A Cryptographic Handshaking Approach to Prevent Wormhole Attack in MANET

Vishal Pahal
Department of Computer Science and Engineering
Jind Institute of Engineering & technology.
Jind, Haryana, India.

Susheel Kumar
Associate Professor
Department of Computer Science and Engineering
Jind Institute of Engineering & technology.
Jind, Haryana, India.

ABSTRACT
A network always suffers from some active or passive attacks. These attacks results the data loss or the information reveal. In case of Dynamic wireless network there are more chances of such kind of attacks. One of such type of attack is Wormhole Attack. It is a tunnel based attack in which a pair of nodes forms a tunnel with false identification. The wormhole attack causes the delay transfer and information steal over the network. In this paper, we have presented the authentication approach to avoid the wormhole attack over the network. In this system we have provided 2 level of authentication using public key cryptography, one level is between node to base station and other between two mobile stations. Further to reduce the security risk from authorized node ,an eligibly test is done ,so that most eligible authorized node is choose for communication. In this work the clustered architecture is presented in which an authenticated tunnel is set between source to base station and base station to destination. The system will minimize the packet loss over the network with authenticity.

General Terms
Security, Algorithms ,Attack on mobile ad-hoc network, diagnosis of attack in mobile ad-hoc network.

Keywords
Wormhole, Authentication, Tunnel, wireless, cryptography

1. INTRODUCTION
Adhoc networks do not rely on any pre-established infrastructure and can therefore be deployed in places wih no infrastructure. .this is useful in disaster recovery situations and places with non-existing or damaged communication infrastructure where people participating in the conference can form a temporary network without engaging the services of pre-existing network.Because nodes are forwarding packets for each other ,some sort of routing protocol is necessary to make the routing decisions. Currently there does not exist any standard for a routing protocol for adhoc networks,instead this is work in ,progress .many problems remain to be solved before any standard can be determined. These research looks at some problems and tries to evaluate some of the currently proposed protocols.

A mobile ad hoc network (MANET) is a collection of mobile computers or devices that cooperatively communicate with each other without any pre-established infrastructures such as a centralized access point. Computing nodes (usually wireless) in an ad hoc network act as routers to deliver messages between nodes that are not within their wireless communication range. Because of this unique capability, mobile ad hoc networks are envisioned in many critical applications (e.g., in battlefields).Therefore, these critical ad hoc networks should be sufficiently protected to achieve confidentiality, integrity, and availability. The dynamic and cooperative nature of MANETs presents substantial challenges in securing these networks. Unlike wired networks which have a higher level of security for gateways and routers, ad hoc networks have the characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration, and highly dependence on inherent node cooperation. As the topology keeping changing, these networks do not have a well-defined boundary, and thus, network-based access control mechanisms such as firewalls are not directly applicable.

Due to the highly dynamic nature of mobile nodes and the absence of a central controller, traditional routing protocols used for a wired network cannot be applied directly to a MANET. Some of the considerations required in the design of MANET [1], [2], [3], routing protocols include the mobility of nodes, unstable channel states and resource constraints such as power and bandwidth. In a MANET, the movement of nodes will cause communication between nodes to be disrupted from frequent path breaks and reconnections. Also, the broadcasting of radio channels can be highly unstable and the network layer has to interact with the MAC layer for available channels. In addition, power availability is often limited since the nodes are connected to batteries.

1.1 Problems with MANET
i). Asymmetric links: Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network

ii). Routing Overhead: In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.

iii). Interference: This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.

iv). Dynamic Topology: Since the topology is not constant; so the mobile node might [4], [5] move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks

1.2 Routing

Because of the fact that it may be necessary to hop several hops (multi-hop) before a packet reaches the destination, a routing protocol is needed. The routing protocol has two main functions, selection of routes for various source-destination pairs and the delivery of messages to their correct destination. The second function is conceptually straightforward using a variety of protocols and data structures (routing tables). This report is focused on selecting and finding routes.

1.3 Security

The dynamic and cooperative nature of MANETs presents substantial challenges in securing these networks. Unlike wired networks which have a higher level of security for gateways and routers, ad hoc networks have the characteristics such as dynamically changing topology, weak physical protection of nodes, the absence of centralized administration, and highly dependence on inherent node cooperation. As the topology keeping changing, these networks do not have a well-defined boundary, and thus, network-based access control mechanisms such as firewalls are not directly applicable. In addition, there is no centralized administration, making bootstrapping of crypto systems very difficult. It is extremely easy for a malicious node to bring down the whole network. As a result, ad hoc networks are vulnerable to various attacks including eavesdropping, spoofing, modification of packets and distributed denial-of-service attacks, WormHole Attack, Rushing Attack, Blackhole Attack. Security services, such as authentication services and access controls, can enhance the security of ad hoc networks. Nevertheless, these preventive mechanisms alone cannot deter all possible attacks (e.g., insider attackers possessing the key). Therefore, it is necessary to have other security mechanisms to deal with misbehaving insider nodes that possess the valid key and access rights. Intrusion detection, which has been successfully used in wired networks to identify attacks, can provide a second line of defense. In particular, intrusion detection and response capability is very important as many of the real ad hoc networks will be deployed in hostile environments in which legitimate nodes could be captured and used by adversaries. Intrusion detection involves the runtime gathering of data from system operation, and the subsequent analysis of the data; the data can be audit logs generated by an operating system or packets "sniffed" from a network. Intrusion detection techniques can be mapped into three concepts: signature-based detection, anomaly detection, and specification-based detection. In signature-based intrusion detection, the data is matched against known attack characteristics, thus limiting the technique largely to known attacks, even excluding variants of known attacks.

In anomaly detection, profiles of normal behavior of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. A training phase in anomaly-based intrusion detection determines characteristics of normal activity; in operation, unknown activity, which is usually statistically significantly different from what was determined to be normal, is flagged as suspicious. Anomaly detection can detect unknown attacks, but often at the price of a high false alarm rate.

In specification-based detection, the correct behaviors of critical objects are manually abstracted and crafted as security specifications, which are compared with the actual behavior of the objects. Intrusions, which usually cause object to behavior in an incorrect manner, can be detected without exact knowledge about them. So far, specification-based detection has been applied to privileged programs, applications, and several network protocols.

1.4 Type of Attacks

Spoofed, Altered, or Replayed Routing Information : This is the most direct attack [6] against a routing protocol. Adversaries may be able to create routing loops, extend or shorten source routes, generate false error messages, partition the network, or increase end-to-end delay latency.

Selective Forwarding : Malicious nodes may refuse to forward certain messages, drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a *black hole* refuses to forward every packet she sees. It is most effective when the attacker is explicitly included on the path of a data flow.

Sinkhole Attacks : Adversary tries to take control of all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole [7] with the adversary at the center. Due to either real or imagine high quality route through compromised node, each neighboring node of the adversary will forward packets destined for a base station through the adversary. Since all packets share the same destination (the only base station), a compromised node needs only to provide a single high quality route to the base station to influence a large number of nodes .

The Sybil Attack : In a Sybil attack, a single node presents multiple identities to other nodes [8] in the network. This type of attack can reduce the effectiveness of fault-tolerant schemes and pose a threat to geographic routing protocols.

Wormholes : In the Wormhole attack, an adversary tunnels messages received one part of the network over a low latency link and replays them in a different part. Wormholes [9] can be used to convince two distant nodes that they are neighbors by relaying packets between the two of them. These attacks can be combined with selective forwarding or eavesdropping.

HELLO Flood Attacks : A laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor. HELLO floods [10] can be considered as one-way broadcast wormholes and uses a single hop broadcast to transmit a message to a large number of nodes unlike the traditional definition of flooding denoting epidemic-like propagation of a message to every node in the network.

2. LITERATURE SURVEY

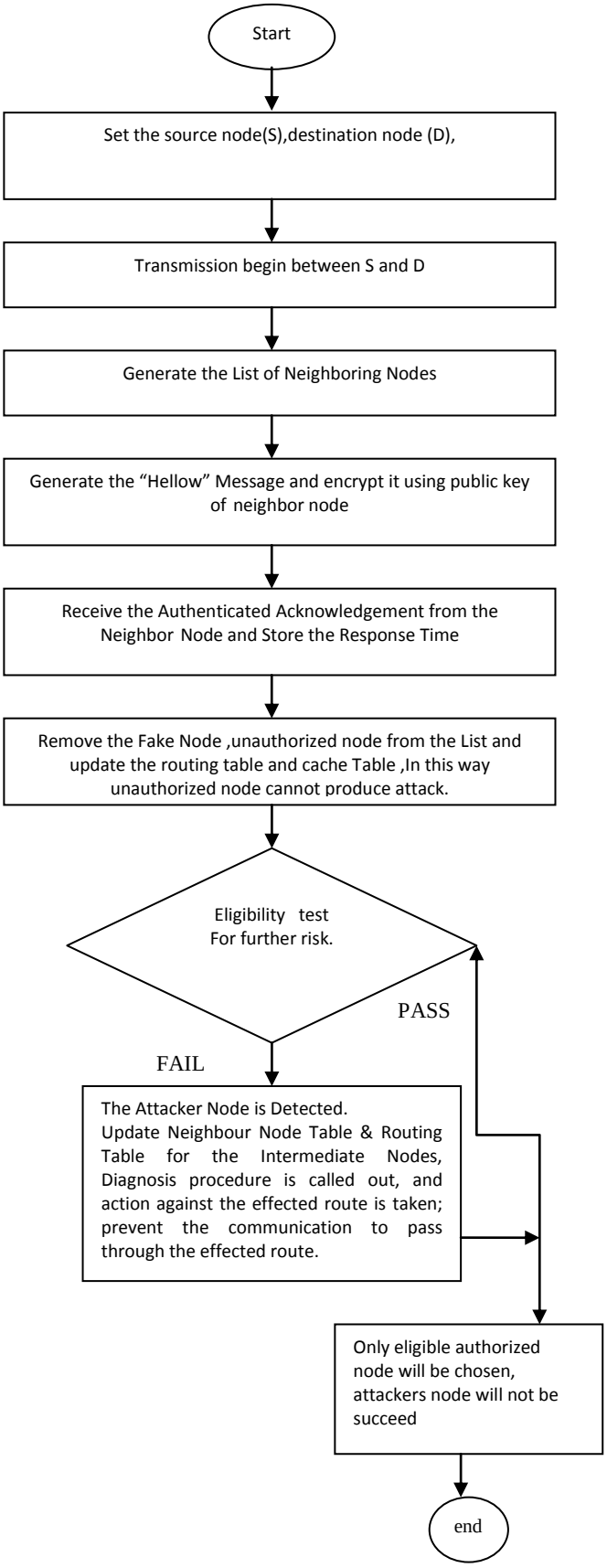
In this section we will give a short overview of existing work and entry points to the literature. Many different types of attacks have been proposed so far. [11] proposes a security solution for manets using a pre-existing routing protocol, ad hoc on-demand vector routing (aodv), using password security for each routing node and timeliness to update routing table. There is a proposed protocol, called SECTOR[12], which relies on a special hardware. The main idea of the proposed protocol is that the distance between two sensor nodes can be measured accurately based on the speed of data transmitted between them. SECTOR does not require any clock synchronization and location information by using mutual authentication with distance bounding (MADB) protocol. This approach [13] is simpler than using location since each node need only maintain a set of its neighboring nodes. A message from a non-neighboring node is ignored by the recipient. Note that any protocol used to maintain accurate

neighbor sets may itself be vulnerable to wormhole attacks, so goal is to design a neighborhood discovery protocol that is not vulnerable to wormhole attacks. The security of our protocol will rely on using directional antennas to obtain relative direction information, and cooperation among nodes to verify possible neighbors. Wireless ad-hoc networks typically assume omni-directional antennas. Here devices are directional antennas. Directional antennas have been shown to improve efficiency and capacity of wireless networks In this approach to detection of wormhole attacks depends on nodes maintaining accurate sets of their neighbors. An attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbor and its messages are ignored. One important property of directional antennas is a node can get approximate direction information based on received signals. The first protocol, directional neighbor discovery, does not rely on any cooperation between nodes, and cannot prevent many wormhole attacks. By sharing information among neighboring nodes, the verified neighbor discovery protocol can prevent wormhole attacks where the attacker controls only two endpoints and the victim nodes are at least two hops distant. Finally, the strict neighbor discovery protocol prevents wormhole attacks even when the victim nodes are nearby.In order to avoid using special hardware, in this approach , there is try to detect wormhole using a so-called Round Trip Time (RTT) between two nodes [14]. A node, say A, calculates the RTT with another node, say B, by sending a message to node B requiring an immediate reply from B. The RTT between A and B is the time between A's sending the request message and receiving the reply message from B. In this mechanism each node (called N) will calculate the RTT between N and all N's neighbors.Because the RTT between two fake neighbors is higher than that between two real neighbors so by comparing these RTTs between A and A's neighbors, node A can identify which neighbors are fake neighbors and which neighbors are real neighbors. The basic theme of their [15] approaches is based on the statistical methodology .To, overcome the failure of hardware and synchronization approaches, there are statistical approaches present . Theses approach is known as SAM (statistical analysis of multi-path). It was proposed to detect exposed [16] wormhole attacks in Multi-path routing protocol. The main idea of the proposed scheme statistical analysis of multi-path is based on the observation that certain statistics of the discovered routes by routing protocols will change dramatically under wormhole attacks. Wormhole attack have a very attractive nature for traffic , most of the time ,node choose the route of wormhole attack , Because wormhole links are extremely attractive to routing requests so it will appear in more routes than normal links. By doing statistics on the relative frequency of each link appear in the set of all obtained routes, it can identify wormhole attacks. This technique is only used to detect exposed attacks. So these is a statistical technique which work on attractive nature of wormhole link , but the main disadvantage of this technique is that if wormhole link does not appears in the route request ,then statistics will not able to detect the most frequent link called wormhole link. In TTM, [17] , to detect wormhole each time a route is requested. There is a two-fold benefit: first, no need to frequently check for wormhole which causes a lot of bandwidth and resource consuming and second, the wormhole will be identified before it can do any harm to the network because wormhole attacks have to interfere in the route setup before they can cause any damage. This mechanism is designed specifically for AODV. The Transmission-based Time Mechanism (TTM), where every Round Trip Time is calculated between two successive nodes in the whole route. The RTT can be calculated by excluding the RREQ time from the RREP time. The approach [18] is based on the observation that the network with malicious nodes has different visualization from that with normal nodes. The layout of the network can be reconstructed and visualized. The wormhole attack can be detected by visualizing the anomalies introduced by the attack. If wormhole attackers exist, the shape of the constructed network layout will show some bent/distorted features and detects the wormhole by visualizing the anomalies introduced by the attack In [19] proposed a wormhole detection protocols that use only connectivity information in the connectivity graph. In the proposed approaches are localized and do not use any special hardware or location information for attack detection. The detection algorithm looks for 'forbidden substructures' in the connectivity graph that should not be present in a legal connectivity graph. They use unit desk graph (UDG) model that have long been used to create an idealized model of multi-hop wireless networks. They run an extra search procedure to determine a critical parameter for the detection algorithm. However, these topology-based approaches alone cannot detect all wormhole attacks in the network. Instead of detecting wormholes from the role of administrators as in previous methods, a new protocol, MHA, using a hop-count analysis from the viewpoint of users without any special environment assumptions.MHA [20] showing the advantages over the previous works which require the role of administrator and their reliance on impractical assumptions.. This method provides good performance for avoiding wormhole attacks, but there could be some attacks anticipating MHA.

3. PROPOSED WORK

The objective of the work is to improve routing by removing misbehaving and selfish nodes thereby increasing the security and improving the performance of Network. In order to achieve the above security goal, the misbehaving nodes and the selfish nodes are to be identified and then their presence in the tree must be made insignificant as to improve security and performance. This is made possible either by pruning away the node or by not routing any packets through that node and finding alternate ways for the child nodes of that "misbehaving nodes". The proposed work is about detection of worm hole attack between the communication taken place between the source and the destination. Our proposed scheme does not require any special hardware [12] ,[13]. Technique [14] is not able to detect the exposed attack. The approach in [15] is unable to detect hidden attacks because in this kind of attack wormhole links does not appear in obtained routes. Location information and shows high detection rate under various scenarios, but our proposed approach can also find hidden and exposed attack. Approach in [16] required some of statistics collection, in [17] require Time synchronization. Our proposed Approach does not depend upon statistics and time synchronization. In case of mobile nodes, visualization approach [18],connectivity based approaches in [19] is difficult to apply and will be insufficent.So in our proposed scheme, we do not apply the visualization and connectivity technique because of mobility of nodes. Attackers may add fake nodes to an intermediate list so the route has a longer distance to save it from get catch , so it can create a problem in approach [20].Our proposed approach try to solve all such issues.

3.1 Flowchart Diagram



3.2 Algorithm

WormHole (S,D)
/* S is the source node and D represents the Destination Node over the network*/
{
Step 1: As transmission begin it will seach for all the intermidate nodes called Neighbour List
Step 2: Generate and Authenticated "Hellow" Message by current Node and encrypt it by the public key of neighbouring nodes and Distribute it to specific neighbouring nodes
Step 3: if x is in NeighbouringList
{
If (PrivateKey(EncryptedMessage)=="Hellow")
{
Print Node is authenticated and Continue the process
}
Else
{
(i) Remove the node from NeighbourList
(ii) Update Cache Table and Report Node x is Block Node
}
}
Step 4. If node x is authenticated it will send the Node information with "reply" message as piggy begging. In this way no unauthorized node can participate in the communication and perform attack. but still after authentication, a further check is done for more eligible authorized node so that it will prevent any security risk .
Step 5: Collect the list of all valid neighbouring node and transfer data to most eligible next node

(i) Eligibility Depends on Distance and Direction
(ii) Also consider the load to decide the Eligibility
(iii) Record the response time node.
(iv) Check for transmission link of nodes.

Step 6. Estimate the Number of packet received and Response time of Reply message and compare it message reply time in case of forwarding message

If No. Packets Recevied<Expected Threshold received
then check for link used

If ResponseTime>Threshold(Response Time)
then check for link used.

Step 7 It check for the link for neighbor table , if it contain too high bandwidth
if lossy link>Expected/Threshold link
Then
that link will be declared as unexpected link .
Follow the following steps :
The Worm hole attack is observed , so
Update Neighbour Node Table & Routing Table for the Intermediate Nodes
Step :8 Such node which get fail in eligibility test ,would not be chosen for communication. the unresponsive node is incapable of responding to the probe message.
Step 9. The diagnosis algorithm will then be called to decide which one is the case. These will provide provide a two way security, no unauthorized node can take participate without authentication , and even after authentication it have to pass eligiblity test , if it get fail in eligibility test :

Then it will be excluded from participation list, hence network is prevented from wormhole attack.
Step 10, The Process from Node one is repeat for each intermediate node till the destination is not arrived and before the actual communication take place.
}

As , we know the wormhole attack have very bad impact on the network performance , it degrade the network performance , so prevention of wormhole attack is one of the major issue in the wireless network .Our proposed method is also giving a prevention scheme against wormhole attack. A flowchart is a type of diagram that represents an algorithm or process, showing the steps as boxes of various kinds, and their order by connecting these with arrows. This diagrammatic representation can give a step-by-step representation of our algorithm so , here we represent our algorithm in the form of a flowchart.
In this work a authentication system is presented here to detect and resolve the problem of wormhole attack. In this work each node is defined as an intelligent node that having the cryptographic algorithm implementation on it. As node starts communication it generates the neighbor nodes list and find the nearest neighbor. It generates a "hellow" message and encrypt it by using the public key of the neighboring node, After the encryption it pass the message to the neighboring nodes. As the neighboring node receives the message it will perform the decryption using its own private key and then send the acknowledgement to the sender node back. If the neighbor node is not authenticated it will remove its entry from the routing table and continue its work after updating of cache table. Immediately , it will transfer data to its most eligible next node. To check the eligibility of authenticated node it will also observe some other factors like load on the node response time etc. As the node reply it check if the response time is greater then its estimated response time then it will again exclude that particular node from the list.A check for link of node is also done , which can also help in detection of getting unexpected link's in the network. So such algorithm will provide a true decision making step for authentication ,detection and prevention of wormhole attack. The complete process is repeated node by node till the destination node is not achieved. In this way it provides security from unauthorized node , it does not allow any unauthorized node to participate in the network so that no malicious node can introduce itself in the network and further there is a eligibility test which can further reduce risk from authorized node ,only eligible authorized node can participate in communication .In this way it provide a prevention method of wormhole link attack ,hence provide a secure communication way in the network.

4. RESULTS

The proposed system is implemented in NS2 environment. DYMOM routing protocol is used to implement the algorithm. Here the basic parameters of the proposed work are presented respective to the simulation environment in table 1

Table1: Simulation Parameters

Parameters	**Values**
Number of Nodes	50
Topography Dimension	670 m x 670 m
Traffic Type	CBR
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Packet Size	512 bytes
Mobility Model	Random Way Point
Antenna Type	Omni directional
Protocol	DYMOUM

As in figure 1 show that the complete work is divided in 5 clusters. Each cluster is having 10 nodes. Each cluster having a base station. The base station here is presented in blue colour and black nodes represents and mobile stations. As the transmission each node generates a public and private key pair and shares it with neighbouring nodes. In this way before communication, an authentication process ,eligibility test and diagnosis action are done to prevent the network from the wormhole link .

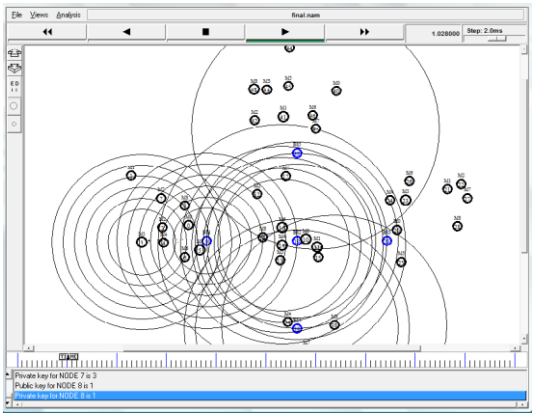


Figure 1 : NS2 Simulation

The final work is presented in the form of graph where the number of packet received, Delay time, loss packets is being compared using Graphs. The results are here presented in Figure2, Figure3 Figure 4 .In this figures the comparison between the secure network with proposed approach and wormhole affected network is done. Red color graph defines the system with wormhole attack and Proposed is the solution with authentication system is shown by blue color graph. In this figure2 the no. of Packet received is presented. As we can see the number of packet received is increased after the implementation of algorithm in the network .Figure 2 show the number of packets received corresponding to the simulation time , we can also conclude that there is great loss of packet in wormhole containing link, Figure 3 shows percentage of number of packets loss with simulation time in wormhole affected network.

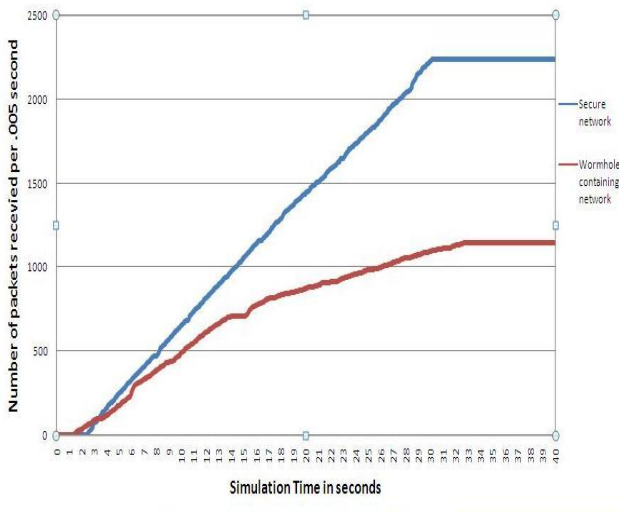


Figure 2: Comparison of number of packet recevied

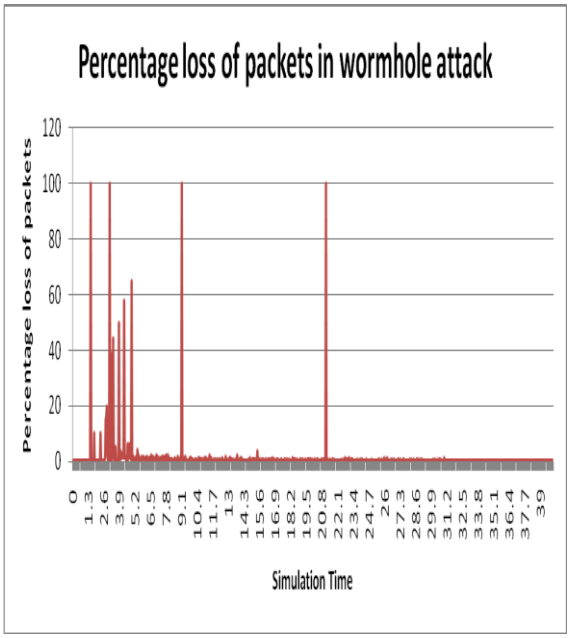


Figure 3: Percentage loss of packets in wormhole link

In the figure 4 , a comparison of total delay time is done, there always some delay in network because of traffic load , but here total delay time increase when the wormhole link is present in the network.

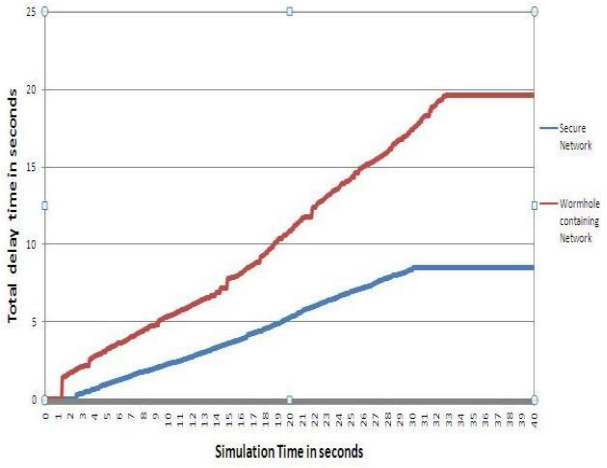


Figure 4: Comparison Of Total Delay Time

5. CONCLUSION

In the proposed system, data communication will be based on authentication ,because of this it will always provide the reliable communication over the network. But still there can be risk in the authorized system, so to overcome the risk of attack, further an eligibility test is performed before the actual communication take place .In this way the proposed scheme provide security from the unauthorized nodes, no unauthorized node can start communication, it have to complete the authentication first, after that it have to pass the eligibility test . When the system passes the test , then it is reliable to communicate and free from attack ,if it fail then diagnosis procedure is called out ,which will take action against the attack ,and prevent the communication to pass through the effected path. In this way prevention against the wornhole attack is done before the actual communication take place.The system is providing better throughput and less packet loss over the network as compare to network contain wormhole link.

6. REFERENCES

[1] Ephremides, Wieselthier, J. E. and Baker D. J., "A design concept for reliable mobile radio networks with frequency hopping signaling," Proc. IEEE, vol. 75, no. 1, January 1987, pp. 56-73.

[2] Bhatnagar, A. and Robertazzi, T. G., "Layer net: a new self-organizing network protocol," Proc IEEE Milcom'90, vol. 2, 30 September- 3 October 1990, pp. 845-849, 30.

[3] Alwan, A., Bagrodia, R. and Bambos, N. et al., "Adaptive mobile multimedia networks," IEEE Personal Commun, vol. 3, no. 2, April 1996, pp. 34-51.

[4] Liu, K., Deng, J., Varshney, P. K. and Balakrishnan, K. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," IEEE Transaction on Mobile Computing, vol. 6, no. 5, May 2007, pp 536-550.

[5] Papadimitratos, P. and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," Proc. IEEE Workshop on Security and Assurance in Ad Hoc Networks 2003, IEEE Press, pp. 27–31.

[6] Karlof, C. and Wagner, D. " Secure routing in wireless sensor networks: attacks and countermeasures,"

Elsevier's AdHoc Networks Journal, vol. 1, no. 2-3, September 2003, pp. 293-315,.

[7] Yang, C. L., Tarng, W., Hsieh, K. R. and Chen, M. "A security mechanism for clustered wireless sensor networks based on elliptic curve cryptography," IEEE SMC eNewsletter, Issue 33, December 2010.

[8] John, R. D., "The sybil attack," Revised Papers from the First International Workshop on Peer-to-Peer Systems: IPTPS 2002, vol. 2429 of LNCS, pp. 251—260.

[9] Kumar, S., Pahal, V. and Garg, S. ,"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.

[10] Hamid, A. and Hong, S., "Defense against Lap-top Class Attacker in Wireless Sensor Network," 8th International conference on advance communication technology, ICACT , vol 1, 2006, pp. 318-323.

[11] Deswal, S. and Singh, S., "Implementation of Routing Security Aspects in AODV", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February 2010.

[12] Capkun, S., Buttyan, L. and Hubaux, J. P., "SECTOR: Secure tracking of node encounters in multi-hop wireless networks," Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks (SASN 03), October 2003, pp.21−32.

[13] Hu, L. and Evans, D. "Using directional antennas to prevent wormhole attacks," in Proceedings of 11th Network and Distributed System Security Symposium, NDSS' 04, San diego, February 2004, pp. 131−41..

[14] Zhen, J. and Srinivas, S. "Preventing replay attacks for secure routing in ad hoc networks," Proc. of 2nd Ad Hoc Networks & Wireless (ADHOCNOW' 03), 2003, pp. 140--150.

[15] Buttyan, L., Dora, L. and Vajda, I., "Statistical wormhole detection in sensor networks," Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2005) Visegrad, Hungary, July 13-14, 2005, pp. 128-141.

[16] Qian, L., Song, N. and Li, X., "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path," Wireless Communications and Networking Conference 2005, IEEE, vol. 4, pp. 2106-2111,

[17] Phuong, T. V., Canh, N. T., Lee, Y. K., Lee, S. and Lee, H, "Transmission time-based mechanism to detect wormhole attacks," IEEE Computer society, 2007, pp. 172-178.

[18] Wang, W. and Bhargava, B., "Visualization of wormholes in sensor networks," Proceedings of the 2004 ACM workshop on Wireless security. ACM Press, 2004, pp. 51−60.

[19] Maheshwari, R., Gao, J. and Das, S. R., "Detecting wormhole attacks in wireless networks using connectivity information," Proc. of IEEE International Conference on Computer Communication, May 2007, pp. 107−15.

[20] Jen, S. M., Laih, C. S. and Kuo, W. C., "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET ," Sensors, vol. 9, 2009, pp. 5022-5039.