ISSN:0975-9646
Arpana Akash Morey et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2373-2376

Review of a Secure Approach to Prevent Packet Dropping and Message Tampering Attacks on AODV-based MANETs

Arpana Akash Morey[1], Jagdish W. Bakal[2]

[1] *IT Dept. Mumbai University, PIIT,New Panvel,MS, India*

[2] *Principal, SSJCOE,Mumbai Universiy Dombivali (E), MS, India*

***Abstract*: Mobile Ad Hoc Network (MANETs) is a network of mobile nodes which can move freely. These nodes have characteristic that they can be dynamically self-organized into arbitrary topology networks without a fixed infrastructure. MANETs are highly dynamic network because nodes may join and leave the network at any time. The Ad hoc on demand distance vector routing is a reactive routing protocol that finds the route on demand i.e. when one node wants to send message to another node. The different network layer attacks such as worm hole attack, black hole attack, packet dropping and message tampering attack causes network operation disturbance. Security at network layer can be provided using different approaches. These approaches used to detect and prevent such attacks in MANET. In this paper we review some techniques that have prevented such attacks.**

***Key words*—AODV, worm hole attack, black hole attack, gray hole attack, message tampering attack, packet dropping attack.**

I. INTRODUCTION

Mobile Ad hoc networks (MANETs) are arrangements of small portable devices that are interconnected by wireless links. These networks have no fixed infrastructure and there is no centralized controlling mechanism in MANET such as base stations. In a MANET, the nodes are free to move anywhere in the network or out of the network and organize themselves into a network. They can be deployed in a diverse range of application domains including wireless sensor and vehicular networks, military communications, and as a viable solution for Internet connectivity in fourth-generation (4G) networks, especially where nodes are located out of radio range, as for example in underground transport systems [13].

The MANET routing protocols can be broadly classified as reactive routing protocol and proactive routing protocol. Proactive routing involves attempting to maintain routes between nodes in the network at all times, plus when the routes are not currently being used. Reactive routing involves searching for routes to other nodes only as they are needed. The process of routing takes place only when a node wishes to communicate with another node if there is no route table entry for that node. Ad hoc on demand distance vector (AODV) is a reactive routing protocol in which network generates routes right at commencement of communication. Arrange a route to destination only when a node wants to send packet to destination. Routes are maintained as long as they are needed. To send messages to destination, it broadcast route request messages (RREQ) to its neighbors which then rebroadcast them to their neighbors. This process continues until RREQ reaches the target destination. On receiving RREQ message from source node, it transmits Route Replay (RREP) on same reverse path. The AODV can be attacked by wormhole adversary [7].

The attacks in mobile ad hoc networks can be classified as attacks at different layers for example attack at network layer are wormhole attack, black hole attack, message tampering attack, packet dropping attack.

A.Wormhole attack [12]:

In this attack an attacker records packets at one location in the network and tunnels them to another location. When routing control messages are tunneled, routing can be disrupted. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

B.Black hole attack [16]:

In this attack two things are take place. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrong doing.

C. Gray hole attack [17]:

This attack takes place in two phases. In the first phase a valid rout towards destination is advertised by nodes itself. In second phase, with a certain probability nodes drops intercepted packets. This attack causes message dropping. This attack is known as routing misbehavior attack.

D .Packet dropping attack [18]:

This attack causes direct interruption to the routing message. In this attack, an adversary collaborates as usual in the route discovery process and launches the constant packet dropping attacks if it is included as one of the intermediate nodes. In addition, instead of constantly dropping all the packets, adversaries might vary their techniques using random, selective, or periodic packet dropping attacks to help their interrupting behavior remain concealed.

E.Message Tampering Attack [13]:

In this attack an attacker changes the contents of the routing messages. It alters the routing messages either by deleting some bytes or by adding few bytes to it and forwards them with falsified information. The immediate malicious nodes are responsible for such intentional malicious activity.

The security is one of the most important challenges of MANET. The unique characteristic of MANET i.e. dynamic and continuously changing network topology, resource constraints such as limited battery power and bandwidth makes it difficult to use the existing security schemes for the conventional networks directly for MANETs. There are security criteria for MANET which is described below in order to evaluate whether the MANET is secure. The first security criteria include availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service. Second is integrity guarantees the identity of the messages when they are transmitted. Third is confidentiality means that certain information is only accessible to those who have been authorized to access it. Fourth is Authenticity is essentially assurance that participants in communication are genuine and not impersonators. Fifth is Non repudiation ensures that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. Sixth is authorization, which is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. Seventh one is anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. The main goal of the security requirements for MANET is to provide a security protocol, which should meet the properties like confidentiality, integrity, availability and non-repudiation to the mobile users. In order to achieve this goal, the security approach should provide overall protection that spans the entire protocol stack [15].

There are many approaches for detection and prevention of network layer attacks. This paper covers review of some of the approaches. The section II of paper contains the overview of AODV based MANETs. The section III contains literature review, section IV contains challenges of approach to prevent attacks in MANET and section V concludes the paper.

II. AODV BASED MANETS

An ad hoc on demand distance vector routing protocol is designed for ad hoc networks for routing. AODV is capable of both unicast and multicast routing. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source. Otherwise, it rebroadcasts the RREQ. Nodes keep track of the RREQ's source IP address and broadcast ID. If they receive a RREQ which they have already processed, they discard the RREQ and do not forward it. As the RREP propagates back to the source, nodes set up forward pointers to the destination. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route [5][7].

MANETs are frequently used in insecure environments like disaster sites and military applications. Ad-hoc On Demand Distance Vector (AODV) is widely used routing protocol. AODV is based on distance vector routing, but here the updates are shared not on a periodic basis but on an as per on demand basis. For example, battle field ad hoc network, in such a network it would surely be first concerned with the efficient and in time delivery of the message but with this, we will have to be more concerned about the strong secrecy of the information also. These kinds of scenarios, where we want to transmit private and secure information very rapidly, and security mechanism is needed [20].

III. LITERATURE REVIEW

In [2] G.S. Mamatha, Amos J Paul proposes the way to identify parallel different types of attacks in MANETs. The proposed approach aims at detecting malicious nodes while computing route in the network using Aodv protocol and re-routing packets around it. The design of algorithm of this

approach is based on three modules. First will be the sender module, second will be the intermediate node module and third will be the receiver module. AODV (Ad hoc on demand distance vector protocol) is used as data forwarding protocol. To develop our proposed system, they use the simple acknowledgement approach which has two way communications, a semantic security mechanism to generate hash code and principle of flow conservation to identify the threshold value for packet dropping. However this approach can not identify and prevent more MANET attacks so it is not more robust approach.

In [1] Mohammad, Isaac Woungang, Sanjay Kumar Dhurandher has proposed a technique to prevent message tampering and packet dropping attacks in Aodv-based MANETs. He enhances the AODV based protocol named highly secured approach against attacks on MANET (HSAM).The overall goal of enhanced HSAM (EHSAM) is to eliminate chances of malicious nodes that compromise the original data packets, while improving the performance of the HSAM scheme. EHSAM outperforms HSAM in terms of packet delivery ratio, throughput rate, and number of broken links. However it can be enhanced in throughput rate.

In [10] Pradeep kumar and Swati Pokhariyal has proposed a novel scheme for detection and elimination of black hole/gray hole attacks in MANET. He proposed an algorithm in which 3-4 candidate nodes are considered out of which the node having highest residual energy is considered as the backbone node (BBN). BBN work is performed by one active node and other nodes are in passive form. If at any point the energy of active node decreases then it transfers the control to the then it transfers control to the next candidate node having the max energy and all other nodes become passive. Only the active node acting as BBN node has read/write access to tables and the tables used for detection are shared among all candidate nodes. Thus, at one point of time, there is only one active node acting as BBN and performing detection activities. This reduces the overhead on network as it is not required to establish a connection between all other candidate nodes and with the help of a single BBN the computation process increases which leads to faster and accurate detection. The attacker node can be eliminated from network using the threshold value and the count of false positives.

In [6] Vishnu K., Amos J Paul has proposed a scheme for detection or removal of cooperative black hole/gray hole attack in MANET. The proposed technique works as follows. Firstly a backbone network of trusted nodes is established over ad hoc network the source node periodically requests one of the backbone nodes for a restricted (unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (RIP) also. If any of the routes responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

In [4] Nidhi Lal has proposed an improved Watchdog mechanism which identifies the malicious node in the network as well as spots the network congestion. In [8] Aarfa Khan has proposed a Normalized Worm hole Local Intrusion Detection (NWHLID) which is the modified version of Local Intrusion Detection Routing Security over mobile Ad-Hoc Network which has a intermediate neighbor node discovery mechanism, packet drop calculator, individual node receiving packet estimator followed by isolation technique. In [5] a new routing technique called security aware ad hoc routing that incorporates security attributes as parameters in to ad hoc route discovery. SAR enables the use of security as a negotiable metric to improve the relevance of route discovered by ad hoc routing protocols. A two tier classification of routing protocol security metrics, and propose a framework to measure and enforce security attributes on ad hoc routing paths. In addition to determining a secure route, the information in routing messages must also be protected against alteration that can change routing behavior. The security of ad hoc routing algorithm is improved with respect to transmission of routing messages. Zapata and Asokan in [7] proposed SAODV i.e. a secure version of AODV which uses digital signature and hash chains to secure the routing messages. By using unique characteristic of Mobile Ad hoc network most applications were developed. The security issue of routing information was an issue not addressed in recent routing protocol. Several potential problems are presented in [14] including computational overload attack, node compromise, energy consumption, and black hole attack. In [15] attacks are categorized as manipulation of routing information and exhaustive power consumption and provide detailed treatment of many characteristic attacks.

In [9] Jasleen Arora Paramjeet Singh, Shaveta Rani has proposed a scheme for detecting and preventing attacks in MANET. The overall objective is to find the nodes which frequently misbehaves and based upon their miss ratio they will be eliminated from the network. In [10] Jonny Karlson has proposed a new MANET wormhole detection algorithm based on traversal time and hop count analysis. Introduces a new wormhole detection paradigm based upon Traversal Time and Hop Count Analysis (TTHCA), which in comparison to existing algorithms, consistently affords superior detection performance, allied with low false positive rates for all wormhole variants. However it is feasible that a participation mode wormhole node will deliberately give false measurement information concerning time measurement, so potentially compromising the wormhole detection mechanism.

IV. CHALLENGES OF APPROACH TO PREVENT ATTACK IN MANET

Security in MANETS is such a hot topic among the research communities, if it is assured properly it can be used as a success factor and for the widespread deployment of the network. Several types of attacks in network layers have been identified and analyzed recently in most research papers. Security countermeasures and the defense against for each of the network attacks so far designed and implemented for MANETS are presented in the above sections. The research proposals till date, in MANETS are

based upon a specific attack. They could work well in the presence of designated attacks, but there are many unanticipated or combined attacks that remain undiscovered. A lot of research is still on the way to identify new threats and create secure mechanisms to counter those threats. More research can be done on the robust key management system, trust-based protocols, integrated approaches to routing security, and data security at network layer [19].

V. CONCLUSION

In this paper we have introduced the MANET network and classification of routing used in MANET. The different MANET attacks on network layer disturb the networking operation. AODV routing protocol finds route from source to destination. But if the malicious node is present in network it does not allow routing messages to properly send to other nodes in network. So the security mechanism that prevents such attacks is required. The security mechanism can be evaluated by different security criteria.

In this paper we reviewed some of techniques that prevent the network layer attacks. Some techniques used to detect network layer attacks in parallel and some of are designed for preventing some specific attacks.

REFERENCES

[1] Mohammad S.,Isaac Woungang,, Sanjay Kumar Dhurandher (2013) *"Preventing Packet Dropping and Message Tampering Attacks on AODV-based Mobile Ad Hoc Networks"* IEEE 2012.

[2] G.S. Mamatha, Amos J Paul ," *Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks"*, 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22.

[3] G. S. Mamatha, Dr. S. C. Sharma" *A New Combination Approach To Secure MANETS Against Attacks"* International Journal of Wireless & Mobile Networks (IJWMN) Vol.2, No.4, November 2010.

[4] Nidhi Lal," *An Effective Approach for Mobile ad hoc Network via I-Watchdog Protocol*" International Journal of Artificial Intelligence and Interactive Multimedia, Vol. 3, No.1.

[5] Seung Yi, Prasad Naldurg, Robin Kravets," *Security Aware Ad hoc routing for Wireless Networks"*

[6] Vishnu K, Amos J Paul," *Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks"* 2010 International Journal of Computer Applications.

[7] M. G. Zapata and N. Asokan, *"Securing Ad hoc routing protocols"* In wise'02 proceedings of ACM workshop on wireless security ACM press 2002.

[8] Aarfa Khan," *Normalized Worm-Hole Local Intrusion Detection Algorithm (NWLIDA*)" International Journal of Modern Engineering & Management Research Vol 1 Issue 3 October.

[9] Jasleen Arora, Paramjeet Singh, Shaveta Rani " *Detecting and Preventing Attacks in MANET"* International Journal of Computer Applications Volume 81 – No5, November 2013.

[10] Jonny Karlsson," *A New MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis"* Sensors 2011

[11] Pradeep Kumar, Swati Pokhariyal" *A Novel Scheme for Detection and Elimination of Blackhole/Grayhole Attack in Manets"* IJCSMC, Vol. 3, Issue. 12, December 2014

[12] Vivek Sharma., *"A Review of Security Attacks in MANETs,"* Vol-II No. 2 (58-63): 2011.

[13] Kaur Sharndeepa, Gupta Anuj,*"a review on different secure routing protocols and security attacks in mobile Ad hoc networks,"* Kaur et al., International Journal of Advanced Engineering Technology.

[14] Sathish Alampalayam Kumar, *"Classification and Review of Security Schemes in Mobile Computing", Wireless Sensor Network, 2010.*

[15] H. Deng *"Routing security in wireless ad hoc networks"*, 2002.

[16] M.Jakobsson,S.Wetzel and B.Yener, *"Stealth attacks on ad hoc wireless networks"* in proceedings of VTC,2003.

[17] O. F. Gonzalez, G. Ansa, M. Howarth, G. Pavlou, *"Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks"*, Journal of Internet Engineering, Vol. 2, No. 1, pp. 181-192,June 2008.

[18] Manikandan, S.P. and R. Manimegalai," *survey on mobile ad hoc network attacks and Mitigation using routing protocols"* American Journal of Applied Sciences, 2012.

[19] G.S. Mamatha, Dr. S.C. Sharma," *Network Layer Attacks and Defense Mechanisms in MANETS -A Survey"* International Journal of Computer Applications.

[20] Ms Darshana Patel , Ms Vandana Verma ," *Security Enhancement of AODV Protocol for Mobile Ad hoc Network"* International Journal of Application or Innovation in Engineering & Management (IJAIEM).