International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.9, September 2014 DOI:10.15693/ijaist/2014.v3i9.128-134

Ensuring the data integrity and Authentication in MANET

S. Prabu

Abstract: **Mobile Ad Hoc Networks is the most popular networks widely used in various applications. It consists of mobile nodes where each node communicates with each other. The control of nodes is not administrated by any access point. Due to this, the network is easily impersonated by several attacks like active and passive attacks. These attacks degrade the performance of networks i.e. means network connectivity, network availability and communication coverage. To withstand the wormhole attacks, we propose the mechanism called Security based Wormhole detection scheme. This scheme comprises of two phases. In first work, we deploy the detection of wormhole attacks which makes the correct balance between safe route and stability. In second work, the RSA algorithm we used. This algorithm provides the integrity and authenticity of packets while travelling from source to destination nodes. By extensive simulation, the proposed scheme achieves better throughput, packet delivery ratio, low end to end delay and overhead than the existing schemes.**

Keywords - MANET, throughput, delivery ratio, packet loss, overall congestion standard, queue length, contention metric, flow control and congestion control.

I. INTRODUCTION

A. *Mobile Ad Hoc Networks (MANET)*

MANET relies on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANET becomes. But supporting a MANET is a cost intensive activity for a mobile node. Detecting routes and forwarding packets consumes network bandwidth, local CPU time, memory and energy. Therefore there is a strong motivation for a node to deny packet forwarding to others, while at the same time using their services to deliver own data.

MANET has various potential applications, which are usually set up in situations of emergency for temporary operations or simply if there are no resources to set up elaborate networks. Some typical examples include emergency search-rescue operations, meeting events, conferences and battlefield communication between moving vehicles and soldiers. With the abilities to meet the new demand of mobile computation, the MANET has a very bright future.

B. Wormhole attacks in MANET

In this attack, an attacker receives packets at one location in the network and tunnels packets to another location in the network, where the packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through a single long-range wireless link or even through a wired link between the two colluding attackers.

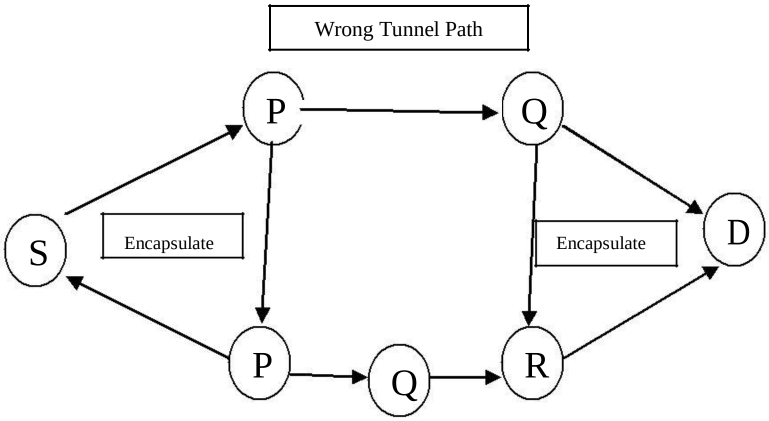

Figure.1. Wormhole Attack

Due to the broadcast nature of the radio channel, the attacker can create a wormhole even for packets not addressed to itself.

Example:

In figure1. **P** and **Q** are two malicious nodes that encapsulate data packets and falsified the route lengths. Suppose node **S** wishes to form a route to **D** and initiates route discovery.

When **P** receives a Route Request from **S,** ***Q*** encapsulates the Route Request and tunnels it to **Q** through an existing data route, in this case {**P --> P --> Q --> R -->**

Q}. When Q receives the encapsulated Route Request for **D** then it will show that it had only traveled {**S** --> **P** --> **Q** --> **D**}. Neither P nor **Q** update the packet header. After route discovery, the destination finds two routes from **S** of unequal length i.e. one is of 4 and another is of 3. If **Q** tunnels the Route Reply back to **P**, **S** would falsely consider the path to **D** via P is better than the path to **D** via R. Thus, tunneling can prevent honest intermediate nodes from correctly incrementing the metric used to measure path lengths. Though no harm is done if the wormhole is used properly for efficient relaying of packets, it puts the attacker in a powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node. Performance of wormhole attack can be shown in figure 2.In this attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point.

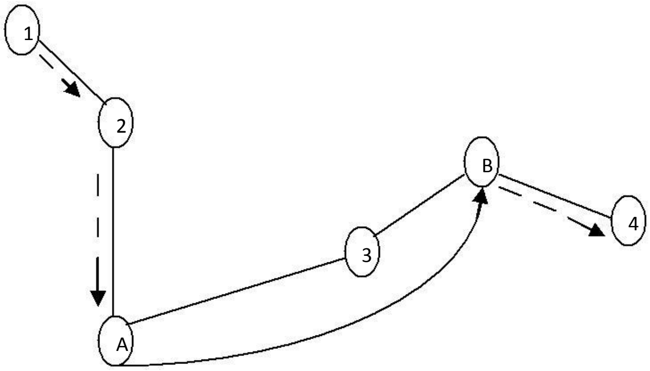

Figure.2. A wormhole attack performed by colluding malicious nodes a and B

Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole. Two malicious nodes share a private communication link between them.Worm hole can eavesdrop the traffic, maliciously drop the packets, and perform man-in- the-middle attacks against the network protocols.

II. RELATED WORK

T. Sakthivel and R. M. Chandrasekaran [1] proposed Path Tracing (PT) algorithm for detection and prevention of wormhole attack as an extension of DSR protocol. The PT algorithm runs on each node in a path during the DSR route discovery process. It calculates per hop distance based on the RTT value and wormhole link using frequency appearance count. Every node in a path has to compute per hop distance of its neighbor with the previous per hop distance to identify the wormhole attack. The corresponding node detects the wormhole if per hop distance exceeds the maximum threshold range. In the routing process, the wormhole link participates in more number than the normal link. This factor is used to detect the wormhole link using a link frequent appearance count.

Shalini Jain and Dr.Satbir Jain [2] presented the novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, they demonstrate that their scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase. It is derived that trust levels in neighbouring nodes based upon their sincerity in execution of the routing protocol. This derived trust is then used to influence the routing decisions, which in turn guide a node to avoid communication through the wormholes.

S. Madhavi and K. Duraiswamy [3] proposed a new methodology to detect and prevent the wormhole attack during the route discovery process. In a reactive routing protocol, whenever the node initiates the communication process, checks its routing table, if the entry is there for the destination node, it sends the data packet otherwise it finds the path through Route Request(RREQ) and Route Reply (RREP) control packets. Source sends the selection packet to the participants to inform valid path for this session. The proposed work has been designed to use hello packets to the calculate decision count at every intermediate node to identify the malicious.

Revathi et.al [4] addressed few related works concerned with wormhole attacks. A graph theoretic approach based on adjacency matrix of a network is proposed which easily detects the presence of wormholes in mobile ad hoc network. This approach is advantageous since it does not increase the computation complexity in a mobile node which is resource constrained.

Xu Su and Rajendra V. Boppana [5] proposed NEighbor Verification by Overhearing (NEVO), in which nodes passively monitor (overhear) the forwarding of broadcast type packets by their neighbors and use the send and overhear times of transmissions of these packets, to mitigate these wormhole attacks. NEVO does not require synchronized clocks, special hardware support, or any special capability. NEVO can detect almost all instances of wormhole attacks and is virtually independent of the routing protocol used. NEVO is simple to implement – requires mostly network layer software changes, has low overhead, and is very robust. NEVO is implemented in the Glomosim simulator and its performance is evaluated.

Issa Khalil et.al [6] proposed a protocol called MOBIWORP for mitigating the wormhole attack in mobile multihop ad hoc and sensor networks. It incorporates two protocols SMP and CAP-CV for differing degrees of functionality afforded to a mobile node. They also proposed local and global isolation protocols that will neutralize the capability of the malicious nodes from launching further attacks after detection, whether at the current location or at a new location. They demonstrated the effect of MOBIWORP under different network conditions and mobility patterns using simulations.

S.Sharmila and G.Umamaheswari [7] explored the transmission time based scheme to detect the wormhole attack using AODV routing protocol. The scheme calculates the transmission time of the route request and reply between every successive node in the routing path. The additional control packet is transmitted between the suspected wormholes for further confirmation. The proposed work is able to detect the both the hidden attack and exposed attack.

Pallavi Sharma et.al [8] presented a mechanism which is helpful for detection and defend against wormhole attack in ad hoc network is"multipath hop counting analysis" (MHA) in which accepting all route request at destination node with in a fixed time period called time to live (TTL) period and then verification of digital signature of sending node by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of multipath hop count analysis with verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

Amol A. Bhosle et.al [10]presented a watchdog mechanism and time of flight to detect and overcome black hole attack and wormhole attack and improve the data security in mobile ad-hoc network.This method first detects a black hole attack in the network and then provide a new route to this node. In this, the performance of original AODV and modified AODV in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio. In a wormhole attack, intruders tunnel the data from one end of the network to the other, leading distant network nodes to trust they are neighbor's and making them communicate through the wormhole link.

The paper is organized as follows. The Section 1 describes with overview of MANETs and Wormhole attacks. Section 2 deals with the Related Work. Section 3 is devoted for the implementation of proposed algorithm. Section 5 describes the performance analysis and the last section concludes the work.

III. IMPLEMENTATION OF PROPOSED ALGORITHM

Our proposed wormhole attack detection mechanism involves two phases. In first phase, the worm hole attack is detected and isolated using alternate path discovery. It is based on mobility and the design is carried out in protocol layers. In second work, the data integrity and authenticity can be provided using RSA algorithm.

A. Reliable Routing Protocol for Defending Against Wormhole Attacks

- Source node S sends a message to Destination node D in order to create a shared secret session key for the communication link using RSA algorithm.
- If Source node receives a reply message from Destination node within the Network Cross Time (N_{CT}). It is the maximum expected time in milliseconds waiting for receiving of a Route Reply (RREP) after sending of Route Request (RREQ).
  then
- Source and Destination node D implements the Reverse Shamir Adleman (RSA) algorithm.
- S sends an encrypted with the secure session key message SSK_ERP to the destination using the Advance Encryption Standard (AES) and records the current time t_{erp}.
- D decrypts the SSK_ERP and includes its destination ID number. It encrypts the SSK_ERP using AES and send back to the Source node.
- If Source node S does not receive the SSK_ERP within the Network Cross Time then
- S considers the route R is attacked by wormhole attack.
- S deletes the route R from its routing table.
- Source node S informs the misbeh_ward with the next hop node.
- Exit
- Else
- Stores the receiving time $t_{erp.}$

- S determines the Original Traversal Time (O_{TT}). It is the time from sending of RREQ until the receiving of a RREP.
- If the O_{TT} is less than or equal to Original Threshold Traversal Time (T_{OTT}). It is calculated as the combination of Probability of misbehavior ratio and Packet Loss Rate.
  Packet Loss Ratio is defined as

$$P_{LT}(t_1,t_2) = \frac{\int_{t_1}^{t_2} 1_{\{G(t)=Dl\}} dK(t)}{\int_{t_1}^{t_2} dK(t)} \qquad (1)$$

where K (*t*) is the arrival process for user packets. Here, the denominator represents the number of user packets sent in (t_1, t_2] and the numerator represents the number of lost user Packets.

Probability of Misbehavior ratio is given as

$$\text{Misbehavior Ratio} \quad P_{MR} = \frac{Max(0, P_{LT}) * P_{BP} * P_{LACK}}{P_{TR}} \qquad (2)$$

P_{BP} = Probability of bad packet occurence.

P_{LACK} = Probability of acknowledgement packet lost due to link failure.

P_{TR} = total number of packets received.

- The Route is considered as a Safe Route.
- Exit
- Else
- S considers the route R is attacked by wormhole attack.
- S deletes the route R from its routing table.
- Source node S informs the misbeh_ward with the next hop node.
- end if

B. RSA Algorithm

We use the RSA algorithm [16] for providing the authenticity and integrity to the mobile nodes. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

Step 1. Select two distinct prime numbers *x* and *y*.

- For security purposes, the integers *x* and *y* should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

Step 2. Compute *z* = *xy*.

- z is used as the modulus for both the public and private keys

Step 3. Compute φ(z) = (x – 1)(y – 1), where φ is Euler's totient function.

Step 4. Choose an integer *m* such that 1 < m < φ(z) and greatest common divisor of (m, φ(z)) = 1; i.e., m and φ(z) are co-prime.

- *m* is released as the public key exponent.
- *m* having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65,537. However, small values of *m* have been shown to be less secure in some settings.

Step 5. Determine *d* as:

$$b = m^{-1} \,(\mathrm{mod}\,\varphi(z)) \qquad (3)$$

i.e., *b* is the multiplicative inverse of m mod φ(z).

- This is more clearly stated as solve for b given (bm) mod φ(z) = 1
- This is often computed using the extended Euclidean algorithm.
- z is kept as the private key exponent.

so, b*m= 1 mod φ(*z*) The public key consists of the modulus *z* and the public (or encryption) exponent m. The private key consists of the modulus *z* and the private (or decryption) exponent *b* which must be kept secret. (*x*, y, and φ(*z*) must also be kept secret because they can be used to calculate b.)

V. PERFORMANCE ANALYSIS

Network Simulator tool is used to simulate our proposed algorithm. The version used is 2.34. In this simulation tool, the C++ language is back end language and tool command language (tcl) is front end language. The basic advantage of this tool is more updation compare to Glomosim, JIST and Qualnet etc. In our simulation, 100 mobile nodes move in a 1000 meter x 1000 meter square region for 100 seconds simulation time. All nodes have the same transmission range of 200 meters. The simulated traffic is Constant Bit Rate (CBR) and Poisson traffic. Our simulation settings and parameters are summarized in table 1.

A. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Packet Delivery Ratio: This factor indicates that ratio of number of packets received to the number of packets sent.

Misbehavior Ratio: The number of routing control packets are affected by the wormhole attacks.

End to end Delay: The delay in the packet from source to destination during the transmission.

Overhead: It is the ratio of number of control packets received to the total number of packets being sent.

Table1. Simulation settings and parameters

No. of Nodes	200
Area Size	1200 X 1200
Mac	802.11
Radio Range	250m
Simulation Time	70 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	Dynamic Source Routing
Pause time	5 msec

The simulation results are presented in the next part. We compare our SWDS with the FTD [17] in presence of congestion environment.

Figure 3 shows the results of packet delivery ratio for varying the mobility from 10 to 100. From the results, we can see that SWDS scheme has higher delivery ratio than the FTD because of RSA secure scheme.

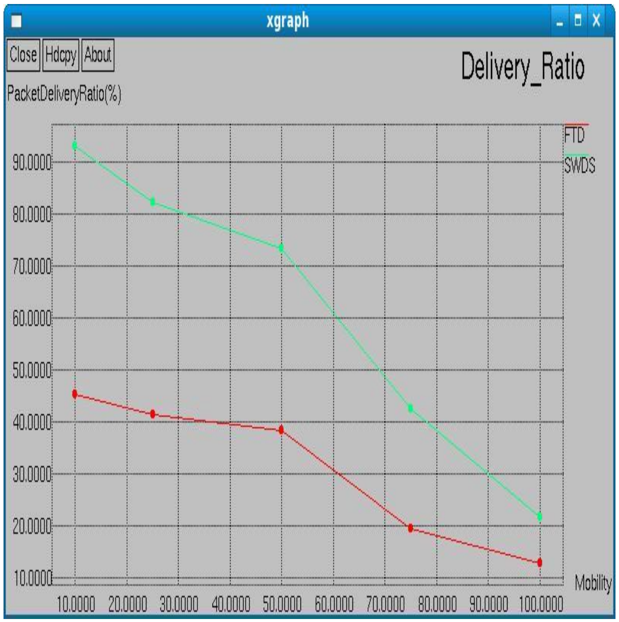

Fig. 3. Mobility Vs Delivery Ratio

Fig. 4, presents the comparison of overhead and throughput. It is clearly shown that the overhead of SWDS has low overhead than the FTP.

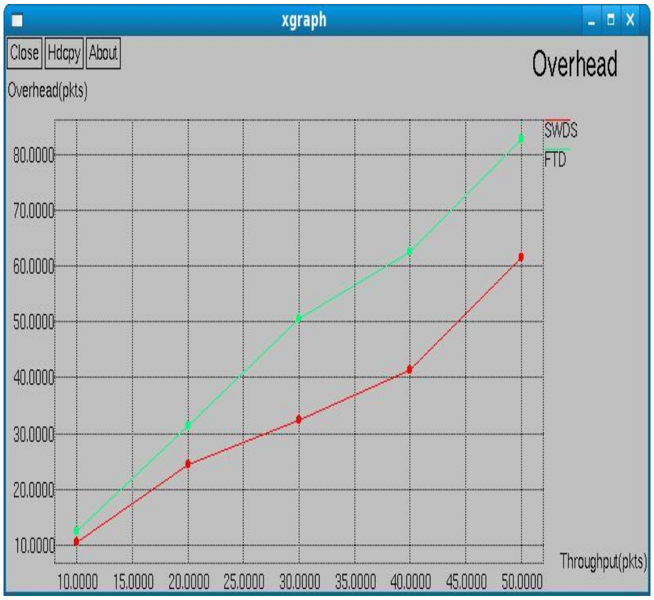

Fig. 4. Throughput Vs Overhead

Figure 5 shows the results of time Vs End to end delay. From the results, we can see that delay of SWDS is lower than the FTD while varying the time from 10 to 100 ms.

Fig. 6, presents the comparison of detection efficiency while varying the number of misbehaving nodes from 20 to 100. It is clearly shown that the detection efficiency of SWDS has relatively high than the FTD.

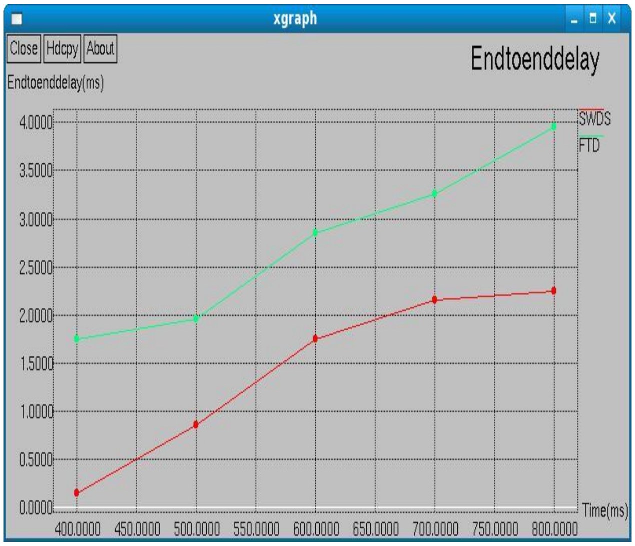

Fig. 5. Time Vs End to End delay

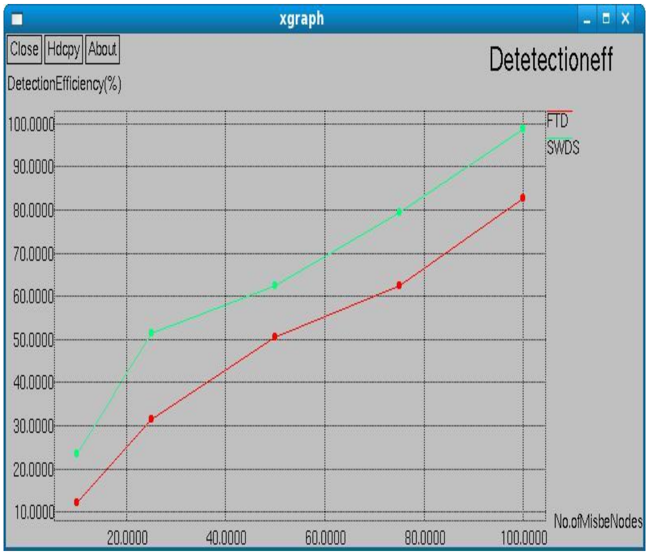

Fig. 6. No. of Misbehaving nodes Vs Detection Efficiency

VI. Conclusion

Due to the presence of attacks in MANET, the nodes are easily impersonated by wormhole attacks. To overcome the issue of wormhole attacks, we propose to design the security enhanced wormhole detection scheme for networks. We achieve the detection of wormhole misbehavior using threshold value of network cross time. In second phase, we have chosen the RSA algorithm to achieve the data integrity. In future, we extend this work to energy consumption model and authentication approach. The Proposed work SWDS achieves the better misbehavior detection efficiency, packet delivery ratio, low delay and overhead than the existing schemes while varying the mobility, time, throughput speed and number of nodes.

References

[1] T. Sakthivel and R. M. Chandrasekaran, "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach", European Journal of Scientific Research, ISSN 1450-216X, Vol.76, No.2, 2012, pp.240-252.

[2] Shalini Jain, Dr.Satbir Jain, "Detection and prevention of wormhole attack in mobile adhoc networks", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010, pp.78-86.

[3] S. Madhavi and K. Duraiswamy, "WAS-DP: Wormhole Attack in SAODV-Detection and Prevention", European Journal of Scientific Research, ISSN 1450-216X, Vol.77, No.4, 2012, pp.560-569.

[4] Revathi Venkataraman, M. Pushpalatha, T. Rama Rao and Rishav Khemka, "A Graph-Theoretic Algorithm for Detection of Multiple Wormhole Attacks in Mobile Ad Hoc Networks", International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009, pp.220-222.

[5] Xu Su, Rajendra V. Boppana, "Mitigating Wormhole Attacks using Passive Monitoring in Mobile Ad Hoc Networks", IEEE Conferences, 2008, pp.1-5.

[6] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks", Ad Hoc Networks, 6, 2008, pp.344–362

[7] S.Sharmila and G.Umamaheswari, " Transmission Time based Detection of Wormhole Attack in Wireless Sensor Networks", Special Issue of International Journal of Computer Applications (0975 – 8887) on
Information Processing and Remote Computing – IPRC, August 2012.

[8] Pallavi Sharma and Prof. Aditya Trivedi, " Prevention of Wormhole Attack in Ad-Hoc Network ",Special Issue of International Journal of Computer Applications (0975 – 8887) on Electronics, Information and Communication Engineering - ICEICE No.5, Dec 2011, pp.13-17.

[9] Weichao Wang, Bharat Bhargava, Yi Lu and Xiaoxin Wu, "Defending against Wormhole Attacks in Mobile Ad Hoc Networks", Wiley Journal Wireless Communications and Mobile Computing (WCMC), 2006.

[10] Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, “Black-Hole and Wormhole Attack in RoutingProtocolAODVinMANET”, International Journal of Computer Science, Engineering and pplications (IJCSEA) Vol.2, No.1, February 2012, pp.45-54.

[11] Shalabh Jain and John S. Baras, “Preventing Wormhole Attacks Using Physical Layer Authentication”, IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks, 2012, pp.2739-2744.

[12] Sana ul Haq and Faisal B. Hussain, “Out-of-band wormhole attack detection in MANETS”, Australian Information Security Management Conference, 2011, pp.87-93.

[13] A.Vani and D.Sreenivasa Rao, “A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks”, International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011, pp.2377-2384.

[14] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni and Ram Pratap, “ Detection of Wormhole Attack using Hop-count and Time delay Analysis”, International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012, pp.1-4.

[15] Mr. Susheel Kumar, Vishal Pahal & Sachin Garg, “Wormhole attack in Mobile Ad Hoc Networks: A Review”, IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No. 2, April 2012, pp.268-275.

[16] http://en.wikipedia.org/wiki/RSA_(algorithm)

[17] Dezun Dong , Mo Li, Yunhao Liu, Xiang-Yang Li & Xiangke Liao , “Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks”,IEEE/ACMTransactionson Networking, Vol.19, Iss.6, pp.1787-1796.

AUTHORS PROFILE

S. Prabu received the B.S.c. degree in computer Science from the Bishop Thorp college, Dharapuram, Bharathiar University ,Coimbatore, India, in Apr 2003, the M.C.A degree in (Computer Application) from the Cherraan’s Arts Science college ,Kangayam, Bharathiar University, Coimbatore, India, in Apr 2006 and the M.Phil degree in Bharathiar University,Bharathiar University, Coimbatore, India, in Nov 2008.His research interests include communication and networks mobile ad-hoc networks, Mobile computing,AI,Network Security . He has about 5 years of teaching experience, since 2007.