International Journal of Computer Science Engineering Research and Development (IJCSERD), ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online), Volume 3, Number 1
Jan- March (2013), pp: 30-40

IJCSERD

© PRJ PUBLICATION

PUBLIC KEY BASED APPROACH TO MITIGATE WORMHOLE ATTACK

Pradnya Patange [1], S. P.Medhane [2]

[1] Bharati Vidyapeeth College of Engineering
[2] Assistant Professor in the Department of Information Technology Bharati Vidyapeeth College of Engineering, Pune

ABSTRACT

Security is one of the vital features in mobile ad-hoc network (MANET). This paper evaluates limit of traditional routing protocols if applied to MANET. This paper also evaluates routing protocols currently used in MANET and put focus on security analysis of routing protocol over several possible security attacks like Attacks using modification, Denial of Service attack, Wormhole attack, Impersonation attacks, Attacks Using fabrication, Rushing Attacks etc.

Wormhole Attack is one of the most critical attacks. This paper proposes a public key based approach to mitigate wormhole attacks.

Keywords: MANET, Secure Routing algorithms, Security analysis, Public Key Cryptography, Wormhole attack.

I. INTRODUCTION

MOBILE Ad-hoc Network (MANET) is a collection of self configurable mobile node connected through wireless links. In MANET much of the research has been done focusing on the efficiency of the network. There are reasonably large numbers of routing protocols that are outstanding in terms of efficiency. More detailed research is at present in progress to develop secure ad hoc routing protocols. Mobile Ad-hoc Network are extremely susceptible to attacks due to their dynamically altering topology, absence of predictable security infrastructures and open medium of communication cannot be secured.

In wireless network a lot of attacks can be initiated but most of them are comparatively easy to detect because of their property of dramatically changing the network data. It is very vital when considering security issues of MANET to consider wormhole attack, which is complex to detect & can spoil important data by directing to illegal nodes. In the route discovery process, a wormhole can relay route request and response messages between far-away nodes, creating the manifestation of shorter path to destination. Since the wormhole can be at anyplace along a path, a source will have to identify it when a node sets up the route. Many protocols have been proposed, their confrontation towards various types of security attacks and efficiency are key point of concern in implementing these protocols.

II. ANALYSIS OF SECURE ROUTING PROTOCOLS

Routing protocols with security for MANET's can be primarily categorized in two major categories: [1] [2]

Prevention: This mechanism involves protocols which prohibit the attacking node to initiate any action. This approach requires encryption technique to authenticate the confidentiality, integrity, non-repudiation of routing packet information.

Detection and Reaction: Detection and Reaction mechanism as the name suggest will identify any malicious node or activity in the network and take proper action to maintain the proper routing in the network.

A. ARAN: Authenticated Routing For Ad Hoc Network

Kimaya Sanzgiri, Bridget Dahilly, Brian Neil Leviney, Clay Shieldsz and Elizabeth M. Belding-Royer developed Authenticated routing for Ad hoc Network based on AODV[3] using Certificates with a Central Certification Authority. Authenticated Routing for Ad hoc Networks (ARAN)[4] routing protocol, is based on Cryptographic Certificates and rely on a central trusted Certification Server (T). Every node entering into the network has to get a certificate signed by T. The certificate contains the IP address of the node, its public key, and time stamp when the certificate was issued and when it will expires. ARAN protocol in its route discovery sends a Route Discovery Packet (RDP) to its neighbor nodes. RDP includes destination IP (d), Source certificate Cert(s), nonce N(s) which is a time stamp for the packet life and the current time't'. And the whole packet is signed by source's private key K(s) [4].

ARAN uses public key cryptography, a Key distribution center and central certification authority server for node authentication and neighbor node authentication in route discovery.

Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbor node authentication through certificates. Participating nodes broadcast redundant route requests across the network. An attacking node can cause jamming in the network, there by compromising the functionality of the network.

Spoofing attacks are prevented by ARAN through digital signatures. All packets in the network is signed by its private key before broadcasted to the next level and checked for the authentication. So spoofing the identity of node is hampered by ARAN. Wormhole attack is possible in ARAN. Two compromised neighbor nodes can collaborate to falsely represent the length of available paths by encapsulating and tunneling the routing message between them. Rushing attack is not possible in ARAN. Table overflow, black hole attacks are impossible due to node level authentication with signatures.

B. SAR: Security- Aware Routing Protocol

Seung Yi, Prasad Naldurg and Robin Kravets developed SAR [5]. SAR based on AODV [3] & uses Security as on of the Key Metrics in its route discovery and maintenance.

SAR uses Security as one of the Key Metrics in its route discovery and maintenance.

The framework and attributes of the security metrics are detailed in [8]. This framework also uses different levels of security for different level of applications.

Each node in the network is associated with a level of trust metric, based on which route will be followed according the security requirements of the application. SAR extends on-demand ad hoc routing protocols (like AODV or DSR) in order to incorporate the security metric into the route request messages. The initiator broadcasts a route request (RREQ) with an additional field (RQ_SEC_REQUIREMENT) that indicates the required security level of the route that wishes to discover. A neighboring node that receives the packet, checks whether it can satisfy the security requirement. If the node can provide the required security then it can participate in the requested route and re-broadcasts the packet to its own neighbors setting a new field called RQ_SEC_GURANTEE to indicate the maximum level of security it can provide. If a node is not secure enough to participate in the requested route it simply drops the RREQ. Therefore, when the destination node receives the RREQ it can be sure that a route to the source node exists and that this route satisfies the security requirements defined by the initiator. The destination sends a route reply (RREP) packet with an additional field (RP_SEC_GUARANTEE) that indicates the maximum level of security of the found route. The RREP message travels back along the reverse path of the intermediate nodes that were allowed to participate in the routing, and each node updates its routing table according to the AODV specification including the RP_SEC_GUARANTEE value. This value is used in order to allow intermediate nodes with cached routes to reply to a request of a route with a specific security requirement.

SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. Rushing attack, Routing table modification and Black hole attacks is not possible in SAR but Wormhole attacks and Denial of- service attacks are possible in SAR.

C. SRP: Secure Routing Protocol

Secure Routing Protocol (SRP), was proposed by Papadimitratos and Hass [5]. SRP is based on DSR [6]. DSR is an on-demand routing protocol, which finds the route as and when required, dynamically. The major difference between AODV and DSR is that DSR uses source routing in which a data packet carries the complete path to be traversed where as in AODV the source node and intermediate nodes store the next hop information for each data packet transmission.

SRP is implemented over DSR [11], with an underlying Security Association (SA) between the source and destination nodes. Key generated by the SA is used to encrypt and decrypt the data by the two nodes.

Secure routing protocol (SRP) was developed based on Destination Source Routing (DSR). The intermediate nodes participating in the route discovery measure the frequency of queries received from their neighbors and maintain a priority ranking inversely proportional to the query rate of node. Due to this malicious compromised nodes participating in the network are given smallest amount of priority to deal with. Rushing attack, Routing table modification, Denial of-service Attacks and Black hole attacks is not possible in SRP but Wormhole attack is possible in SRP.

D. SEAD: Secure Efficient Ad Hoc Distance Vector Routing Protocol

SEAD is designed based on the DSDV (Destination Sequenced Distance Vector) protocol. SEAD was proposed by Yih-Chun Hu, David B. Johnson and Adrian Perrig [7]. Destination Sequenced Distance Vector routing protocol is one of the first protocol proposed for ad hoc wireless networks. It was developed based on the distributed Bellman-Ford algorithm where each node maintains a table that contains the shortest distance and the first node on the shortest path to every other node in the network. It's a table driven routing protocol. Routes to all destinations are readily available at every node at all times. The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology. Whenever there is a change in the network topology, the table entries are updated.

SEAD was developed based on DSDV and incorporates One-Way Hash function to authenticate in the routing update mechanism in order to enhance the routing security. Securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. Distance vector protocols encapsulate the route information into a hop count value and a next hop. Attacking node cannot build a valid route with a larger sequence number that it received because of properties of hash function.

As SEAD incorporates neighbor authentication through Hash functions, an attacker cannot compromise any node. Routing table overflow attacks are possible in this, as SEAD is based on a table driven approach. A compromised node can advertise routes to nodes which are not in the network and there by fill in the space allocated in the routing table with false node routes. Spoofing attack is potential through compromised node performing like a destination node in the route discovery process by spoofing the identity of the destination node that can cause route destruction. Black hole attack is also possible through a compromised node advertising the shortest roots to non-existing nodes in the network. Wormhole attack is also possible through compromised nodes. Rushing Attack and Denial of-service attack is not possible. Table driven protocols are much more prone to security threats.

E. ARIADNE

Ariadne is a secure routing protocol developed by Yih-Chun Hu, David B. Johnson and Adrian Perrig based on the Dynamic Source Routing protocol (DSR) [6].

The basic routing mechanism of DSR is used in Ariadne[7] and it uses TESLA [12] broadcasting authentication protocol. Ariadne provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the pair of communicating nodes. In Ariadne a route request packet (RREQ) contains eight fields: RREQ, initiator, target, id, time interval, hash chain, node list, and MAC Address List.

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime.

Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops in routing, since a packet is passing only through legitimate nodes will not be forwarded. Rushing attack, Routing table modification, Denial of-service Attacks and Black hole attack is not possible in Ariadne but Wormhole attack is possible in Ariadne.

F. SLSP: Secure Link State Routing Protocol

A The Secure Link State Routing Protocol (SLSP) [9] has been proposed to provide secure proactive routing for mobile ad hoc networks. This secures the neighbor discovery and the distribution of link state information both for locally and network-wide scoped topologies. SLSP can be employed as stand-alone solution for proactive link-state routing, or combined with a reactive ad hoc routing protocol creating a hybrid framework. The Secure Link State Routing Protocol (SLSP) is used to secure the discovery and the distribution of link state information. This protocol makes use of asymmetric key for the security purpose. Participating nodes are identified by the IP addresses of their interfaces. SLSP can be logically divided into three major steps which are as follows:

- Public key distribution: SLSP do not make use of any central server for key distribution. Distribution of public key is done by the node to the nodes within its own neighborhood. This distribution of the key is called as public key distribution (PKD).
- Neighbour discovery: Link state information of the node is broadcast periodically using Neighbour Lookup Protocol (NLP). Hello message contains sender's MAC address and IP address of the network. These messages are also signed. NLP can be used for identifying the discrepancies or the malicious node.
- Link state updates (LSU): Link state update (LSU) packets are identified by the

IP address of the initiating node and include a 32-bit sequence number for providing updates. Intermediate nodes LSU verify the attached signature using a public key they have previously cached in the pubic key distribution phase of the protocol. The hops traversed field of the LSU is set to hashed hops traversed, the TTL is decremented and finally the packet is broadcasted again.

To protect against denial of service attacks, SLSP nodes maintain a priority ranking of their neighboring nodes based on the rate of control traffic they have observed. High priorities are given to nodes that generate LSU packets with the lowest rate. This functionality enables the neighbors of malicious nodes that flood control packets at very high rates to limit the effectiveness of the attack.

SLSP provides a proactive secure link state routing solution for ad hoc networks. SLSP offers protection against individual malicious nodes by securing the neighbor discovery process and using NLP as a way to detect discrepancies between IP and MAC addresses. As it is mentioned by the authors, SLSP is vulnerable to colluding attackers that fabricate non-existing links between themselves and flood this information to their neighboring nodes. `Rushing attack, routing table modification, Denial of-service Attacks and Black hole attack is not possible in SLSP but Wormhole attack is possible in SLSP.

G. SAODV: Secure Ad Hoc On-Demand Distance Vector Routing

SAODV is a secure routing protocol developed based on AODV. SAODV was developed by Manel Guerrero Zapata, N. Asokan [10]. SAODV in its implementation assume that there is already a central key management system through which every node can obtain public keys. Digital signatures are used to authenticate the fields of the message and hash chains to secure the hop count information. SAODV uses hash chains to authenticate RREQ and RREP flows between neighbor nodes in the route discovery process. A hash chain is formed with a one-way hash function and random seed. Every time a node originates a RREQ

or a RREP message, the maximum hop count field is set to the max time to live. The top hash value is calculated using the hash function 'h´ and the random seed to it. Every time RREQ or RREP are received by a node it verifies the hop count, [h (max hop) – hop count time] to check it with the value contained in the top hash value.

The intermediate node after the verification of its integrity and authentication, prepares a RREQ or RREP if it's the destination node. The node applies the hash function to the hash value in the signature extension to account for the new hop. The hash function field indicates which hash function has to be used to compute the hash.

When a node first receives a RREQ, it first verifies the signature before creating or updating a reverse route to that host. When the RREQ reaches the destination node, RREP will be sent with a RREP signature extension. When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. Only if the signature is verified, it will store the route with the signature of the RREP and the lifetime.

Once successful route discovery is made, the source and destination nodes communicate along the discovered routes. If a link break occurs in the topology a Route Error (RERR) message is generated like in AODV. This RERR's are secured again with digital signatures.

SAODV is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. Wormhole attack is possible through two compromised nodes. And Denial of-service Attacks is also possible. But Rushing attack, Routing table modification, and Black hole attack is not possible.

H. Byzantine Algorithm

N This protocol is used to protect the network from Byzantine failures which include modification of packets, dropping packets, attacks caused by selfish or malicious nodes. Byzantine algorithm [11] consists of three different phases:

• Route Discovery: When a source node wants to send the message, it broadcasts a route request packet containing source address, destination address, a sequence number, a weight list and the private key for authentication to its neighbors. On receiving the RREQ packet the intermediate node checks for RREQ entry in its cache. If there is no entry is found for the RREQ, it verifies the key for authentication and appends it in the list and rebroadcast it to other nodes. When the destination node is reached, it verifies the key and creates a route reply message (RREP). On receiving the RREP packet, source node confirms the private key. It also compares the received path and the existing path in routing table. If the received path is better than the existing path then it updates this path in its routing table.

• Fault Detection: In this phase source node for every received packet. If number of unacknowledged packets moves above some threshold value, a fault is registered on the path.

• Link Weight Management: This phase of the protocol calculates the weight of the links. If a link is identified as faulty by the fault detection phase its corresponding weight value gets doubled. In the route discovery phase link with lower weight value will be taken as better link.

This protocol is used to protect the network from Byzantine failures which include modification of packets, dropping packets, attacks caused by selfish or malicious nodes. Rushing attack, Denial of- service and Routing table modification attacks is not possible in Byzantine Algorithm. But Wormhole attacks and Black hole attacks are possible in Byzantine Algorithm.

I. Core

The CORE (a collaborative reputation mechanism to enforce node cooperation in MANET) is a protocol which works on the co-operative behavior of the nodes. It makes use of Reputation Table and Watchdog mechanism to identify the co-operative or misbehaving node. The reputation table component maintains a table of intermediate nodes and the associated reputation or ratings. The Watchdog component calculates the function and provides the Reputation value [12].

This protocol consists of a sender and one or more intermediate node. In this protocol, whenever an intermediate node refuses to co-operate with the sender node, CORE scheme will decrease the repudiation of intermediate node. This can lead to elimination of intermediate node from the network.

CORE is a protocol which works on the co-operative behavior of the nodes. It makes use of Reputation Table and Watchdog mechanism to identify the co-operative or misbehaving node. Rushing attack, Routing table modification Wormhole attacks and Black hole attacks are possible in CORE but Denial of- service attacks is not possible in CORE.

J. Confidant

The Confidant (Cooperation of Nodes: Fairness In Dynamic Ad hoc Networks) protocol is use to identify the non cooperative nodes. This protocol consists of: the monitor, the path manager, the reputation system and the trust manager. The monitor component is responsible for monitoring passive acknowledgements for each packet it forwards. The trust manager component deals with the sending and receiving of alarm messages. When a node finds that a node is misbehaving, it sends an alarm message. Such messages are exchanged between nodes that are pre-defined as friends. Alarms from other nodes are given substantially less weight [13].

The reputation system component maintains a table of nodes and the associated ratings. Ratings are modified according to a rate function that makes uses of small weights if an alarm is reported for a misbehaving node and greater weights for direct observations. The path manager component manages all path information regarding addition, deletion, and updating of paths according to the feedback it received from the reputation system. If a rating falls under a certain threshold the path manager component is called in order to remove the path containing the identified malicious node.

The Confidant protocol is use to identify the non cooperative nodes. Rushing attack, Wormhole attacks and Black hole attacks are not possible in Confidant. But Denial of- service and Routing table modification attacks are possible in Confidant.

K. Watchdog and Path rater

Number The watchdog and path rater protocol is used to find out the malicious nodes which deny forwarding the packets however they have agreed to forward it earlier. The role of Watchdog is to watch that the next node in the path is forwarding the data packet or not. If not then it will be taken as the malicious behavior. Role of path rater is to evaluate and find the reliable path from the result generated by watchdog [14].

When a node transmits a packet to the next node in the path, it tries to listen if the next node will also transmit it and also tries to find out that the next node do not modify the packet before forwarding it. If a node shows any malicious activity like denial of service or modification of data packet, Watchdog will increase its failure rating. This failure rating is helpful in finding out the reliable path from source to destination.

The watchdog and path rater protocol is used to find out the malicious nodes which deny forwarding the packets however they have agreed to forward it earlier. Rushing attack, Denial of- service Routing table modification attacks and Black hole attacks are possible in Confidant. Detection of Wormhole attack is not possible in Watchdog and path rater and approaches for detecting wormhole attacks are proposed in [15-18].

III. PROPOSED APPROACH

Every node should share its public key with its neighbors during neighbor discovery phase. HELLO message is having following structure

HELLO (Source, Hash (source), public key of source)

HELLO_REPLY has following structure

HELLO_REPLY (Source, destination, Encrypt (Hash (source)), public key of source)

Where hash value is encrypted with private key of source, so source of HELLO_REPLY is verified.

Routing table in proposed algorithm will hold public key of destination node along with next_node and delay.

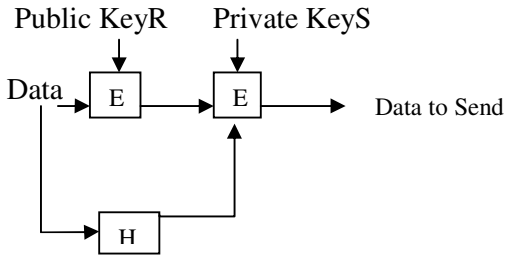

Figure: 3.1 Encryption and Authentication

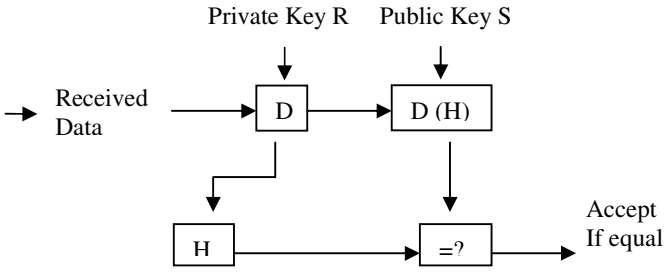

Figure: 3.2 Decryption and Verification

Data Transmitted by node is in encrypted form as
ED=Encrypt (KSprivate, Encrypt (KRpublic, D)) + Encrypt (KSprivate, H(D))
Where
E is public key encryption function,
KSprivate is private key of sender node,
KRpublic is public key of Receiving Node,
H (M) is hash function to calculate message digest.
This eliminated pretending identity of neighbor node completely even if attacker in present at time of neighbor discovery. If node receives data with false digest value then it declares packet received through wormhole node and discards packet. It also discards routing entry for wormhole node.

IV. RESULTS AND DISCUSSION

Proposed system is simulated on OMNeT++ with 200 X 200 meter network with 10% attacking nodes.

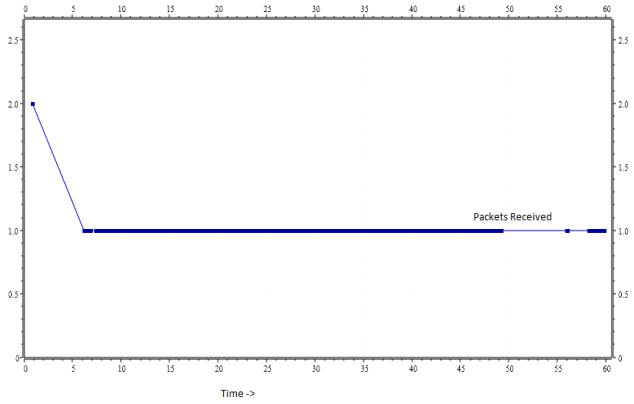

Figure: 4.1 No of Packets Received by attacker Node

Figure 4.1 shows that number of packets received by attacker node decreases as it is excluded from routing table and packets are not routed through it to mitigate wormhole attack.

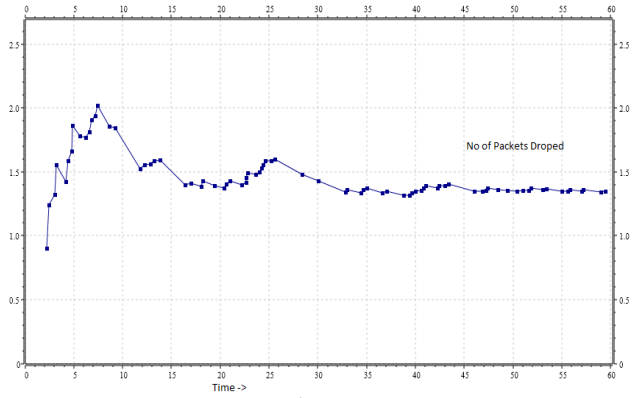

Figure: 4.2 No of affected and dropped packet

Figure 4.2 shows that in initial phase no of affected packets are more, but with time attacking nodes are detected and routing table is changed to avoid attacking nodes. This results into decrease in packet drop due to modification by attacking node.

V. CONCLUSION

In this paper we analyzed secure routing protocols and their effectiveness to detect several possible security attacks on MANET environment. Most of the secure routing protocols are not effective to detect and mitigate wormhole attack. This paper proposes a routing algorithm with public key cryptography to detect and mitigate wormhole attacks. Simulation results shows that proposed algorithm is effective is detecting and mitigating wormhole attack.

ACKNOWLEDGMENT

Thanks to Bharati vidyapeeth College of Engg. Pune, & Moze College of Engg., Balewadi.

REFERENCES

[1] Stallings W, Network Security Essentials: Security Attacks. Prentice Hall. , 2000 (pp. 2-17)

[2] Parul Tomar, M. K. Soni and P.K. Suri "A Comparative Study for Secure Routing in MANET" from YMCA University, MRIU and Kurukshetra University, in International Journal of Computer Applications (0975 – 8887), Volume 4 – No.5, July 2010, pp. 17-22.

[3] C. Siva Ram Murthy and B.S. Manoj. Ad Hoc Wireless Networks, Architecture and Protocols: 2004 Pearson Education (pp. 321-386, 473-526)

[4] Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02), 2002.

[5] Seung Yi, Prasad Naldurg and Robin Kravets in the Dept. of Computer Science, University of Illinois at Urbana-Champaign.

[6] Basagni, S. Conti, M. Giordano, S. Stojmenovi & cacute (Edit). Mobile Ad Hoc Networking: September 2004 Wiley-IEEE Press. (pp. 1-33, 275-300, 330-354), 2004.

[7] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02).

[8] P. Papadimitratos and Z. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In IEEE Wksp. On Security and Assurance in Ad Hoc Networks, 2003.

[9] P. Papadimitratos and Z. Haas. Secure Link State Routing for Mobile Ad Hoc Networks. In IEEE Wksp. On Security and Assurance in Ad Hoc Networks, 2003.

[10] M. Zapata and N. Asokan. Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. ACM Mobile Computing and Communications Review, vol. 3, no. 6, July 2002, pp. 106-107.

[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru and H. Rubens. An On-Demand Secure Routing Protocol Resilient to Byzantine Failures. WISE'02, Atlanta, Georgia, September 2002, pp. 21-30.

[12] P. Michiardi, R. Molva. Core: A Collaborative Reputation mechanism to enforrce node cooperation in Mobile Ad Hoc Networks. In Communication and Multimedia Security Conference, 2002.

[13] S. Buchegger, Jean-Yves Le Boudec. Cooperation of Nodes — Fairness in Dynamic Ad-hoc NeTworks. IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC).

[14] Sergio Marti, T.J. Giuli, Kevin Lai and Mary Baker.Mitigating routing misbehavior in mobile ad hoc networks. ACM MobiCom, 2000, pp- 255-265.

[15] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2008, pp. 343-348.

[16] Wang, W.; Bhargava, B. Visualization of Wormholes in Sensor Networks. In Proceedings of the 2004 ACM workshop on Wireless Security (WiSe), ACM WiSE'04, Philadelphia, PA, USA, October 2004; pp. 51–60.

[17] Shah Vrutik, Dr.Nilesh Modi and Patani Ashwin, "AODVGAP-An Acknowledgment Based Approach to Mitigate Selective Forwarding Attacks in Manet" International journal of Computer Engineering & Technology (IJCET), Volume 3, Issue 2, 2012, pp. 458 - 469, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375, Published by IAEME.

[18] Mrs. S. A. Nagtilak and Prof. U.A. Mande, "A Survey Of Mitigating Routing Misbehavior In Mobile Ad Hoc Networks" International journal of Computer Engineering & Technology (IJCET), Volume 1, Issue 2, 2010, pp. 106 - 117, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375, Published by IAEME.

AUTHORS' INFORMATION

Pradnya R. Patange has completed B.E.I.T. from Govt. College of Engg. Karad. Currently doing MTECH IT from Bharati Vidyapeeth College of Engg., Pune..

Sampat Medhane working as a Assistant professor in Department of Information Technology at Bharati Vidyapeeth College of Engg, Pune.