Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 9, Issue. 3, March 2020, pg.47 – 57

A Trust Based Approach for Avoidance of Wormhole Attack in MANET

Ashok Panwar[1]; Bhavana Panwar[2]; D. Srinivasa Rao[3]; G. Sriram[4]

[1]Technical Officer (C) in ECIL (NPCIL), Tarapur, Mumbai, India
[2]Research Scholar
[3]Associate Prof. in CSE, MITM, Indore, India
[4]Associate Prof. in CSE Andhra University, Visakhapatnam, India
[1] ashok.panwar1991@gmail.com; [2] bhavanabachhane002@gmail.com; [3] sridas712@gmail.com; [4] ram.gopalam@gmail.com

Abstract: Mobile ad hoc network (MANET) is one of the well-known technologies in network and communication. MANET offers significant features that help to improve applications. In this paper for MANET's secure routing and improved routing protocol is introduced. The proposed routing technique is a trust-based routing protocol that evaluates the characteristics of intermediate nodes in the network. During the evaluation of nodes, a weighted trust value for all intermediate routers is calculated to create a secure path establishment. To compute weighted trust the network parameters of nodes are used i.e. packet drop ratio, RRT and energy consumption rate. Additionally, a trust threshold is used for classifying the malicious and legitimate nodes in a network path. Therefore trust threshold is used to make decisions for the selection of a secure and efficient path. Finally, a comparative study between traditional AODV and proposed trust-based AODV is performed. The experimental results demonstrate the proposed routing is efficient and secure as compared to traditional AODV routing protocol.

Keywords: mobile ad hoc network, security, trust computation, routing protocol improvements, implementation.

I. INTRODUCTION

Mobile ad hoc network (MANET) is one of the popular networks and communication technology. The MANET is a set of wireless nodes that are enabled to communicate with each other by using Wi-Fi. The nodes are limited to communicate in a specific range, thus the intermediate nodes are used to create a path and convey messages [1]. The MANET self-organizing network thus nodes are free from the network. So, any time a new node can join or leave the network. Additionally, the network is not involving any centralized administration or control thus the routing and other decisions are made by the nodes itself [2].

The properties of MANET enable different applications to take advantage of different industrial and military operations [3]. In this paper, an army application is proposed to secure network communication. Where we assumed, the network contains two malicious nodes that are connected with a high-speed LAN. Additionally both the attackers are trying to suspend the communication of the network. Such kind of situation is known as a wormhole attack.

The wormhole attack is mostly deployed using two or more internal attackers. These attackers are tunneling the information from one position of the network to another [4]. Due to this congestion in the network is formed. As congestion is created most of the network data is failed to deliver [5]. Therefore the wormhole is a serious attack condition in the network. In this paper, a detailed investigation of the wormhole attack is presented and a trust-based solution is proposed. This section provides an overview of the proposed work and the next section provides the details of the wormhole attack.

II. WORMHOLE ATTACK IN MANET

This section provides details about the wormhole attack and the working of AODV routing. These details help to understand the proposed solution.

A. Wormhole attack

The wormhole attack is one of the routing based attacks in MANET. During this when a malicious node receives the communicated packets at one place it tunnels it to another location in the network [6]. In order to do this activity in network two or more attackers create a high-speed channel. This malicious channel is known as a wormhole link. This wormhole link is a wired link between two attackers [7].

An example of a wormhole attack is given in figure 1. In this diagram, a MANET is demonstrated with two nodes source (S) and destination (D). There are some intermediate nodes also available which are labeled as A, B, and C. Except these intermediate nodes two additional nodes are also present in this diagram X and Y [8].

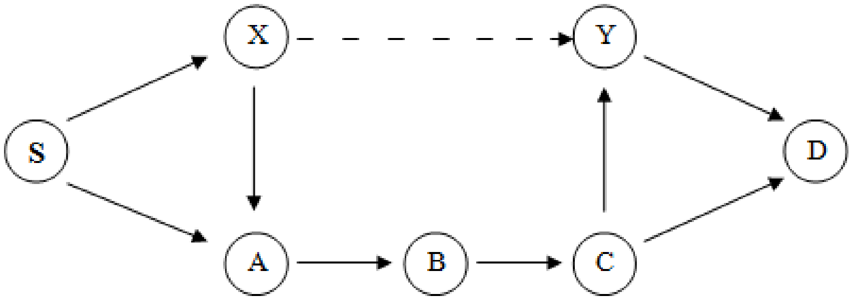

Figure 1 wormhole attack

X and Y are assumed as the malicious nodes, which are connected to each other using a dotted line. This dotted link between both is a high-speed bus that carries packets from source X to the Y position using the tunnel. Due to these phenomena, most of the traffic is passing on through created wormhole links [9]. When a significant amount of traffic is tried to passing through the malicious link the condition of congestion is created and most of the packets are dropped [10].

B. AODV routing

AODV routing protocol is also known as ad-hoc on-demand vector routing. The AODV contains three phases of route discovery and management. The first phase is known as route discovery, the source node broadcasts an RREQ (route request) message, and the neighbor nodes who receive the RREQ message check the IP address of destination [11]. If IP address matched with receiving node then node keeps the RREQ message otherwise re-broadcast the message to their neighbors. As the RREQ packet received by the destination, the destination node broadcast the RREP (route reply) message for source node [12]. The same process is used to deliver the RREP message to the source node. As the source node received the RREP message the route is established. Source node usages the same path to communicate with the destination node. The second phase is known as route maintenance, if any routing node leaves their place then route becomes abundant. Thus the intermediate node tried to recover the path using alternate nodes. If the route is not recovered then the third phase is processed and re-route discovery is initiated [13].

This section provides an overview of the two key concepts of the MANET. The next section includes the proposed work in detail.

III. PROPOSED WORK

This section provides an understanding of the proposed work and the solution for improving the security of the AODV routing protocol.

A. System overview

MANET is valuable in different real-world applications. The mobility of nodes makes it more valuable. Thus, the network can be used for different military and disaster management operations. Therefore, where instant deployment and its removal required the MANET configuration is used. In different applications, i.e. confidential operations, disaster, and relief management these networks are much fruitful. In this work, a scenario is assumed where a group of armed forces is deployed. Here each group member of the team is considered as a node. Every node communicating with each other but there are two hidden attackers present who are connected with a wired LAN to interrupt the communication [14].

According to the characteristics of the hidden attacker nodes, it is a condition of a wormhole attack. Therefore a potential solution is required that can identify the attacker nodes and avoid or bypass these malicious nodes. Therefore the proposed work is intended to design a trust-based routing protocol. That protocol pre-examines the network nodes and only communicates with the trusted nodes. This section provides an overview of the proposed work. The next section provides the proposed routing protocol's working.

B. Methodology

The proposed technique of secure routing is depending upon the modification of the AODV routing protocol. In this context, the extension of AODV is proposed by the incorporation of trust factors calculation. The extension of the protocol involves the evaluation of each node which is involved in active communication. Therefore, network characteristics are used for identifying the node trust values.

Parameters:

The following parameters are measured for trust computation:

1. **Round trip time:** due to congestion formed by the wormhole attackers, the packet delivery speed is affected. Thus we calculate the round trip time (RTT) for the nodes. To calculate RRT the following formula is used:

$$RTT = \frac{T_R - T_s}{2H_c}$$

Where, T_R is the time of receiving the packet, T_s is the time of sending packet, and H_c is the hop count.

2. **Packet drop ratio:** Due to the wormhole attack network suffers from congestion. Thus the malicious node has a significant amount of packet drop. Thus packet drop ratio is included as the trust factor. To calculate the packet drop ratio of a node the following formula is used:

$$PDR = \frac{total\ drop\ packets}{total\ packets\ sent}$$

3. **Rate of energy consumption:** The sending and receiving of data and control packets require a fixed amount of energy. Thus if any node in network consumes more energy as compared to other nodes, thus it means it behaves abnormally. Therefore, it is an essential factor for trust computation. To compute the energy consumption rate of the node, we assumed a node has a fixed energy level E_1 at sampling time T_1, and during the next sampling time T_2 the energy level becomes E_2. Thus the rate of energy consumption can be computed using the following formula:

$$\delta = \frac{E_1 - E_2}{T_2 - T_1}$$

Or

$$\delta = \frac{\Delta E}{\Delta T}$$

Trust Computation:

To manage trust during the communication we initiate with a normal functioning network. That network contains a set of nodes without any malicious node. We select three pairs of nodes randomly. Each pair contains a source node and a destination node. Now each source node initiates communication and using this communication described three factors are calculated. Let the pair (S_1, D_1) compute RTT_1, PDR_1 and δ_1. Similarly, all pairs of node calculating the given three parameters. After that, a threshold value is computed as.

$$RRT_{threshold} = \frac{RTT_1 + RTT_2 + RTT_3}{3}$$

$$PDR_{threshold} = \frac{PDR_1 + PDR_2 + PDR_3}{3}$$

And

$$\delta_{threshold} = \frac{\delta_1 + \delta_2 + \delta_3}{3}$$

Now we have three different thresholds for finding the malicious node. And to make rule-based classification the computational overhead increases. To preserve the computational resources we combine all parameters into a trust value. To calculate combined trust value we use this formula:

$$Trust = RRT_{threshold} * w_1 + PDR_{Threshold} * w_2 + \delta_{threshold} * w_3$$

The trust value is used to evaluate each node in the network. If a node's trust value higher than or equal to threshold trust value then protocol avoid node. Using this rule the network becomes secure and provides the preservation in the performance of the network.

C. Proposed algorithm

This section introduces the process of proposed trust-based routing. Table 1 contains the required steps. According to the given process, we have a network with N number of nodes. The source initiates the route discovery process by communication of RREQ and RREP messages. The protocol waits for all the possible replies from the destination. Therefore, we have multiple route options between source and destination. By using the routing table entry each path is evaluated against the calculated trust values. Additionally among the entire available options most secure route is elected as the primary routing path.

```
Input: Network nodes N

Process:
    1. Source node initiate route discovery
    2. Wait for reply message from all destination
    3. For each path in routing table
        a. Compute node RTT
        b. Compute node PDR
        c. Compute Node $\delta$
        d. Calculate Node trust
        e. If $Node_{trust} < trust_{threshold}$
            i. Node is legitimate
            ii. Go to next node
        f. Else
            i. Node is malicious
```

```
                ii.   Go to next path
            g.   End if
    4.   End for
```

Table 1 proposed algorithm

The above-given algorithm explains how trust values are used to evaluate the routes. If any un-trusted node found in the path then the algorithm avoids that node and tries to search another path.

IV. SIMULATION

This section provides the details about the implementation and simulation scenarios.

A. Simulation setup

The following configuration of the network is suggested to simulate the proposed routing protocol. Table 2 contains the parameters and relevant values.

S. No.	**Simulation properties**	**Values**
1	Antenna model	Omni Antenna
2	Radio-Propagation Model	Two Ray Ground
3	Channel Type	Wireless Channel
4	Routing Protocol	AODV
5	No of Mobile Nodes	20, 40, 60, 80, 100
6	Simulation area	1000 X 1000

Table 2 simulation setup

B. Simulation scenario

To demonstrate the effectiveness of the proposed trust-based routing protocol to avoid the wormhole attack. Two experimental scenarios are proposed.

1. **Simulation of traditional AODV routing with wormhole attacker nodes:** In this scenario, traditional AODV routing is configured with network. Additionally, two attacker nodes are deployed. After it two nodes i.e. source and destination nodes are initiating the communication. During this experiment, a trace file is generated. That trace file is used for computing the performance of the network. Figure 1 shows the simulation of normal AODV based simulation.

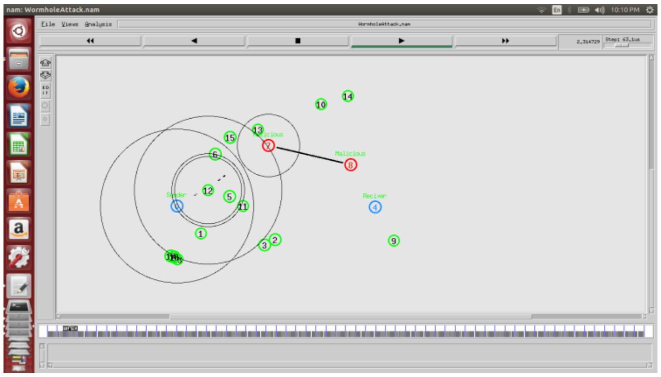

Figure 1 network with normal AODV

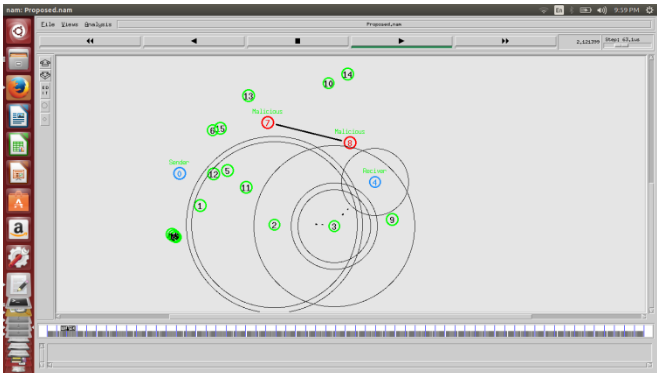

Figure 2 network with proposed AODV

2. **Simulation of secure Trust based AODV routing with wormhole attacker nodes:** In this simulation, the trust-based AODV routing is implemented using the NS2 tool. The network is configured with different numbers of nodes during experiments. The trace files are generated and used for performance computation. Figure 2 shows implemented simulation scenario with the proposed routing protocol.

V. RESULTS ANALYSIS

This section provides an analysis of network performance for both kinds of experimental scenarios. During experiments, different performance parameters are measured and reported.

A. End to end delay

The end to end delay is defined as the amount of time required to deliver a packet from source to destination. To calculate end to end delay the following formula is used:

$$E2E\ delay = Receiving\ time - sending\ time$$

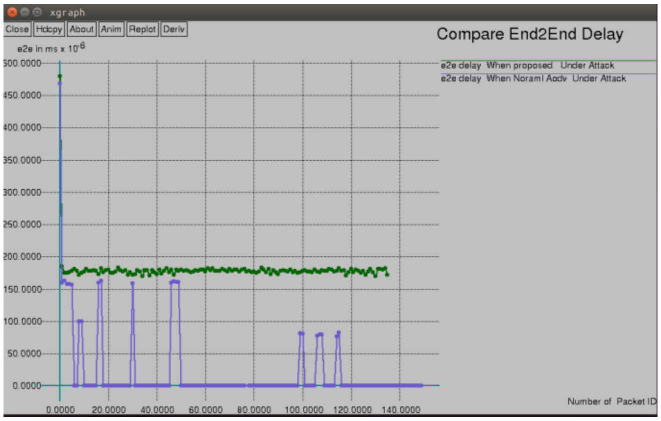

Figure 3 end to end delay

End to end delay of the network for both routing techniques. Figure 3 demonstrates performance of both routing strategy under attack condition. The blue line shows the e2e delay of traditional AODV and the green line shows the performance of the trust-based protocol. According to observed results traditional AODV routing unable to deliver packets to the destination. Thus end to end delay of the network tends to 0. On the other hand, the proposed technique is able to avoid the effect of wormhole attack.

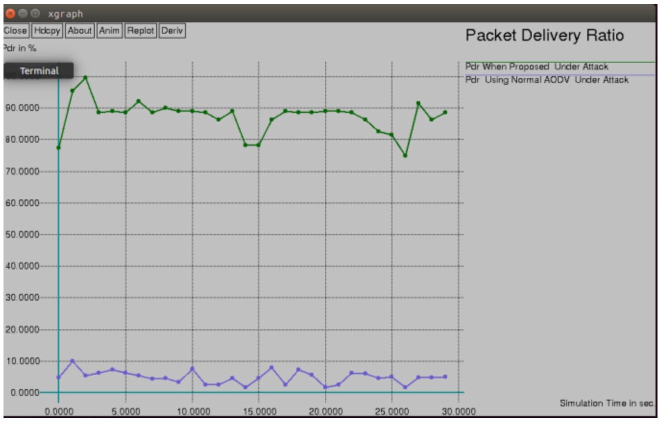

Figure 4 packet delivery ratio

B. Packet delivery ratio

The number of packets successfully delivered to the target node and ratio of a total number of packets is known as packet delivery ratio. The packet delivery ratio (PDR) is calculated using the following formula:

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

The packet delivery ratio of both approaches is reported in figure 4. In this diagram, the green line shows the proposed approach performance and the blue line is used for traditional AODV performance demonstration. As the given line graph the proposed approach shows the higher degree of packet delivery ratio as compared to the traditional technique of routing because the traditional technique is not able to send the data to the target node during the attack conditions.

C. Network Throughput

It is a measurement of network efficiency. The throughput of the network can be defined as the rate of successfully message delivery with respect to time. It is normally measured in terms of bits per second or data packets per second.

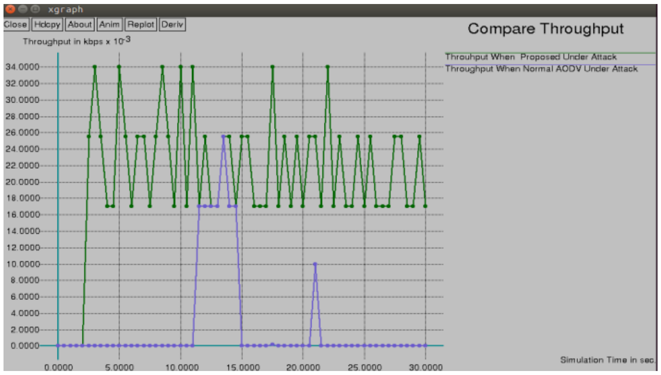

Figure 5 throughput

Figure 5 shows the comparative throughput of both the protocols. The experimental observations are represented in figure 5. The proposed technique shows higher throughput as compared to the traditional AODV. Because traditional AODV is not able to deliver packets due to attack and proposed technique avoid the malicious nodes in routes.

D. Energy consumption

The network requires an amount of energy to perform network events. Even during sending and receiving any packets. Therefore an efficient network performance is also described by the energy consumption of network nodes. Figure 6 demonstrates the energy consumption of the network for both the protocols. Here the green line shows the energy consumption of the traditional AODV and the red line shows the performance of the proposed secure routing protocol.

According to the obtained energy consumption of the networks, the proposed method preserves the energy as compared to the traditional technique. Thus the proposed technique is energy efficient and highly secure for preventing the wormhole attacks in MANET.

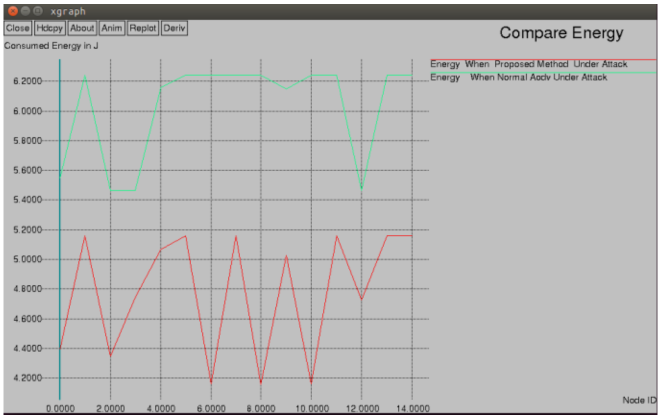

Figure 6 energy consumption

E. Packet drop Ratio

The rate of unsuccessfully delivered data can be termed as a packet drop ratio. Thus it is the ratio of undelivered packets and the total packets sent. That can be calculated using the following formula:

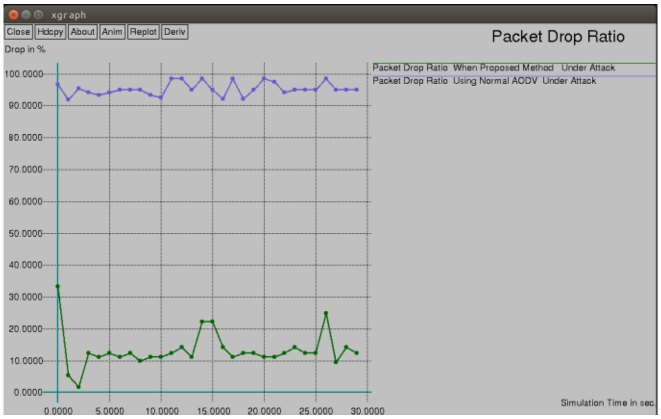

Figure 7 packet drop ratio

$$PDR = \frac{total\ undelivered\ packets}{total\ packets\ sent}$$

The comparative packet drop ratio of the proposed secure AODV routing protocol and traditional AODV routing protocol is given in figure 7. In this diagram, the green line shows the amount of packet drop using the proposed method and the blue line shows traditional AODV performance. According to the obtained performance, the proposed technique has the less packet drop ratio as compared to the traditional technique. Thus the proposed technique is efficient, energy preserving and effective for securing the network and can be used to secure the communication in different real-world applications.

VI. CONCLUSION & FUTURE WORK

This section provides a summary of the entire research work performed for securing MANET against the wormhole attack. Thus based on experimental observations and design points of view the conclusion and future extension of the work are presented.

A. Conclusion

The mobile ad hoc network is an effective technology for communication networks. The nodes are independent, mobile, self-organizing, and decentralized. Therefore that network is used in various applications. But the network is not much secure for the different kinds of routing based attacks. In this context, the proposed work is dedicated to investigating different routing based attacks. Additionally, the focus is made to study the wormhole attack. The wormhole attack is always deployed using two or more attackers. These attackers tunnel the information from one position of the network to another location of a network using high-speed links. Due to this, the network creates congestion and most of the data dropped.

In order to rectify the discussed wormhole problem in the mobile ad hoc network, a trust-based solution is proposed for design and implementation. The proposed trust-based technique first computes the threshold trust values based on the ideal network conditions. After measuring the threshold trust each path is evaluated against the computed threshold and if the node trust is less than the computed threshold we mark that node as legitimate otherwise that node is labeled as the malicious node.

The implementation of the proposed technique is performed using NS2 (network simulator 2). Additionally for measuring the performance of the system the X graph tool is used. The computed performance of both the network techniques is demonstrated using table 3.

S. No.	Parameters	Proposed AODV	Traditional AODV
1	Packet delivery ratio	High	Low
2	End to end delay	High	Low
3	Throughput	High	Low
4	Packet drop ratio	Low	High
5	Energy consumption	Low	High

Table 3 performance summary

According to the obtained results as given in table 2 the proposed routing protocol is secure, energy-efficient and offers reliable information delivery under the wormhole attack. Thus the proposed technique is acceptable for different areas of applications and utilities.

B. Future work

The main aim of the proposed work is to improve the security of the routing protocol for the wormhole attack is achieved successfully. The given work is effective and can be extended for the following research areas:

1. The proposed trust-based routing technique currently prevents the wormhole attack in the near future it is tried to involve the other attacks to rectify the security issues.
2. The proposed work involves the computation of limited network parameters, in the near future, more network characteristics are investigated for improving the security of MANET.

REFERENCES

[1] M. Arioua, Y. E. Assari, I. Ez-zazi, A. E. Oualkadi, *"Multi-hop cluster based routing approach for wireless sensor networks"*, Procedia Computer Science 83 (2016) 584 – 591, 2016 Published by Elsevier B.V

[2] S. Chettibi, S. Chikhi, *"Dynamic fuzzy logic and reinforcement learning for adaptive energy efficient routing in mobile ad-hoc networks"*, Applied Soft Computing 38 (2016) 321–328, 2015 Elsevier B.V

[3] D. M. Shila, W. Shen, Y. Cheng, X. Tian, and X. Shen, "AMCloud: Toward a Secure Autonomic Mobile Ad Hoc Cloud Computing System", IEEE Wireless Communications • April 2017, 1536-1284/17/$25.00 © 2017 IEEE

[4] Anal Patel, Nimisha Patel, Rajan Patel, "Defending Against Wormhole Attack in MANET", 2015 Fifth International Conference on Communication Systems and Network Technologies, 978-1-4799-1797-6/15 $31.00 © 2015 IEEE

[5] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taşkın, E. Ayday, *"A survey on information security threats and solutions for Machine to Machine (M2M) communications"*, J. Parallel Distrib. Comput. 109 (2017) 142–154, 2017 Elsevier Inc.

[6] P. Amish, V. B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", Procedia Computer Science 79 (2016) 700 – 707, 2016 The Authors. Published by Elsevier B.V

[7] N. Nissar, N. Naja, A. Jamali, *"Lightweight authentication-based scheme for AODV in ad-hoc networks"*, 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), 10.1109/WITS.2017.7934616

[8] H. S. Chiu, K. S. Lui, *"DelPHI: wormhole detection mechanism for ad hoc wireless networks"*, 2006 1st International Symposium on Wireless Pervasive Computing, IEEE 2006, DOI: 10.1109/ISWPC.2006.1613586

[9] D. Hlavacek, J. M. Chang, *"A layered approach to cognitive radio network security: A survey"*, Computer Networks xxx (2014) xxx–xxx, 2014 Elsevier B.V. All rights reserved.

[10] M. Bouabdellah, N. Kaabouch, F. E. Bouanani, H. B. Azza, *"Network layer attacks and countermeasures in cognitive radio networks: A survey"*, Journal of Information Security and Applications 38 (2018) 40–49, 2017 Elsevier Ltd

[11] P. Patel, R. Bansode, b. Nemade, *"Performance Evaluation of MANET Network Parameters using AODV Protocol for HEAACK Enhancement"*, Procedia Computer Science 79 (2016) 932 – 939, 2016 The Authors. Published by Elsevier B.V

[12] A. Nayyar, *"Flying Adhoc Network (FANETs): Simulation Based Performance Comparison of Routing Protocols: AODV, DSDV, DSR, OLSR, AOMDV and HWMP"*, 978-1-5386-3060-0/18/$31.00 ©2018 IEEE

[13] A. Dhaka, A. Nandal and R. S. Dhaka, *"Gray and Black Hole Attack Identification using Control Packets in MANETs"*, Procedia Computer Science 54 (2015) 83 – 91, 2015 The Authors. Published by Elsevier B. V.

[14] Mamata Rath, Binod Kumar Pattanayak, "Methodical survey on real time applications in MANETS: Focussing on key issues", 978-1-4799-5958-7114/$31.00 102014 IEEE.

AUTHOR'S PROFILE:-

ASHOK PANWAR received has Three Year Polytechnic Diploma in Computer Science and Engineering, B.E. / B. Tech. and M.E. / M. Tech. Degree both in Computer Science and Engineering from the University of R.G.P.V. (Rajiv Gandhi Proudyogiki Vishwavidyalaya) Bhopal, Madhya Pradesh. He is currently working as a Technical Officer (C) in **ECIL** (Electronics Corporation of India Limited), India, against the site requirements of **NPCIL** (Nuclear Power Corporation of India Limited), TAPS (Tarapur Atomic Power Station 1 to 4) Tarapur, Mumbai, Maharashtra, India. Working in **ACS** (Access Control System) and Simulator Department. He is Ex. Worker / Employee in Defence Research & Development Organisation **(DRDO)** in Defence Scientific Information & Documentation Centre **(DESIDOC)** Lab, Govt. of India, Ministry of Defence, in Department of Knowledge Management Division **(KMD**), **Metcalfe** House, Near Civil Lines, New Delhi, Delhi-110054, India. He has one year of Teaching Experience in Computer Networking. His area of Main Research Interests include:- Ad-hoc Networks, MANET, Network Security, Cryptography, Big Data, Information Security, Distributed Systems, Document Analysis and Cryptanalysis, Cyber Security, Data Mining & Image Processing. He has guided 90 above Graduate Students, and 50 above Post Graduate Students. He has Published 02 Papers in International Journal. He is many PPT's Published in Various topics. He has attended One National Level Conference. He has attended Two National Level Event's of Microsoft Dream Spark Yatra at IET - DAVV, Indore. He has attended Five Day's National Level Workshop on Android Security System. He has attended Two Day's National Level Workshop in **NS2 (**Network Simulator and Design 2) and attended Three Day's National Level Seminar on Udhyamita Jagrukta Shivir. He has attended more than 35 Workshops / Seminars in Various events.

BHAVANA PANWAR received her M.Sc. in Mathematics Science in 2016 and B.Sc. in Computer Science in 2014 both Degree's from the University of DAVV (Devi Ahilya Vishwavidyalay) Indore, Madhya Pradesh, and also Pursuing B. Ed. (Bachelor of Education) from the University of DAVV (Devi Ahilya Vishwavidyalay) Indore, Madhya Pradesh. She is working as a Research Scholar as well as Faculty from Sardar Vallabh Bhai Patel H.S. School Kasrawad, Khargone, Madhya Pradesh. She has 02 years of Teaching Experience in Mathematics as well as Computer. Her area of interests include:- Real and Complex Analysis, Fluid Mechanics, Mathematical and Numerical Analysis, Quantitative Risk Analysis, Computer Networks, Algebra and Cryptography, Big Data, Document Analysis, Network Security, Optimistic, Distributed Systems, Information Security and Data Mining. She has attended more than 20 Workshops / Seminars in Various events etc.

D. SRINIVASA RAO M.Tech, Ph.D is working as an Associate Professor in the Department of Computer Science & Engineering at Medi-Caps University, Indore, Madhya Pradesh, India. He has 25 years of teaching experience. His area of interest in Adhoc Networks, Distributed Systems, Network Security & Image Processing. He has guided more than 60 Post Graduate Students. He has published 2 books and 19 papers in international journals. He presented 2 papers in National Conferences, 1 paper in International Conference and has attended 37 National Workshops / FDP / Seminars etc. He is a life member of Professional Society like ISTE.

G. SRIRAM M.Tech, Ph.D is working as an Assistant Professor in the Department of Computer Science, School of Distance Education, Andhra University, Visakhapatnam, India. He has 15 years of teaching experience. His area of interest in Adhoc Networks, Data Mining & Networks Security. He has guided 50 Graduate Students. He has published 6 papers in international journals. He has attended 10 National Workshops / FDP / Seminars etc.