Journal of Theoretical and Applied Information Technology
20th September 2013. Vol. 55 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PREVENTION OF WORM HOLE AND BLACK HOLE ATTACKS IN SECURE VBOR FOR MOBILE AD HOC NETWORKS

[1]T. PEER MEERA LABBAI, [2]V. RAJAMANI
[1]Department of CSE, SRM University, Kattankulathur, Chennai, Tamilnadu, India
[2]Department of ECE, Indra Ganesan College of Engg., Manikandam, Tiruchirappalli, Tamilnadu, India
Email:[1] peermeera69@yahoo.co.in ,[2] rajavmani@gmail.com

ABSTRACT

In Mobile ad hoc networks, security is the main among the challenges to be considered. There are various types of attacks such as passive attacks and active attacks. Active attacks are more harmful than passive attacks. Some of the active attacks are more dangerous in mobile ad hoc networks since there is no central authority in MANETs. Examples of these attacks are: Worm hole attack, Black hole attack and Distributed Denial of Service (DDoS) attack and etc., In this paper, Secure VBOR is taken as our base paper. In Secure VBOR, groups are formed based on the residual energy of the node. Then the keys are exchanged among the user inside the group. Gateway members are playing the main role in group formation and preventing these attacks.

Keywords: *MANET, Wormhole Attack, Blackhole Attack, VBOR, Energy Consumption, Delivery Ratio*.

1. INTRODUCTION:

As we increasingly rely on information systems, computers and networks, to support critical operations in telecommunication, banking, electronic commerce, defense and other systems. Intrusions present serious obstacles and threats on the deployment of various computing systems and networks. Undoubtedly, if the next generation of network technology is to operate beyond the levels of current networks, security is one of the main concerns and issues to be addressed. Up to now, various solutions for data protection during transmission have been proposed and applied in a hierarchical manner. For example, at the application layer the information may be protected by authentication protocols, digital signatures and encryption techniques [1]. There are also many techniques that can be used to intercept information during data transfer, to generate and inject known and novel attacks and anomalies in the network.

In wireless networks, nodes have limited resources and battery and forwarding data is resource consuming. Thus, a node may not be spending its resources to forward data for other nodes. Some of other protocols assume that nodes are malicious and they will destroy the network and damage other nodes as in Ariadne [2] and SAR [3]. Malicious nodes falsify packets of other nodes. With these selfish and malicious behaviors the wireless network would not work properly.

Attacks on the Internet can lead to enormous destruction [4], since different infrastructure components of Internet have implicit or explicit relationships with each other. Furthermore the performances of various classes of traffic in Internet are strongly correlated, and therefore the performance degradation in one class due to an attack, may impact negatively the performances of other services as well, therefore leading to several anomalies. There are several types of attacks in the Internet that may range from information leakage, to routing table poisoning attacks, to packet mistreatment, to Denial-of-Service (DoS), etc.[5]. Some of these attacks may affect a single user, while others may affect the performance of a large group of users or classes of service. In this paper, we mainly emphasize on the detection of attacks and/or intrusions that fall in the latter category, since in general they present an impact on the performance of the whole network, or of a significant part of it. Such an attack for instance is the DoS attack. These attacks become extremely dangerous and very hard to prevent, especially when a group of attackers coordinate in DoS [5, 6]. In addition to intentional direct DoS attacks against specific servers or hosts, it should also be noted that several other attacks against the transmission infrastructure, such as routing table poisoning and packet mistreatment, may result in massive DoS attacks against entire groups or whole portions of the Internet. In recent years all the attacks have been significantly gaining in sophistication and power to harm. Attacks are increasingly automated, so that now the attack tools may initiate new attack cycles by themselves, with no person involved. Distributed attack tools are capable of coordinating use of numerous attack platforms and scripts spread out through the Internet, thus launching truly devastating DoS attacks. Moreover the attack methods seem increasingly capable of considerable stealth that aims to evade recognition of their characteristic signature. As part of this masking strategy, they often use dynamic variation of methods and activities with pre-determined or random patterns.

Furthermore, in Ad hoc networks exists a strong motivation for non-participation in the routing system. Both the routing system and the forwarding of foreign packets consume a node's battery power, CPU time, and bandwidth, which are restricted in mobile devices. Consequently, selfish nodes [7] may want to save their resources for own use. There are three main causes for a node not to work according to the common routing protocol: Selfish nodes try to save their own resources, as described above. Malicious nodes are trying to sabotage other nodes or even the whole network, or compromise security in some way. In our proposed approach, we are providing the prevention method for preventing blackhole and wormhole attacks. The MAC value 'C' is found by using the keys of the user since MAC function provides authentication. MAC is very robust because it found by using only the sender's identification and its unique transaction identifiers. In this paper, we propose a new method to prevent the wormhole and black hole attacks. Section 2 explains the previous works that were carried out in the past years. Section 3 provides basic information about the attacks and types of attacks. Section 4 describes the proposed scheme which rectifies the previous problem and develop a new scheme to prevent the attacks. Section 5 describes about the simulation made on packet delivery ratio, throughput and routing overhead over misbehavior nodes.

2. RELATED WORK:

Rashid Hafeez Khokhar et al [8] have discussed about the review of current routing attacks in mobile ad hoc networks. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET. However, these mechanisms are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. They have examined different routing attacks, such as flooding, blackhole, link spoofing, wormhole, and colluding misrelay attacks, as well as existing solutions to protect MANET protocols.

In [9], Satoshi Kurosawa et al, have proposed a dynamic learning method for overcoming black hole attack for AODV based mobile ad hoc networks. In a black hole attack, a malicious node impersonates a destination node by sending a spoofed route reply packet to a source node that initiates a route discovery. By doing this, the malicious node can deprive the traffic from the source node. we propose an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

Rutvij H. Jhaveri [10] et al have proposed a method to detect wormhole attack against AODV protocol. The main objective of their work is to address some basic security concerns in MANET, operation of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. Wormhole attack commonly involves two remote malicious nodes shown as X and Y. X and Y both are connected via a wormhole link and they target to attack the source node S. Wormhole attack is a real threat against AODV protocol in MANET. Therefore, trustworthy techniques for discovering and detection of wormhole attack should be used.

Rouba El Kaissi et al [11] have given a Defense mechanism against Wormhole attacks for Wireless sensor networks. They addressed the wormhole attack, which is a severe attack in wireless sensor networks whereby an attacker stores transmitted packets and then replays them into the network. Defending against such an attack is challenging because it can be launched even if all network communication is authentic and confidential. They have designed DAWWSEN, a proactive routing protocol based on the construction of a hierarchical tree where the base station is the root node, and the sensor nodes are the internal or the leaf nodes of the tree.

The tree construction is initiated by the base station which broadcasts a request packet in order to discover its children nodes. A request packet contains the ID of the node that originates the request packet and the hop count which is equal to one in the case of a request packet sent by the base station.

Mehdi Kargar and Mohammad Ghodsi [12] We study routing in ad hoc and wireless networks from a game theoretic view point. Based on this view, the network consists of selfish and greedy nodes who accept payments for forwarding data for other node, if the payments cover their individual costs incurred by forwarding data. Also, route falsification attacks are easy to launch by malicious nodes in ad hoc networks. These nodes falsify data and routes in the network. Thus, mitigating this attack is vital for the performance of the whole network. Here we present a truthful and secure mechanism for routing in ad hoc networks that cope malicious and selfish nodes. The purpose of a mechanism design problem is to define and explain a game. This game should be played in such a way that the outcome of the game played by independent agents according to the rules set by the mechanism designer will be the preferred outcome. This outcome is called the social optimum. The game should be designed based on the dominant strategy and results in the social optimum. The dominant means that no player has no incentive to lie and deviate from the strategy. The final state is called dominant-strategy equilibrium if all players playing dominant strategies in the game.

3. TYPES OF ATTACKS

In general, there are two types of attacks in network security. They are : passive attack and active attack. Passive attacks are less harmful than active attack since they do not affect or modify the existing data. But active attack does modification to the existing data. Since there is no central control entity in mobile ad hoc networks, the nodes have to keep themselves secure. The following are the popular types of active attacks in MANET:

i. Wormhole attack
ii. Blackhole attack
iii. Rushing attack
iv. Sinkhole attack
v. Sybil attack and so on.

There are two types of routing protocols in MANET namely proactive and reactive routing protocols. Both the protocols are affected by these active attacks.

When we use proactive routing protocol such as DSDV and WRP, the nodes are periodically sending HELLO and BEACON signals to every other node in the network. When a source node S wants to send the data to destination D, it may send the data through some malicious node M. after getting the data, it will forward the data to D. In this time the destination D will not know about the presence of M and thinks that S and itself are direct neighbors. If D wants to send some data to S, D is unknowingly sending the data S through malicious node M.

In case of on-demand routing protocols such as AODV, DSR and etc., is also affected by the same way. That is, if a source node S wants to communicate with a destination node D, it will initiate to send route request packets. These RREQ packets are forwarded through malicious nodes unknowingly. So D will think that the packets are coming only from S. These type of wormholes are possible more often in mobile ad hoc networks.

The malicious node can attack in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations.

i. Wormhole Attack:

Wormhole attack is a silent and severe type of attack since it simply copies the packet at one location and replays them at different location or within the same network. So, in wormhole attack, there are two neighbor malicious nodes. They copy the packet at one location and replay the same packets without any changes in the content at different location or within the same network.

For example, if a source node S wants to communicate with a destination node D, S will initiate the route request packets to its neighbors B and C. then both B and C forwards the route request packets to their neighbors. But C doesn’t know about the presence of such pair of malicious nodes M1 and M2. When M1 receives the packet, it forwards or tunnels the packet to its pair M2. Then M2 forwards the packet to E and E sends the packet to destination D. This time D will not about the malicious nodes M1 and M2. Also the route request packets are forwarded through multiple paths in on-demand routing protocols. In this scenario, the route request packets are sent through B also. B forwards the packet to F and F forwards the packet to destination D. But D ignores the second path that is via S-B-F-D only it accepts the path S-C-D. But the path S-C-D involves two malicious nodes. In future, D will select the path D-C-S to send the data to S.

ii. Blackhole Attack:

Blackhole attack is also an important and suspicious attack in mobile ad hoc networks. It sends fake or false routing information to the source node that it has fresh routing path from source to destination. In on-demand routing protocol, if a source node S starts to send route request(RREQ) packets to initiate the transmission. At that time, S sends route request packets to its neighbors. They are forwarding the packets to their neighbors. In this way the route request packets are sent up to the destination. In blackhole attack, the attacker captures the route request packets and sends route reply(RREP) packets back to the source node S that it has the fresh route from S to destination D. Source node S discards the other route reply packets that are coming from other route.

After getting the route reply from attacker node, S decides to send the further data along that path. But the data is transmitted only to the attacker node. And attacker node will decide whether the data may be forwarded or to be discarded.

iii.Rushing Attack:

Rushing attack is one of the most important types of Denial of Service (DoS) attack. It is against all currently reactive (on-demand) routing protocols in MANETs. An attacker can forward route request packets (RREQs) more quickly than legitimate nodes, and thus increase the chance that routes which include the attacker will be discovered rather than other valid routes. After the attacker includes itself into the routes, it can launch different attacks such as dropping the packets that it receives, or modifying the content of the packets.

iv. Sinkhole Attack:

In a sinkhole attack for ad hoc and sensor networks, the attacker tries to attract nearly all traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the attacker at the center. Like black hole attacks in ad hoc networks, sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with

1. If the secret key is generated by the attacker node, it is used to encrypt the above parameter like query sequence number etc.,

2. Encrypts the following information along with route reply by using the secret key

3. Attacker found the MAC value and forward the route reply packets to the source node S

4. Also it sends the information about the intermediate nodes that are passed by the route request packets.

5. Then source node S will check the MAC value once again by using the same secret key and MAC function ‘C’

6. If two MAC values are same, then it is accepted thus the node that sent the route reply is not the attacker

7. Otherwise, that is the attacker node. So source node S simply discards the route reply, and S reinitiates the route discovery process, respect to the routing algorithm

v. Sybil Attack:

The attacker presents multiple identities to other nodes in the network. The sybil attack can significantly reduce the effectiveness of fault-tolerant distributed storage systems, routing algorithms, data aggregation, voting, fair resource allocation and so on.

4. PREVENTION OF WORMHOLE ATTACK:

In secure VBOR [6], the route request packets are sent by computing the message authentication value (MAC). After appending the source and destination addresses, query sequence number, query identifier and security association number along with the RREQ, the MAC value is found with subjection of MAC function ‘C’. After the source sends RREQ packet through intermediate routers, they will not verify the packet because they do not know the shared secret key of source and destination. Instead, intermediate nodes are adding their identifiers along with existing packet without any encryption, so the message after leaving from one of the intermediate routers looks like

$$M = C(K_{st}(RREQ, SA_{NUM}, Q_{ID}, Q_{SEQ}, SA, DA))\, SA, DA, NGIEH_{ID1} \quad (1)$$

In this MAC value along with neighbor identifier are passed through many more intermediate routers until the destination is reached. Finally the packet reaching the destination will contain the MAC value, and the accumulation of ID’s through which the message was traveled from source to destination. The destination can get different routes from different paths.

By this way, we can prevent the wormhole attack. Because the MAC value is computed by using the secret key of two users, the wormhole attacker doesn’t get the secret key, thus can’t able to find the MAC value. The colluding attackers are not finding the MAC value ‘M’.

5. PREVENTION OF BLACKHOLE ATTACK:

In MANET, the nodes are forwarding the packets using formula 1. In black hole, the attackers are getting the route request packets and say that it is having the latest and fresh route to the destination. But it is not having the route to that particular destination. Based on the MAC value, the route request packets are decrypted by the mobile nodes. It is difficult for the attacker to generate the secret key, since it should be shared among the nodes. There are some conditions that make the algorithm as efficient:

After receiving the route requests from many paths, the destination will reply back to the source with the message that contains a session key (K_S) through the path based on the selection criteria. The session key will be used for encrypting/decrypting the original data .The session key is sent to the source by encrypting the session key along with security association number, query identifier, query sequence number, IP addresses of source and destination, route reply using the shared secret key of source and destination (Kst).Then all the values are subjected into a MAC algorithm like SHA-1 or MD5. The destination also finds the MAC value as,

$$M = C(K_{st}(RREQ, SA_{NUM}, Q_{ID}, Q_{SEQ}, SA, DA))\, SA, DA, NGIEH_{ID1},$$
$$NGIEH_{ID2}, ...NGIEH_{IDN} \quad (2)$$

By receiving this message from destination, the sender can decrypt and compute a new MAC value by using this message and then the sender compares the new MAC value with the one it received from receiver. If they are same the sender assures that there are no alterations in the transmission otherwise the message will be dropped. Here the destination will store all the query sequence number that it received. By using this query sequence numbers the destination will identify the message replaying and denial of source attacks.

6. PERFORMANCE ANALYSIS

Simulation study has been carried out to show the performance of the proposed secure VBOR protocol against various attacks like blackhole, wormhole. Simulation results have been compared for different types of attacks for different types of secure protocols. In our simulation, test area is set as 1500m x 1500m along with IEEE 802.11 MAC protocol. Various propagation parameters are considered for two ray propagation model. Transmission range is set to 250meters for 100 numbers of nodes. We have taken the packet size as 512 bytes and initial energy as 100 joules

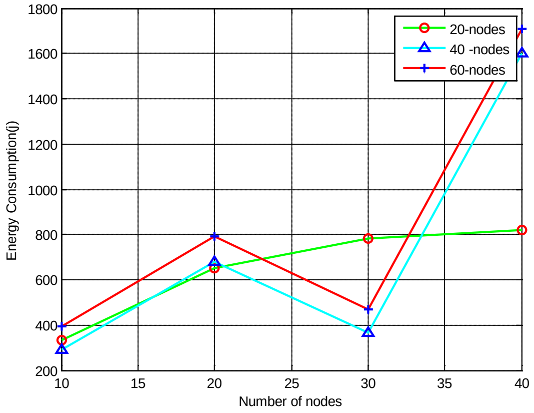

Figure 1: Energy Consumption Vs Number Of Nodes

The energy consumed by the cluster nodes and gateway member is very high for the number of nodes 40 and 60 is depicted in figure1. Here, the energy consumption is very high due to the count of beacons and calculation of transmitted and received beacons by every node When the mobility of the nodes is low for 20 nodes, the energy consumption is high because of very less computation of beacons of node movement. But for the 40 and 60 nodes, the energy consumption is high because of node mobility.

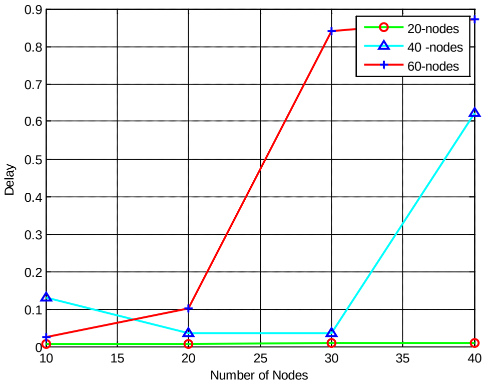

Figure 2: Variation In Delay With Number Of Nodes

The delay that is depicted in figure 2, defined as difference between the time at which the packets are sent and time at which the packets are received. Our simulation shows that the delay is very low when the number of nodes is less that is 20. But the delay becomes high when the number of node is 40 and 60. The delay is high when the movement of nodes is very high in the case of 60 nodes. But when the number of nodes is 40 and mobility is high, the delay peaks to high from its starting point finally it gets down since there are no movements of the nodes. The delay for 20 nodes is very low however there is little movement of nodes.

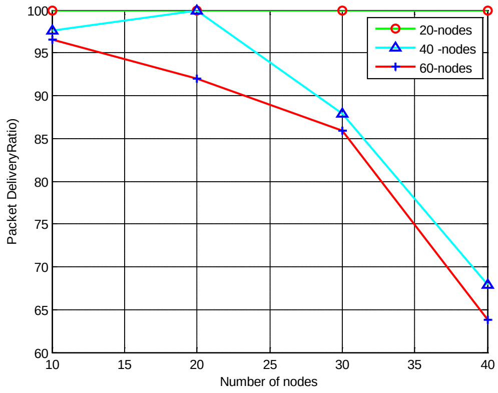

Figure 3: Packet Delivery Ratio Vs Number Of Nodes

In figure 3, we have achieved the packet delivery ratio for varying number of nodes 20, 40 and 60. Packet delivery ratio for 20 nodes is very high when compared to 40 and 60 nodes. When the number of node is increased, the packet delivery ratio should be low because of high number of nodes and their mobility.

The following table shows that our proposed protocol SVBOR performs better for the attacks that are listed below.

Table I: Defense Against Attack Of Various Secure Protocols

Attack	**Protocol**				
	SRP	**SEAD**	**Ariadne**	**SAODV**	**SVBOR**
Black hole	No	No	No	No	Yes
Worm hole	No	No	No	No	Yes
Rushing	Yes	Yes	Yes	Yes	Yes
Sinkhole	NA	NA	NA	NA	NA
Sybil attack	No	Yes	Yes	Yes	Yes

7. CONCLUSION:

In wormhole attack, there are two neighbor malicious nodes. They copy the packet at one location and replay the same packets without any changes in the content at different location or within the same network. Blackhole attack is also an important and suspicious attack in mobile ad hoc networks. It sends fake or false routing information to the source node that it has fresh routing path from source to destination. We have shown the various secure protocols against various attacks. However, we have taken only two types of attacks for our work called prevention of attacks for secure VBOR namely, wormhole and blackhole. Here in this work, we have shown the MAC value found with the source and destination addresses along with the neighbor information. Thus the attackers in blackhole and wormhole attacks are not being able to get the secret key of the particular nodes since the secret keys are generated among the legitimate nodes and used by these nodes only. Since the MAC value is found by using sender's identification, it is restricted to use only the authentication mechanism. So in some times, the data can be attacked because the whole MAC value 'C' is encrypted only by the secret key. This secret key is vulnerable to few attacks like Sybil attack. In future, this approach can be taken in to consideration for avoiding and preventing these types of attacks.

REFERENCES

[1]. Ashwani Kush, P. Gupta and C.Jinshong. Hwang, "Secured Routing Scheme for Adhoc Networks, International Journal of Computer Theory and Engineering" , Vol. 1, No. 3, August, 2009,1793-8201

[2]. Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in *Proceedings of MobiCom02*, 2002.

[3]. S. Yi and R. Kravets, "Security-aware ad hoc routing for wireless networks," in *Proceedings of MobiHOC01*, 2001.

[4]. Karan Singh, Rama Shankar Yadav and Ranvijay, "A Review Paper on Ad-Hoc Network Security, International Journal of Computer Science and Security", Volume (1): Issue (1) 2010

[5]. J. Nafeesa Begum, K.Kumar and Dr.V.Sumathy, "Multilevel Access Control in a MANET for a Defense Messaging system using Elliptic Curve Cryptography", International Journal of Computer Science and Security, Volume (4): Issue (2) 2012

[6]. Jun Jiang and Symeon Papavassiliou, "Detecting Network Attacks in the Internet via Statistical Network Traffic Normality Prediction", Journal of Network and Systems Management, Vol. 12, No. 1, March 2004

[7]. T.V.P.Sundararajan , Dr.A.Shanmugam, "Performance Analysis of Selfish Node Aware Routing Protocol for Mobile Ad Hoc Networks", ICGST-CNIR Journal, Volume 9, Issue 1, July 2009

[8]. Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, volume (2) issue (3) 2011

[9]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

[10]. Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, **"**MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010

[11]. Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, DAWWSEN: "A Defense Mechanism Against Wormhole Attacks In Wireless Sensor Networks", International Conference on Innovations in Information Technology (IIT'05), 2005

[12]. Mehdi Kargar and Mohammad Ghodsi, "Truthful and Secure Routing in Ad Hoc Networks with Malicious and Selfish Nodes", International Journal of Security and its Applications Vol. 3, No. 1, January, 2009