Lightweight Node Authentication and Establishing a Secure AODV protocol in Mobile Ad hoc Network

V. JoshibhaBency, C. Annadurai, D. Ramkumar, R. Rajesh

Abstract*: *A MANET is an independent network communication through a wireless medium without requiring any fixed infrastructure, where a target node is not in the direct range of transmission over a sender node, and where midway nodes are needed in order to forward packets. The midway nodes here are not only the host but also acts as a router for hand over packets. Nonetheless, it is very simple to attack the defenseless character of the ad hoc networks by malicious node like the dropping or hand over of forged data etc. As the need for dynamic network is constantly developing, security problems in the network layer in particular must be properly solved according to MANETs. This paper discusses a series of routing violations and proposes an improvement in AODV's design to authenticate route requests using digital signatures to prevent malicious node attacks.

Keywords*: *MANET, AODV Protocol, Attacks, Secure Routing, Cryptography, Digital signature.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a wireless autonomous network which forwards packet over a wireless link. MANET is an infrastructure less network in which mobile nodes act as router and host to communicate with each other. MANET does not have any centralized control unit for communication since MANET is decentralized in nature which means it does not have any relay on fixed routers to route packet from initiator to target. MANET does not have any fixed topology for communication and its topology is dynamic in nature. MANET has various advantages such as low cost and it is fast to deployment. Since it is an open medium for communication it has various applications on the battlefield, rescue operation and some other where we do not have any centralized Control unit.

Nodes in MANET will communicate with each other in this with proficient reactive protocol like AODV and there are some loop holes in this protocol are the serious problem since MANET are open medium for communication there may be some malicious node which may attack our data which we are transferring within nodes. Various attacks are there, one among them is black hole attack. In MANET the most dangerous attack is Black hole attack which affects mostly Ad-hoc On-demand Distance Vector (AODV) reactive routing protocol. Black hole attack concentrate mostly on route discovery process in ad hoc routing.

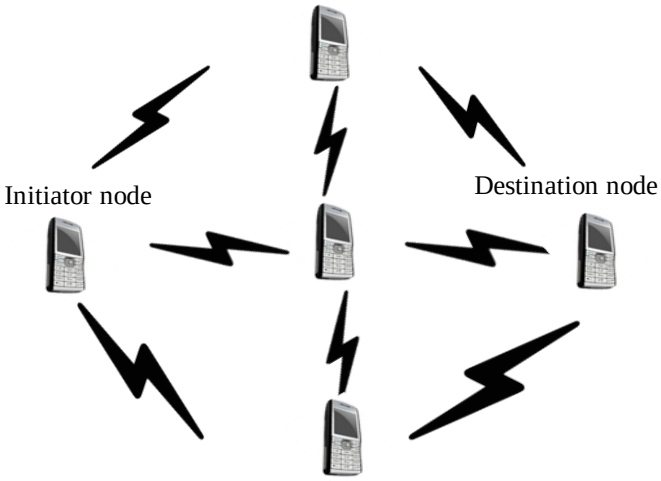


Fig.1 MANET Architecture

Here, black hole node bluffs other nodes in the network by sending least route and updated route to reach the target node. In this paper, we do simulation analysis for performance comparison of our proposed protocol with traditional AODV protocol based on various node mobility. The success of any network depends on the authentication of nodes to receive packet and transfer packets. Hence, the challenge is to design a light weight node authentication protocol for the resource constrained ad hoc network.

II. AODV PROTOCOL

Ad-hoc on demand Distance vector (AODV) is a standard routing protocol for wireless ad hoc networks the attack of network by malicious nodes creates a major problem in this AODV protocol. Each node maintains the routing table with the help of RREQ packet for forwarding data to target. In order to send data through a particular node it checks the routing table about the availability of route to that target. If the route is available in the routing table it transmits the packet else it broadcast RREQ packet to its neighbors to identify the new route. Next step to identify route is by comparing destination sequence (DS) number of RREQ packet in routing table.

Revised Manuscript Received on May 8, 2019.

V. Joshibha Bency, Department of Electronics and Communication Engineering, SSN College of Engineering, Kalavakkam, TN, India.
Dr. C. Annadurai, Department of Electronics and Communication Engineering, SSN College of Engineering, Kalavakkam, TN, India.
D. Ramkumar, Department of Electronics and Communication Engineering, SSN College of Engineering, Kalavakkam, TN, India.
R. Rajesh, Department of Electronics and Communication Engineering, SSN College of Engineering, Kalavakkam, TN, India.

If DS number is present in the routing table then it will be the last route reply by the target and the RREP packets (Route reply) are sent through reverse route to reach target node. Then the initiator node update with target route and sends the data through the obtained route path where if any link failure occurs on the path means the node will reply with RERR (Route error) packet.

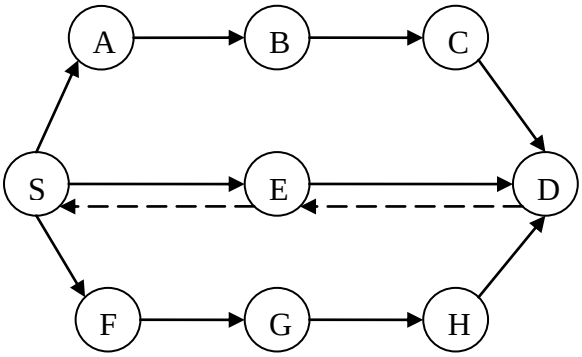


Fig. 2 Route Discovery Mechanism

III. SECURITY IN MANETS

Wireless ad hoc networks are highly exposed to attack when compared with wired networks. Wireless Security plays an important role to provide secure environment for ad hoc networks. Another import issue remains the reliability as networks operate under battery constrained and hostile environment. Mostly, ad hoc networks are observed to be affected by interference of control messages. Each layer performs various tasks as a result providing security is a challenging task in mobile ad hoc networks. In this paper, we concentrate highly on network layer security. Considering the various disciplines of ad hoc networks, most routing protocols are simple in design and can be easily attacked by attackers. In general, levels in which a attacker node can operate are given below

- The topology of the network generated by the protocol in which the attacker aspire to impede the function of routing nodes targeted in order to disconnect them from the rest of the network.
- The malicious nodes bluff the nodes in network topology to stop its function in order to destroy network functionality.
- Communication among nodes.

Example attacks are:

Black hole attack [1]: Malicious node advertise itself as the path for sending packets to initiator node.
Byzantine attack [2]: Malicious node degrades the routing QoS by creating collision and packet disorder.
Location disclosure attack [3]: Malicious node identifies the structure of network and location of target nodes. The main aim of this attack is to create performance degradation and location disclosure.
Wormhole Attack Model [4]: A type of network layer attack created by one to many number of malicious nodes. It uses wormhole link to channels the packets.
Sleep deprivation attack [5]: A Denial-of-Service (DOS) attack affects the battery life of network in a critical situation. The main aim of this attacker is to send unwanted control packets to reduce the battery power of nodes.

IV. LITERATURE SURVEY

Several researchers have proposed different solutions to provide ad hoc network secure routing to prevent a network from malicious node especially blackhole attack. Sandeep Lalasaheb et al. [1] summarized about various routing protocols in adhoc networks and proposed a reactive detection method to remove routing messages overhead problem in the network but the protocol suffer high packet loss in routing its data. LalitHimra et al. [2] suggested a method to identify Black Hole attacks with its sequence number, the large difference between initiator and midway sequence number affects RREP packets. Nabil Nissar et al. [3] proposed an improved AODV protocol with digital signatures to reduce routing attacks over malicious intruders NishuKalia et al. [4] suggested a method for black hole attack detection where sender node broadcasts its own address and sequence number included into fake RREQ packet instead of target address and target sequence number as the target nodes sequence number is the most recent and fresh sequence number. But in this situation, the legitimate midway node will use small initiator sequence number described by fake RREQ packet because only initiator node will have its latest or fresh enough sequence number. But if there exists malicious nodes in the network, then they reply with RREP packet as it will advertise itself have the shortest route with the highest sequence number. AdwanYasin et al. [5] proposed a technique to identify black hole attacks using timer and bait message which contains Non neighbor Reply and two phase Baiting. Dhara Buch et al. [6]suggested a method to overcome the wormhole attack without any external hardware algorithms where he developed two-hop neighbors Route Reply packet using Probe message and Acknowledgement message from its two hop neighbours.JiwenCai et al. [7] in this paper introduced collision rate reporting system for MAC layer by lowering the false positive rate of the network with high overload situation.Aqeeltaha et al. [8] highlighted the use of fitness function to reduce the energy consumption using AOMDV with the fitness function (FF-AOMDV). The fitness function values are helpful to identify the optimal route from sender node to target node by reducing energy utilization in routing. SisilySibichen [9] proposed a security techniques based on Rivest Shamir Adlemen algorithm and avoided rekeying problem using double key encryption techniques among neighbor nodes in the ad hoc network.

Ali Dorri [10] defined security parameters in two different aspects for MANET. One is comprehensive approach and next defeating approach against various attacks with performance metrics. Yang [11] has discussed the various security challenges in design of network and functionalities of network layer in transmitting packets in wireless channel. The similar studies have been revealed in [12]. Lehane B et al [13] introduced a new method to generate shared RSA algorithm. The main goal of this technique is to provide message authenticity using robust key management. S. Sumathy and B. Upendra Kumar et al. [14] developed group communication of nodes with RSA public key cryptography. Here, all participating node in the network is assigned with symmetric key. Key aim is to do encryption and decryption of transmitted, symmetric key is used by each node to access all other node in the network. RSA public key cryptography helps in exchanging symmetric key between initiator and target. Rezvani et al introduced [15] a collaborative based reputation technique to evaluate credibility of each node in the ad hoc network. Here, the trustworthiness and credibility of nodes helps to identify malicious nodes to stop it from receiving attacker data.

V. PROPOSED WORK

The proposed work here is to provide solution from the malicious activities performed by the blackhole attackers. The AODV protocol has works under on-demand approach. i.e. when the pioneer node needs to communicate with the target node, the route will be created instantly and the life time of the route get expires once the transmission gets over, this approach is called on demand approach. Here, AODV protocol is a network unprotected protocol because it does not think about any system to authenticate the messages exchange between the midway nodes. Commonly, AODV routing protocol is flat to several kinds of attacks that mainly concentrate on integrity, authentication, and non-repudiation. Our proposed method is depends on route request authentication technique and timer based route reply technique.

Route Request Authentication Technique

The main intention of using route request authentication for routing messages are to assurance the following security characteristics:

Integrity: This property makes sure that AODV routing nodes content from the initiator node has not been altered or modified by malicious nodes, thanks to digital signature verification. A hop-to-hop and end-to-end message authentication technique is supported for the integrity of routing messages.

Non-repudiation: In our proposed directing system, the route request messages are encrypted using a confidential key by the sender, and will be approved by the collector node using open key of the sending node. This successful validation ensures that the messages are not repudiated and that the message is sent by the node which has signed the message and cannot be reputed by any other nodes especially malicious nodes. The authentication method is planned in two steps: hop-by-hop authentication at mdiway nodes and end-to-end authentication at the target node. Here the public key cryptosystem Rivest-Shamir-Adleman (RSA) is used for authentication; therefore messages for the route request are signed by the initiator node as well as all midway nodes using a private key and verified by the receiving nodes with a public key of the sender. When initiators need to communicate to a target node, a route request message (RREQ) will first be broadcast to its neighboring nodes by the initiator node. The initiator ID and broadcast ID of a RREQ packet are unique. When a midway node has received the RREQ packet, it creates the route response packet for the previous hop node, to which the RREQ packet is sent. At the same time, the midway host will check its routing table for a path to the target node, and the path will be fresh enough, if it sends the RREP (Return Packet) to the initiator node by using the Return Path, and if that is not, will increases the number of hops filed and retransmit the RREQ. By removing every RREQ packet with the same initiator ID and broadcast ID, the loopback problem prevents the mid-node. Until the target node, the RREQ packet will be broadcast. Once the RREQ is received by the target node, only the first RREQ will be elected to form the opposite route, with the remaining RREQ from the same initiator ID and broadcast ID get discarded. The target nodes unicasts the RREP packet answer to the initiator node. Every midway node receiving RREP in the opposite direction unicasts it back to the initiator node in the opposite way, according to the previously defined reverse route. Finally, the initiator node can start sending data via the route that has just been established, once the RREP reaches the initiator node. Within our technique, each node wishing to connect with the network must have the ability, and its public key must be transferred to its network nodes to verify the signature of initiator or midway nodes. This verifies the original route request from the initiator or midway node has been end-to-end authenticated / hop-to-hop, integrity and non-repudiation. The following two phases are composed of our proposed method.

Authentic Route Request (RREQ) Phase

The scheme of our Authentic Route Request (RREQ) phase begins as soon as an initiator node S sends a data to a target node D. It begins with the sender sending a message called "RREQ". This RREQ is a packet sending by the initiator node to initiate the route establishment process. The RREQ packets created by the initiator node S have two main fields: payload and digital signature. The RREQ are secured in the Payload packet format and described by them. The following fields are included in each:

Payload: {RREQ}.
Digital Signature :{(SID, DID, RID, SSN, DSN); Kpr_SN}.

Payload	Initiator Node Signature
RREQ	Digital Signature_SN:{(SID, DID, RID, SSN, DSN); Kpr_SN}

The digital signature append by the initiator node

- **RREQ:** Route Request
- **SID:** represents the Initiator node ID.
- **DID**: represents the target ID.
- **RID**: represents the route request ID.
- **SSN**: represents the initiator sequence number.
- **DSN**: target sequence number.
- Kpr_SN: is the private key of the initiator node.

After a neighboring node n receives RREQ from the initiator node S with single signature, it first checks the integrity of the request by confirming the initiator signature with the public initiator key. The next node will continue to update, for instance, the hop count on the RREQ when the RREQ is successfully authenticated. The neighboring node n generates its own signature using its private key and attaches this signature at the end of the RREQ packet before its starts forwarding. The new packet format of route request is as follows:

RREQ		**Digital Signature of Neighbor node**
Payload	Initiator Node Signature	Digital Signature_NN:{(SID, DID, RID, SSN, DSN, HopCount; Kpr_NN}
The digital signature append by the neighbor node		

Any midway node, which is a one - hop node outside the initiator node, will receive a RREQ message with double signature during the route request phase. Once the node i receive a double signed RREQ message, the signature will only be authenticated using the exchanged and assurance public keys on the basis of the hop-by-hop authentication of the forwarding node. If authentication succeeds, after you have signed your RREQ message, node i will re-transmit the RREQ packet and replace the signature of the transmission node with the signature of its own in the RREQ packet. The node format of the broadcast message is as follows:

RREQ		**Digital Signature of Midway node**
Payload	Initiator Node Signature	Digital Signature_IN:{(SID, DID, RID, SSN, DSN, HopCount; Kpr_IN}
The digital signature append by the midway node		

The attested RREQ packet will reach target node D by repeating the above procedure, the signature of the forwarding node is first confirmed and the signature of the initiator node Kpr SN is then confirmed by the target node D. The message is guaranteed if validation succeeds, that the route request packet is unchanged with malicious nodes (integrity), and was actually sent by S initiator node (non-repudiation). Then target node confirms the signature of its next node as in the previous section's midway node. This end-to-end authentication scheme can prevent attacks that cannot be solved using the authentication method of hop-by-hop authentication.

Route Reply Phase

Every midway nodes must sends a RREP packet to the initiator node during this phase. First the target node uniquely unifies the RREP packet in the reverse path to the neighboring node to reach the initiator node.

Timer based route reply

We propose a style which will be able to avoid malicious attack to access data especially black holes attacks. We suggested doing that by an initiator node can create a table called route response table (RRT). When the RREP message is received by the initiator node it must wait a while to receive any additional RREP message from another path. It sets timer to collect additional requests from different midway nodes after the first route reply message is received. The initiator sequence number and arrival time of the RREP message will be stored in route response table (RRT). There will be an expiration of the timeout, the initiator node checks first in RRT if the table has more than one route. If the RRT table accommodates multiple route response, then the initiator node should assumes that the blackhole attackers either can present over the first route, and the second path is taken as correct, or the likelihood of malicious routes is limited. The initiator node therefore discards the first path and selects the second path as the best way to transmit data.

Working principle

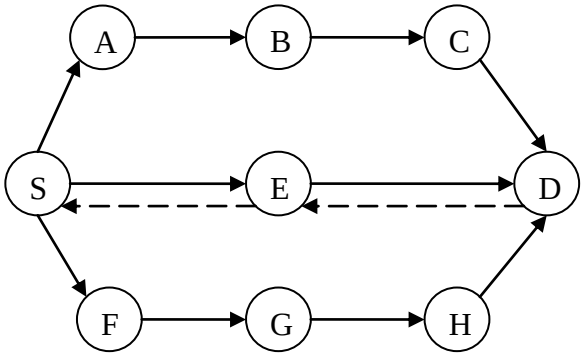


Fig. 3 Proposed Route Discovery Mechanism

The initiator node S in the figure wants to pass on information to the target node D. Node S therefore transmits the secured route detection packet (RREQ) to its next immediate node. This packet for secured track detection includes payload and digital signature. Once a next immediate nodes n receives a single digital signature RREQ from the initiator node S, the route request integrity is first checked by confirming the signature of the initiator by the initiator's public key. The next immediate of initiator node continues, such as the hop count updates on the RREQ, when the RREQ is successfully authenticated. The next immediate nodes n produces its own signature on the RSA Public-Key Cryptosystem using its private key and hook up the signature to it prior to shipment at the end of a route request packet.

When a node that is one-hop from the initiator node is a second node called midway node receives a RREQ packet with double signature. The first signature is signed by initiator node and the second signature is signed by next immediate node of the initiator node. Only the second signature will become authenticated by the hop-by-hop authentication on the basis of the exchanged and trusted public keys, if the node receives the double-signed RREQ message. If the authentication is successful, the midway nodes replace the signature in the RREQ packet of the forwarding node with its own signature before forwarding them. After signing the RREQ message node will retransmit the message similar to the previous one. The authenticated RREQ packet arrives at the target node D by repeating the above procedure. It first verifies the signature of the forwarding node and then the Kpr_SN signature of the initiator node. The message validates the integrity and non - repudiation of the packet. In the same process as in the midway nodes granted in the above section, the target node confirms the signature of its nearest node. This end-to-end authentication system can prevent changes and impersonation attacks which cannot be solved by hop-by-hop. The target node consolidates the RREP packet in the reverse path back to the next node to reach the initiator node. After the RREP packet is received by the initiator node, it has to wait for some time to receive any other RREP message from any other path. It sets timer for the collection of additional requests from different nodes after the first route message is received. The initiator sequence number and time that the route reply packet arrives, is stored in a Route Response Table (RRT). When the timeout get expire, the initiator node checks first in the RRT if the table accommodate more than one route response. If more than one route is found on the RRT table, the initiator node can assume that this indicates the presence of the blackhole attackers in the first path and the second path is correct path for the data transmission. This way the initiator node neglects the first path and chooses the second path as the best path to transmit data.

VI. SIMULATION RESULTS

Our authentication method is proposed to secure the RREQ message from the malicious node. The initiator node therefore found secured path or the target node that guaranteed a received RREQ message was received from the regular node, so it can't spoof another node ID for sending a message due to the authentication of a digital signature. Our technique can therefore prevent a node from attacking especially network layer routing attacks.

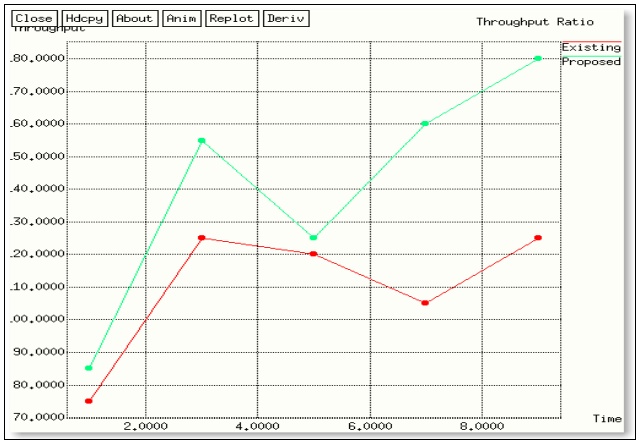
The NS2 network simulator was used to simulate the system. We can analyze the performance of the network by changing the nodes mobility.

Simulation Parameters

Simulator: NS-2.34
Speed: Max 15mpbs
Simulation Time: 250s
Routing Protocol: AODV
Packet size: 512bytes
Coverage area: 800x800m
Node : 25,50,100,150
Attack: Routing Attacks

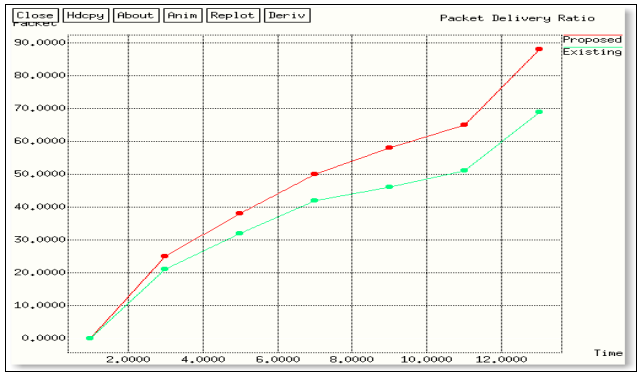
Throughput

Performance is the amount of output that can be prepared in a certain time period. The number of packets received successfully in one unit time. Calculation of the performance with the awk script processes the trace file and produces the result. The simulation was done using NS2 network simulator to calculate the throughput for data transmission over the dynamic network. By frequent changes in the nodes, the performance of the network can be analyzed. The graph analysis can be showed in the following figure. Here the throughput of the proposed method can produce better result compared with existing technique.



Packet Delivery Ratio (PDR)

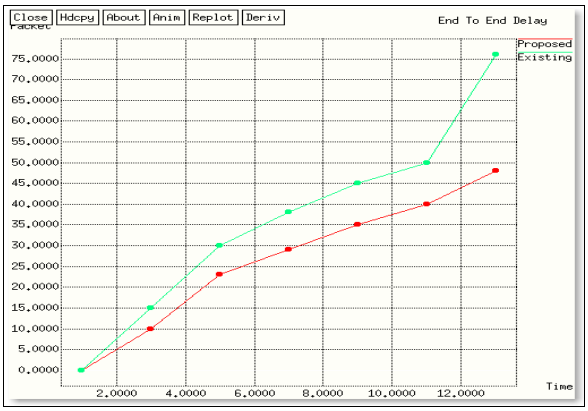
The packet delivery ratio (PDR) calculation is based on packets that are received and generated in the trace file. PDR is generally defined as the ratio of packets received by the target node and ratio of packets sent by the initiator node.



End To End Delay

Delay is the difference between the sender's time and the recipient's time of receipt of the packet. Here the end-to-end delay is comparatively high compared with existing technique due to ensuring node authentication done at every node over path.

Even the delay is considerable while we achieve the delivery rate for packets are high even in the presence of malicious node.



VII. CONCLUSION

In this work, we have proposed an authentication route request and a timer based route reply security solution for AODV routing protocol. We have been trying to integrate safety mechanisms that are best suited to the authentication and detection of nodes. These mechanisms have been suggested while guaranteeing security services for messages routing. In the beginning we offer a solution for node authentication in order to guarantee integrity and non-repudiation with a cryptography technique. In comparison with other proposed solutions due to a hop-to-hop and final authentication, this technique had some smaller delay and overhead routing.

REFERENCES

1. SandeepLalasahebDhende, Dr. S. D. Shirbahadurkar, Dr. S. S. Musale, Shridhar K Galande 'A Survey on Black Hole Attack in Mobile Ad Hoc Networks',International Conference on Recent Advances in Information Technology,2018.
2. LalitHimral, Vishal Vig&Nageshchand 'Preventing AODV Routing protocol from Black Hole Attack',International Journal of Engineering Science and Technology,2011.
3. NabilNissar, NajibNaja, AbdellahJamali 'Lightweight Authentication-based Scheme for AODV in Ad-hoc Networks', International Conference on Wireless Technologies, Embedded and Intelligent Systems, 2017.
4. NishuKalia, Harpreet Sharma 'Detection of Multiple Black hole nodesattack in MANET by modifying AODV protocol' International Journal on Computer Science and Engineering, 2016.
5. AdwanYasin, Mahmoud Abu Zant 'Detecting and Isolating Black-Hole Attacks inMANET Using Timer Based Baited Technique', Wireless Communications and Mobile Computing, 2018.
6. DharaBuch and DeveshJinwala 'PREVENTION OF WORMHOLE ATTACK INWIRELESS SENSOR NETWORK', International Journal of Network Security & Its Applications, Vol.3, No.5, Sep 2011.
7. Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU 'An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network', IEEE International Conference on Advanced Information Networking and Applications,2010.
8. Aqeeltaha, Raedalsaqour, Mueenuddin, Mahaabdelhaq and tanzilaSABA 'EnergyEfficient Multipath Routing Protocolfor Mobile Ad-Hoc Network Using theFitnessFunction', IEEE Journals & Magazines, 2017
9. SisilySibichen, SreelaSreedhar, 'An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks', pg: 1-6, IEEE Conferences, 2013.
10. Hao yang, Haiyunluo, Fan ye, Songwulu, and Lixiazhang, 'Security in Mobile adhoc networks', Volume:11, Issue: 1Page s: 38 - 47, IEEE Journals & Magazines, 2004.
11. Ali Dorri and Seyed Reza Kamel and Esmailkheyrkhah, 'Security Challenges In Mobile Ad Hoc Networks: A Survey', Vol.6, IEEE Journals & Magazines, 2015.
12. C.Siva Ram Murthy and B.S.Manoj," Ad hoc Wireless Networks–Architectures and Protocols", Pearson Education, 2007.
13. Lehane B., Doyle L., O'Mahony D, "Shared RSA key generation in a mobile ad hoc network", Military Communications Conference, 2003, IEEE Xplore, Volume 2, pp. 814 - 819, 2003.
14. S. Sumathy and B.Upendra Kumar, "Secure Key Exchange and Encryption Mechanism for Group Communication in Wireless Adhoc Networks", International Journal on Applications of Graph Theory in Wireless Adhoc Networks and Sensor Networks (Graph-Hoc), Volume 2, No. l,pp. 9-16, 2010.
15. Rezvani, M., Ignjatovic, A., Bertino, E., Jha, S.: A collaborative reputation system based on credibility propagation in WSNs. In: IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS 2015), pp. 1-8, December 2015
16. D. Ramkumar and C. Annadurai " Continuous Authenticaion Consoles in Mobile Ad hoc Networks (MANET)", Cluster Computing, Springer, Nov 2017.

AUTHORS PROFILE

V. JoshibhaBency is PG scholar in the Department of ECE at SSN College of Engineering, Kalavakkam, Chennai, India. She received B.E degree in 2017, from Anna University, Chennai, and pursuing M.E at SSN college of Engineering, Kalavakkam, Chennai, Tamil Nadu, India. Her research interest includes several aspects of Wireless Communications, Mobile Ad hoc Networks, Pervasive Computing and Wireless Sensors Networks.

C. Annadurai received a PhD degree in Information and Communication Engineering from Anna University in 2016. He is an Associate Professor in the Department of Electronics and Communication Engineering at SSN College of Engineering, Kalavakkam, Chennai, India. He received M.E degree and B.E degree in 2002 and 1991, respectively, from Bharathiar University, Coimbatore India. He is Life time member of ISTE and IEI. His research interests include several aspects of wireless communications such as MIMO, Cooperative communication and Embedded Design.

D. Ramkumar is currently pursuing PhD in mobile ad hoc networks at SSN College of Engineering (affiliated with Anna University), Kalavakkam, Chennai, India. He received M.E degree and B. Tech degree in 2012 and 2007, respectively, from Anna University, Chennai, India. His research interests include several aspects of Wireless Communications, Mobile Ad hoc Networks, Pervasive Computing, Wireless Sensors Networks, Internet of Things, and Network Security.

R. Rajesh is currently pursuing PhD in Internet of Things at SSN College of Engineering (affiliated with Anna University), Kalavakkam, Chennai, India. He received M.E degree and B.E degree in 2010 and 2006, respectively, from Anna University. His research interests include several aspects of Internet of Things, Wireless Communications, Mobile Computing, Database Management System and Network Security.