IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.
www.ijiset.com
ISSN 2348 - 7968

Detection of Wormhole Attack Using USOR

Sathish kumar.R[1], Mohamed Ismail.K[2]

[1] **Shivani Engineering College, Trichy, Tamillnadu, India**

[2] **Shivani Engineering Colleges, Trichy, Tamillnadu, India**

Abstract: Mobile Ad hoc Networks are infrastructure less networks and this kind of networks are more vulnerable to different types of attacks. There are several number of schemes proposed for providing security and protect against various attacks. The wormhole attack also affects the routing at various levels because it is more dangerous to different routing protocols. Our approach for wormhole detection enables the receiver to detect wormhole nodes using unobservable routing .We proposed an efficient method to identify the wormhole nodes exists in the routing path and rediscover new routes from the source node to target node . By applying an improved hop count based detection checking its one hop neighbors from its neighbor table. Once the wormhole nodes are detected then remove the wormhole entries from its neighbor table. We also improve the simulation results with the help of ns2.

Keywords: Mobile Ad-Hoc Network, Routing, Security, Wormhole Attack

I. Introduction

MANETs are group of mobile nodes communicate with each other without having a fixed infrastructure. These networks mostly suffer from different kinds of attacks. This is caused due to the mobility of nodes are always dynamic in nature. They are characterized by changing topology caused by the mobility of nodes or by nodes leaving and joining with the network. Because of the dynamic nature of the mobile nodes, routing plays an important role in communication. In such networks mobile nodes communicating with each other in a muti-hop fashion and each device in a MANETs is free to move independently in any direction and changes its links to other devices frequently.

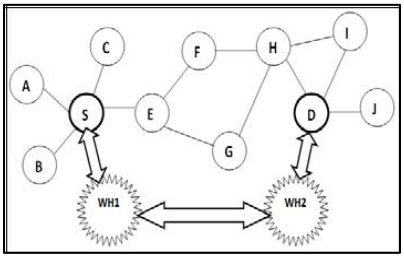

Fig.1 Wormhole Attack

1 creates a tunnel and captures the routing message from source and forwards them through a secret tunnel. In wormhole attack, an attacker records a packet at one location and tunnels them into another location and retransmits them into the network. The attacker receives data packets from the source node and forwards them to another malicious node, thereby utilizing the network resources and spreading fake information about routes in the network [8]. The wormhole attacker simply drops the packets or it can forward the packets so that it cannot be easily detected.

The wormhole attack usually occurs at the network layer and affects the routing path in ad hoc networks. The unobservable routing protocol helps to identify the wormhole nodes during data transmission. Most of the routing protocols failed to detect wormhole nodes because the adversaries can monitor the sender and receiver [10]. It also knows the source id and the target id. But in the unobservable routing protocol the anonymity is set between the each and every node. The adversary cannot find the source id and target id. The packets are indistinguishable from other packets to outside adversaries. The information about the data packets like packet header are also protected from an attacker. Because the adversary is able to compromising nodes to achieve such kind of attacks.

Ad-Hoc networks are vulnerable to different types of attacks includes spoofing, modification of packet, black hole attack, distributed DoS attack, Sybil attack and rushing attack. The security of our routing protocol relies on using directional antennas to obtain relative direction information, and cooperation among nodes to verify possible neighbors. The objective of our routing scheme improves the performance of simulation parameters thereby removing the wormhole nodes.

1.1Problem Statement

The security is an important issue in wireless networks because there are several kinds of attacks also affects routing at different layers. This paper focuses on detection of most dangerous attack; wormhole attack creates a tunnel between the sender and the receiver. This type of attacks mostly occurs in ad hoc networks.

ISSN 2348 - 7968

The existing routing protocols are not efficient to detect wormhole attack. Most of the routing protocols depend on public key cryptography which results in high computation overhead. The attacker generates the traffic through the wormhole nodes. It may also perform dropping data packets and modification of packets. Our routing protocol also satisfies stronger privacy protection than any other anonymous on demand routing protocols such as MASK [12] and ALARM [3]. The main objective of this project describes the process of detection and removal of wormhole attack using an unobservable routing protocol.

2. Related Work

Hu et al.[13] proposed an approach namely packet leashes to protect against wormhole attack. In these attack two kinds of leash information was used. They are Geographical leash and temporal leash. In geographic leashes every node in the network must know its exact location information and also performs loose clock synchronization. In temporal leashes, each node must have its accurate clock synchronization. The geographical leashes are less efficient because it requires broadcast authentication. The main advantage of geographical leashes is that it has to predict the location of each and every node with accuracy. The advantage is that geographical leashes used in conjunction with a signature scheme. The temporal leashes [13] limit the range of packet using the time it remains valid. This method always based on time and each node must have accurate clock synchronization. Every packet should be delivered to the next node within computed life time of a packet. If the life time expires then assume that the path has a wormhole.

Su et al. [9] introduced a method called WARP, Which is a modified version of AODV routing protocol used to defend against wormhole attack. By using this approach the wormhole nodes are isolated by adopting link disjoint multipath routing takes place between the source and destination. WARP enables the one hop neighbour to trace the wormhole nodes during route discovery. It also discovers the abnormal routes from the source to destination.

Gupta et al. [10] proposed an attack detection protocol WHOP using hound packet. By using this approach a hound packet will be send to every node after the process of route discovery using AODV protocol. The hound packets are processed by every node except the nodes that are involved in the route. WHOP modifies the packet structure of RREP by hiding the information of the source node forms the route and communicates with the destination node. To identify the wormhole attack in the route sender node creates the hound packet. Each node will cache the hound packet for threshold time, the destination node detect wormhole in the route if exists within the scheduled time.

3. Proposed Routing Algorithm

The proposed algorithm consists of three parts. The first part describes Key generation and key exchange. The second part describes route discovery in detail. The third part illustrates the concept of wormhole detection and elimination.

3.1 Key Establishment

In this phase anonymous key establishment is employed by each and every node anonymously constructs a set of secret session keys with each of its neighbors. After the construction of session keys two nodes exchange their session keys without knowing the sender and receiver. In mobile ad hoc networks every node communicates directly with its neighbors within its radio range for anonymous key establishment. In this routing protocol the group signature is implemented for anonymous key exchange. The key server generates a group public key gpk which is publicly known by everyone, and a private group signature key gsk for every node. The group signature scheme ensures full anonymity which means a signature does not reveals the signers identity but everyone can verify its validity.

3.2 Route Discovery

The route discovery process can be initiated by the source node to discover a route to the destination node. In this process each node except the source node and the destination node needs one ID based decryption. The route discovery process also comprises of route request and route reply. The route request messages can be flood throughout the whole network, and then the corresponding route reply messages are sent backward to the source node only. Each node maintains a routing table, and updates the content while receiving a routing message. When a originator needs to send data to a destination, if in the originator's routing table, the path toward the destination is out of date, or there is simply no path toward the destination, the originator would broadcast an RREQ to all nodes.

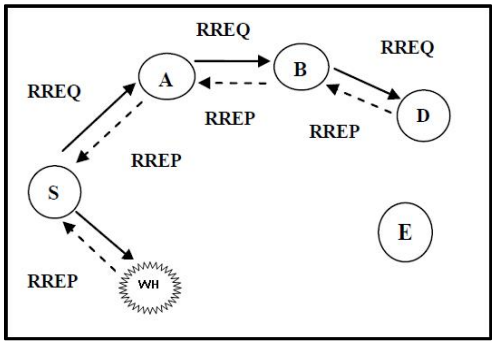

Fig.2 Route Discovery Process

The sender broadcasts the route request initially and

ISSN 2348 - 7968

hence the RREQ message is broadcasted to all other nodes. The node which decrypts the message with its own session key constructed in the earlier phase. It is widely used to authenticate the neighbors with a valid session key. After receiving the RREQ message then the receiver sends the route reply to the source node. The secure route is constructed between the source the destination.

3.3 Hop count Based Detection

This part includes one hop neighbor discovery, hop count calculation and comparison finally detection and removal of wormhole nodes during data transmission. Initially the sender starts discovering its one hop neighbors. Each node sends a hello message for discovering its neighbors. If a node receives a hello message then immediately sends a reply. Each node updates its neighbor id from the neighbor table. Each node compares its neighbor list with its neighbor's neighbor list. The sender checks the corresponding routes to the destination using its one hop neighbors. After identifying one hop neighbors, it will find the target hop count value by checking its target node entry in the routing table. The hop count value is calculated and it is compared with the target hop count, if it is lesser then the sender will assume that the target node and previous one hop neighbors are wormhole nodes.

3.4 Wormhole Elimination

Once the wormhole nodes are identified by using this approach, the sender sends worm announcement messages to all nodes. Any node receives the worm announcement message then it removes the wormhole node id from its neighbor table and its routing table. If any forwarding node receives the worm announcement message it will send RERR message to the source. It will reinitiate the Route discovery process and finds the new routing path to the destination without wormhole node.

4. Implementation and Performance Evaluation

An implementation has been done using NS2. We have deployed 10 nodes participating in this network. The data packets are transmitted within the given range. The behavior of wormhole is analyzed among 10 nodes and also improves the performance in terms of packet delivery ratio. We describe the implementation of wormhole detection and performance evaluation of the unobservable routing protocol.

We deployed the 10 mobile nodes are randomly distributed in 200m x 100m area with the transmission range of 250m.
The packets are transferred with the actual data rate. We evaluate the performance in terms of simulation parameters such as packet delivery ratio, No. of packets send, No. of packets received, throughput and control overhead. The simulation results or outputs will be plotted using the graph. The hop count based detection helps to trace the wormhole nodes. The wormhole nodes are placed near the source and destination and perform packet dropping within a short distance. For example the wormhole attack is achieved by an attacker with the minimum of 2 hops. The packet delivery ratio also improved by removing the wormhole nodes after the process of identifying one hop neighbors.

5. Simulation Results

In our simulation, ad hoc networks are deployed as shown in fig.4. The process of key generation and key exchange as shown in fig. 3 can also be implemented by using group signature. During data transmission the wormhole nodes are detected by analyzing their behavior. As shown in Table 1, our proposed wormhole detection scenario is created with the simulation parameters. There are different evaluation metrics are used.
They are:

1. Packet Delivery Ratio: The ratio of the total number of data packets sent to the receiver to the total number of data packets received by the receivers.
2. End-to-end delay: It represents time gap between the times of packet to the source to the time up to the last bit arrival of the packet to the target.
3. Control Overhead: It gives the ratio of total number of the control packets transmitted by the sender to the number of data packets will be delivered to the receivers.

The following table 1 shows the list of simulation parameters

Parameter	Value
Number of Nodes	10
Wormhole Nodes	2
Routing Protocol	USOR
Simulation Time	300s
Packet size	512bytes
Transmission area	100m by 100m
Traffic type	CBR
Antenna type	Omni Directional
Transmission range	250m
Simulation area	200m x 100m

Table 1: Simulation Parameters

The wormhole attack detection scenario is shown in the fig. 4.

It illustrates detection of wormhole nodes as node 1 and

ISSN 2348 - 7968

node 8. The two nodes are located near the source and the destination. We analyzed the performance of the USOR routing protocol and prevents wormhole attack to improve the packet delivery ratio.

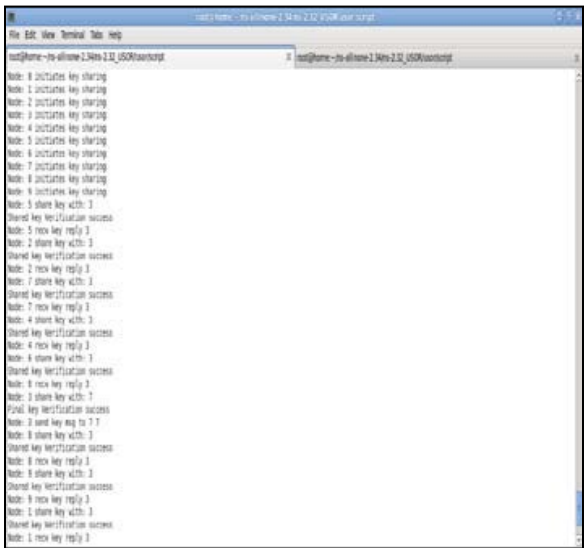

Fig.3 Key Generations and Key Sharing

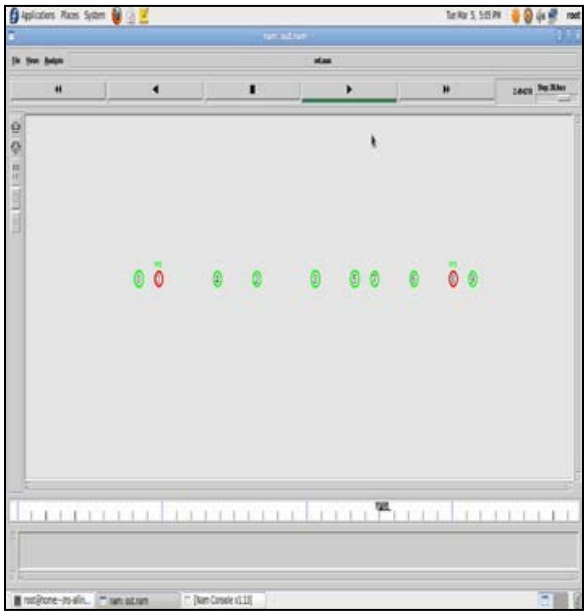

Fig.4 Wormhole Detection

6. Conclusion

In this paper, we focused on detection and removal of wormhole attack during data transmission. We proposed an unobservable routing scheme USOR to provide unobservable for every node. The hop count based wormhole detection also helps to detect wormhole nodes launched by an attacker. The USOR provides more security to hoc networks and also prevent from such kind of attacks. It helps to increases the packet delivery ratio and reduces the control overhead by improving the performance of the routing protocol. We evaluate the performance of USOR and detection of wormhole in terms of packet delivery ratio. In future we also improve the security of wireless ad hoc networks by deploying such efficient methods to prevent DoS attacks and hybrid attacks with the help of USOR routing scheme.

Acknowledgment

I would like to thank the reviewers for their constructive comments that helped to improve the quality of this work.

References

[1] Bo Zhu, Zhiguo Wan,Feng Bao,Robert H.Deng, Mohan S.Kankanhalli,“Anonymous secure routing in mobile ad-hoc networks” in Proc.IEEE Conference on Local Computer Networks, pp. 102-108, 2004.

[2] Boukerche A,El-Khatib K,Xu L, Korba L,“SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks”, In Proc. IEEE LCN, pp. 618-624, 2004.

[3] Defrawy K.E, G.Tsudik,“ALARM: Anonymous location-aided routing in suspicious MANETs”, IEEE Trans. Mobile Comp. Vol. 10, No. 9, pp. 1345-1358, 2011.

[4] Denh Sy, Rex Chen, Lichun Bao,“ODAR: On-demand anonymous routing in Ad-Hoc networks”, In IEEE Conference on Mobile Ad-hoc and Sensor Systems, 2006.

[5] Divya Sai Keerthi T, Palappa Venkatraman,“Locating the Attacker of wormhole attack by using the Honeypot”, In Proceedings of the 11th international conference on Trust, Security and privacy in computing and communications. IEEE, Vol. 978, pp. 7695-4745, 2012.

[6] Karim El Defrawy, Gene Tsudik,“Privacy preserving location based on-demand routing in MANETs”, IEEE J.Sel. Areas Communication, Vol. 29, No. 10, pp. 1926-1934, 2011.

[7] Kong J, Kong X,“ANODR: Anonymous on demand routing with untraceable routes for mobile Ad-Hoc networks”, In Proceedings of ACM MOBI-HOC’03, pp. 291-302, 2003.

[8] Lijun Qian Ning Song, Xiangfang,“Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach”, Journal of network and computer applications, Vol. 30, pp. 308-330, 2007.

[9] Ming-Yang Su,“WARP: A Wormhole avoidance routing protocol by anomaly detection in mobile Ad-Hoc networks”, Journal of computers and Security, Vol. 29 pp. 208-224, 2010.

[10] Saurabh Gupta, Subrat Kar, Dharmaraja,“WHOP: Wormhole attack detection protocol using Hound packet”, In Proceedings of the international conference on Innovations in information Tech, IEEE Vol. 978, No. 1 pp. 4577-0314.

[11] Stefaan Seys, Bart Preneel,“ARM: Anonymous routing protocol for mobile ad hoc networks”, Int. J.Wire. Mob. Comput., Vol. 3, No. 3, pp. 145-155, 2009.

[12] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, “MASK: Anonymous on demand routing in mobile ad hoc networks”, IEEE Trans. Wireless Commun., Vol. 5, No. 9, 2006.

[13] Yih Chun Hu, Adrian Perrig and David B.Johnson “Packet Leashes: A Defense against Wormhole Attacks in Wireless networks”, In Proc of international conferene on IEEE computer and communications, Vol. 3, pp. 1976-1986, 2003.

[14] Zhang Y, Liu W, Lou W,“Anonymous communications in mobile Ad-Hoc networks”, In IEEE INFOCOM, 2005.