hoc Networks", vol. 2, no. 6, pp. 6–11, 2013.

[14] T.P. Kumar, E. Suresh, B.V. Ramana, and B.S. Shashank, "Survey : Routing Protocols in Cognitive Radio Mesh Networks", vol. 6, no. 1, pp. 603–608, 2015.

[15] Farid Na¨ıt-Abdesselam, Brahim Bensaou and Jinkyu Yoo1, "*Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol*", IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

[16] D.B. Johnson, D.A. Maltz, Y. Hu, and J.G. Jetcheva. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet draft, February 2002. Draft-ietf-manet-dsr-08.txt.

[17] E.S. Babu and M.H.M.K. Prasad, "An Implementation Analysis and Evaluation Study of DSR with Inactive DoS Attack in Mobile Ad hoc Networks", vol. 2, no. 6, pp. 501–507, 2013.

[18] Elizabeth M. Belding-Royer, Charles E. Perkins Evolution and future directions of the ad hoc on demand distance-vector routing protocol-Elsevier, 2003

[19] E.S. Babu, C. Nagaraju, and M.H.M.K. Prasad, "An Implementation and Performance Evaluation of Passive DoS Attack on AODV Routing Protocol in Mobile Ad hoc Networks PROTOCOL OF", vol. 2, no. 4, 2013.

[20] Yang Shengju*, Shi Shaoting, Zhao Xinhui, "Research on Security of Routing Protocols Against Wormhole Attack in the Ad Hoc Networks", *TELKOMNIKA Indonesian Journal of Electrical Engineering* ISSN: 2302-4046, Vol.12, No.3, March 2014, pp. 2110 ~ 2117.

[21] Jogendra Kumar, " Broadcasting Traffic Load Performance Analysis of 802.11 MAC in Mobile Ad hoc Networks (MANET) Using Random Waypoint Model (RWM)", *International Journal of Information & Network Security (IJINS)* ISSN: 2089-3299 Vol. 1, No. 3, August 2012, pp. 223~227.

BIOGRAPHIES OF AUTHORS

Mr. A. Peda Gopi received his B.Tech degree in Information Technology from KLCE College of Engineering, Guntur, pursuing M.Tech degree in Computer Networks and Security from K.L.University Guntur. He has published 5 research papers in various International Journal. He has attended 8 seminars and workshops. His areas of interests are wireless networks, security issues in MANETs and vehicular networks.

Mr. E. Suresh Babu received his B.Tech degree in Computer Science from RGM College of Engineering, Nandyal, M.Tech degree in Computer Science from V.T. University Belgaum and pursuing PhD in Computer Science & Engineering from J.N.T.University Kakinada. Currently, he is working as an Associate Professor in the Department of CSE in K L University Vijayawada, He has got 12 years of teaching experience. He has published 8 research papers in various International Journal and 10 research papers in various National and International Conferences. He has attended 32 seminars and workshops. His areas of interests are Wireless Networks, Network Security, and MANETs. He is member of various professional societies like IAENG, CSTA,and CSI

Dr. C. Naga Raju is currently working as Associate Professor and Head of the Department of Computer Science and Engineering at YSR Engineering College of Yogivemana University, Poddatur, Kadapa District, and Andhra Pradesh, India. He received his B.Tech Degree in Computer Science from J.N.T.University, Anantapur, and M.Tech Degree in Computer Science fromJ.N.T.University Hyderabad and PhD in digital Image processing from J.N.T.University Hyderabad. He has got 18 years of teaching experience. He received research excellence award, teaching excellence award and Rayalaseemavidhyaratna award for his credit. He wrote text book on & Data structures. He has six PhD scholars. He has published fifty three research papers in various National and International Journals and about thirty research papers in various National and International Conferences. He has attended twenty seminars and workshops. He is member of various professional societies like IEEE, ISTE and CSI.

Mr. S. Ashok Kumar received his B.Tech degree in Information Technology from RVR & JC College of Engineering, Guntur, pursuing M.Tech degree in Computer Networks and Security from K.L.University Guntur. He has published 3 research papers in various International Journal. He has attended 10 seminars and workshops. His areas of interests are wireless networks, security issues in MANETs and vehicular networks.