ANALYSIS ON MOBILE AD HOC NETWORK ATTACKS AND EXTENUATION USING ROUTING PROTOCOLS

K.Kiran Reddy
Associate Professor,Dept.of.CSE
MLRIT, Dundigal Hyderabad,India

M.Pallavi
Asst.Prof.Dept.Of.CSE.
MLRITM,Dundigal,HYD

Dr P.Bhaskara Reddy
Director
MLRIT,Dundigal,Hyd

ABSTRACT

Mobile Ad hoc Networks (MANET) due to its unpredictable topology and bandwidth limitations are Vulnerable to attacks. Establishing security measures and finding secure routes are the major challenges Faced by MANET. Security issues faced by ad hoc networks are node authentication, insider attack and Intrusion detection. Implementing security measures is challenging due to the presence of limited resources in the hardware device and the network. Routing protocols attempt to mitigate the attacks by isolating the malicious nodes. In this study, a survey of various kinds of attacks against MANET is studied. It is also proposed to study modification of AODV and DSR routing protocol implementation with regard to mitigating attacks and intrusion detection. This study studied various approaches to predict and mitigate attacks in MANET.

Keywords: Mobile Ad Hoc Networks (MANET), Security Mechanism, Ad Hoc on Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Attacks in MANET

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) depends upon all the available nodes for routing of data packets, service discovery in the network due to the limited range of transmission. Thus, all the nodes in the network perform critical network functions like routing. The most common routing security is in the form of node and message authentication. Most of the routing protocols are based upon the assumption that all the nodes are trustworthy and they do not maliciously tamper with the messages. Though malicious nodes can easily alter routing messages due to which network traffic is dropped, redirected to different destination or take a longer route. Thus, even one malicious or compromised node can cause failure of the

network (Xiao et al., 2007). Authentication and encryption are used as first line of defense against attacks and intrusion detection is used to detect and respond for newer attacks against the network.Secure routing protocols are mainly based on reactive routing protocols such as Dynamic Source Routing (DSR) Imielinski and Korth, 1996) or Ad hoc On-Demand Distance Vector (AODV) (Perkins and Royer, 1999). In on-demand routing the routes to destinations are discovered only when the source node has a packet to forward, thus, have lower routing overheads. DSR is a source routing protocol in which the data packet carries the route information from source to destination. Route discovery and route maintenance are the basic mechanisms of DSR. A Route Request is sent out to all the neighboring nodes when source node wants to establish a route (Imielinski and Korth, 1996). The neighboring nodes on receiving the request update themselves on the source route and forward it to their neighbors. Either destination node sends a Reply message containing the full source route on receiving the Route Request or a node with route information in its route cache to the destination sends the reply to the source node. The source on receiving several routes picks up the shortest route and sends along the data packet along that path. Route metrics such as the number of hops, delay, bandwidth and the time taken for the Reply to reach the source are all taken into consideration by the source node while selecting route and storing it in its cache. Route maintenance comes into play when intermediate nodes find a link break between itself and the next node, it sends a Route Error message back to source node. The source node then removes the route containing the broken link from its cache and uses another route for the destination or starts a route discovery process. DSR performs effectively in small to medium-sized networks than in large and dynamic networks.

AODV routing protocol is based on DSR and Destination Sequenced Distance Vector (DSDV) routing Protocols (Perkins and Royer, 1999). AODV uses hello messages and sequence number as in DSDV and the route discovery process is similar to DSR. The use of sequence number on route updates avoids the counting- to-infinity problem and also ensures loop-free routes. Route requests (RREQ), Route Replies (RREP) and Route Errors (RERR) are the messages used by AODV for route discovery and maintenance. Route discovery is similar to DSR, when a route is to be established, RREQ is broadcasted. RREQ on reaching destination or an intermediate node with route information to destination, an RREP is initiated and is unicasted back to source node with the route information. Nodes on detecting link break in the active route use a RERR message to notify the other nodes about the break. AODV updates all the information in route table, containing information about routes available to destination with hop count, sequence number and other information. When a link break isdetected, the route is invalidated and the sequence number in the route table entry is marked invalid. The main difference between DSR and AODV is that the data packets in DSR carry full routing information whereas in AODV packets carry only the destination IP address.

In this study, a survey of various kinds of attacks against MANET is studied. And also explore several DSR and AODV routing protocol implementation with regard to intrusion detection and mitigating attacks.

2. MATERIALS AND METHODS

In this study, we broadly classify the study into three sections namely, Attack in MANET, Intrusion Detection and secure routing.

1.1 Attacks in MANET

Snooping where the nodes misuse the inherent trust between nodes to eavesdrop on packets to obtain packet payload data and routing information. Flood storm attacks where malicious nodes flood the network with route requests and route replies, effectively paralyzing the network. In tampering attacks, the intermediate nodes modify the packet content or change source and destination address. Data packets are prevented from reaching node and also nodes are prevented from sending data packets in denial of service attacks (Douligeris and Mitrokosta, 2004). In rushing attacks, a malicious node establishes routes through it (Hu et al., 2003b).

Malicious nodes advertise itself as having shortest route to destination node, thus all traffic is forwarded to it and the node does not forward any traffic at all in Blackhole attack. These black holes can be detected only by 4 monitoring for lost traffic (Weerasinghe and Fu, 2007).

A wormhole attack (Hu et al., 2003a; 2005) creates a tunnel called, wormhole tunnel, between two nodes. A wormhole tunnel diverts packets to some random node in the network rather than the intended destination. The wormhole attack is shown in Fig. 1. The path W-W, in Fig. 1, denotes the wormhole tunnel. The correct path is S-A-B-C-D. A Sybil attack (Douceur, 2002) occurs when the malicious node acts like two or more nodes. Sybil nodes are created by false identities or impersonation of nodes in the network.

1.2. Intrusion Detection Systems

Many researchers have conducted various studies on the Intrusion Detection Systems (IDS) for MANET. Some of them based on DSR and AODV are reviewed in the following paragraphs. Tseng et al. (2003) proposed a solution using specification based technique to detect attacks on AODV. Specification based monitoring capture the correct behavior by comparing the behavior of objects with their associated security specifications. Thus, intrusions which cause incorrect behavior can be detected without exact knowledge about them. The proposed approach uses finite state machines for describing the valid flow of

Issue 3, Vol.4 (June-July 2013)
ISSN 2249-6149

AODV routing behavior. Violations in the specifications are detected by the distributed network monitors. The approach also proposes to add a field in the protocol message to enable monitoring. The proposed algorithm is based on tree structure and a node coloring scheme. The IDS is built on the monitoring architecture that traces AODV request-reply flow. Detail procedures for constructing and processing the trees for detecting attacks are discussed. The proposed method detects AODV routing attacks efficiently and with low overhead.

Zapata (2002) presented AODVSTAT, a network based, real time IDS for networks based on AODV.The study also surveys various attacks against AODV based network and is summarized as shown in Fig.2.

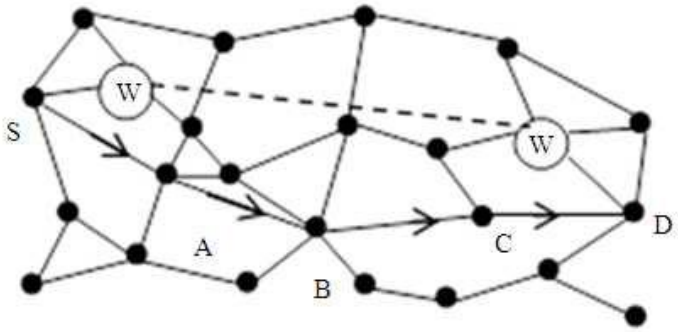

Fig. 1. Wormhole attack

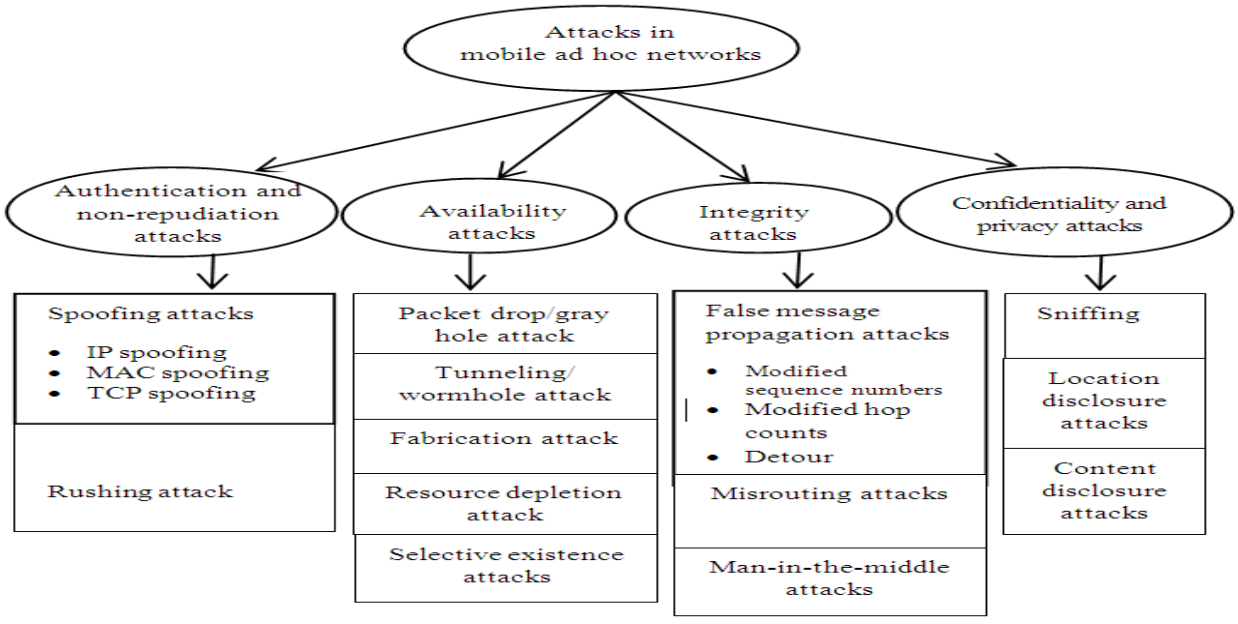

FIG: 2 Various Attacks in MANET"S

The proposed tool (Vigna et al., 2004) is based on the State Transition Analysis Technique (STAT). AODVSTAT sensors are deployed either on stand alone or distributed basis on a subset of the nodes of the network. The sensors perform real-time stateful analysis on the packet stream to detect signs of

intrusions. Experimental results show that the proposed method successfully detects attacks against AODV routing protocol with low number of false positives and low overhead.

Marti et al. (2000) proposed a watchdog mechanism implemented on DSR by categorizing nodes based on dynamic measured behavior. The proposed method complemented DSR with a watchdog and pathrater. The watchdog was used for detection of malicious behavior and runs on each node, listening to all the transmissions of neighboring node. Pathrater is used for trust management and routing policy, every used path is rated. A buffer is maintained by the watchdog which contains recently sent packets and it is removed from the buffer when the packet is forwarded by the next hop. If the packet remains in the buffer, watchdog assumes that the node is misbehaving. Thus, enabling nodes to avoid malicious nodes in their routes and deliver the data packet. On simulation, the proposed method performed efficiently, increasing the throughput by 17% in the presence of 40% misbehaving nodes.

Mangai and Tamilarasi (2011) studied the malicious nodes in Improved Location aided Cluster based Routing Protocol (ILCRP) for GPS enabled MANETs. The proposed method used the location information with security against attacks in high packet delivery ratio. Simulations are performed using NS2 by varying the number of nodes. The simulation results show that the ILCRP provides higher delivery ratio with IDS.

It is observed that watchdog mechanism (Marti et al., 2000) is not only able to mitigate attacks but also improve the throughput with high number of misbehaving nodes. Though Tseng et al. (2003) technique displays the type of attacks better than other methods found in literature, it does not provide a mechanism to mitigate the attacks.

1.3. Secure Routing

Zapata (2002) presented an overview of various approaches to secure routing protocols in Mobile Ad Hoc Networks (MANET). An extension of AODV, Secure AODV, was proposed which provides security features to the routing protocol. Features like digital signatures and hash chains were incorporated to secure the AODV messages. Digital signatures are used to authenticate the non-mutable fields of the messages and hop count information secured using hash chains. The route error messages generated by a node are signed using digital signatures and forwarded. Neighbor nodes verify the signature before forwarding.

Hu et al. (2005) presented a new protocol ‘Ariadne’ based on the DSR protocol for routing protection. Several authentication mechanisms such as digital signatures, MACs computed with pair-wise secret keys, or TESLA could be used with the proposed protocol. Hash chains are used to authenticate every route request protecting the network from overload, thus denial of service attacks are prevented. Attacks from compromised nodes from tampering with the uncompromised nodes are also prevented by the

proposed method.

Combinations of TESLA authenticators (MACs) are added by intermediate routers and a hashing technique to protect the discovered routes. The proposed method's security mechanisms are effective and can also be applied to wide variety of routing protocols.

BucheggerandBoudec(2002)proposed CONFIDANT protocol, as an extension of reactive source routing protocols, such as DSR. The proposed protocol uses a reputation system that rates nodes based on malicious behavior. The neighborhood watch listens into the transmission of the neighboring nodes and observes the route protocol behavior. On detection of any intrusive activity, the node sends an alarm message about the malicious neighbor to other nodes on its friends list. Nodes on receiving alarm messages, evaluates it. The reputation of an accused node is changed only if the source of the alarm is a fully trusted node or the node was similarly accused by several partially trusted nodes.

All three methods mentioned in (Hu et al., 2005; Zapata, 2002; Buchegger and Boudec, 2002) use different techniques for securing the routing protocol. Zapata (2002) method is highly secure at the cost of higher processing power which is scarce in hand held devices. These issues are overcome by Hu et al. (2005) where the option is provided to the end user to propose the level of security. Buchegger and Boudec (2002) overcomes the additional processing overheads by proposing trust based systems which relatively have lower overheads in terms of additional control packets and processor utilization. However the security level is much lower as node can act as friend initially and can cause problems in the network.

1.4. Mitigating Attacks

Deng et al. (2002) performed a study on the security issues in particular about blackhole attacks when routing is performed in a MANET and also proposed a solution for Ad hoc on-Demand Distance Vector (AODV) routing protocol. The authors discussed the routing security issues in a MANET and give an overview of current security schemes proposed for MANETs in the literature. To mitigate the blackhole attacks, it was proposed to disable the ability of the intermediate nodes to reply and all reply messages can be sent from the destination node only but the routing delay increases considerable to make it infeasible. A more workable solution was proposed where using one more route to the intermediate node that replays the RREQ message to check whether the route to the destination exists or not and also use the method only when there were suspected node in the network. Simulation results showed that the proposed method was able to secure AODV from blackhole attack and achieve increased throughput.

Su and Boppana (2007) proposed mechanism to resist creation of in-band wormhole attacks. The proposed method was based on distributed techniques based on the propagation speeds of requests and statistical profiling. The major advantage of the method was that it does not require network-wide

synchronized clocks, do not impose any additional control packet overhead and need only simple computations by the sources or destinations of connections. The proposed approach was implemented in Ariadne and evaluated using the Glomosim simulator. Experimental results show that in-band wormhole creation and usage can be reduced by a factor of 2-10 with very low false alarm rates.

Hu et al. (2003a) presented a protocol, TIK, for detecting and defending against wormhole attacks. The proposed protocol introduces a general mechanism of packet leashes to detect wormhole attacks. Two types of leashes were used: geographical and temporal leashes, to restrict the maximum transmission distance of a packet. The temporal leash is incorporated in the proposed protocol TIK which also provides instant authentication of data packets received. The proposed protocol protects against replays, spoofing and wormhole attacks.

Viswanatham and Chari (2008) proposed using My- AODV agent for detecting and analyzing various attacks on MANET. The My-AODV agent is utilized to introduce various attacks against the network. The proposed system works in two levels, it initially detects nodes which drop data packets, divert routes or consume extra resources. After detection, the recovery process is started where the malicious node is isolated from the network. Thus the network has more secure communication. Simulation results show that the performance of the proposed method improves significantly by reducing the number of packet drops in various attacks. Nodes are periodically checked to check whether they are malicious or not. Simulation results show that the proposed method provides more security and reduce the packet drops.

Cumulative frequency based detection technique for detecting MAC layers attacks

#Packets are detected using data forwarding behavior detection technique

#Authentication code based technique for packet modification

3. RESULTS

From the various literature reivew studied, it can be seen that mitigating security attacks requires extensive hardware and network resources in terms of bandwidth. Trust and reputation based systems utilize the hardware resources to a minimal compared to other resources where authentication and encryption mechanism sytems are in place.

4. DISCUSSION

It is evident from this study that higher processing power becomes an essential component to secure the network. It can be seen that Tseng et al. (2003) method for intrusion detection shows best advantage in bandwidth and resource constrained environment due to its distributed nature. Buchegger and Boudec (2002) have proposed a trust based security mechanism which can provide the first line of defense against

attacks. The proposed method does not increase the processing overheads. Su et al., mechanism provides distributed mechanism for mitigating attacks which supports energy constrained nodes.

5. CONCLUSION

This study investigated various types of attacks in a MANET. It can be seen that most of the attacks that have been detected are modifications of infrastructure based wireless networks and wired networks. Various methods to mitigate attacks proposed in literature are studied. Trust and Reputation based systems are seen as an emerging method to mitigate security attacks. Further work needs to be done to understand the effect of Trust and reputation in MANET.

6. REFERENCES

1.Bhalaji, N., S. Banerjee and A. Shanmugam, 2008. A novel routing technique against packet dropping attack in adhoc networks. J. Comput. Sci., 4: 538-544. DOI: 10.3844/jcssp.2008.538.544

2.Buchegger, S. and J.Y.L. Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceeding of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, Jun. 9-11, ACM, Lausanne, Switzerland, pp: 226-236. DOI: 10.1145/513800.513828 Deng, H., W. Li and D.P. Agrawal, 2002.

3.Routing security in wireless ad hoc networks. IEEE Commun.Mag.,40:70-75.DOI 10.1109/MCOM.2002.1039859

4.Douceur, J.R., 2002. The sybil attack. Peer-to-Peer Syst. Lecture Notes Comput. Sci., 2429: 251-260. DOI: 10.1007/3-540-45748-8_24

5.Douligeris, C. and A. Mitrokosta, 2004. DDoS attacks and defense mechanisms: Classification and state- of-the-art. Comput. Netw., 44: 643-666. DOI:10.1016/j.comnet.2003.10.003

6.Hu, Y.C., A. Perrig and D.B. Johnson, 2003a. Packet leashes: A defense against wormhole attacks i wireless networks. Proceedings of the IEEE Societies 22nd Annual Joint Conference of the IEEE Computer and Communications, Mar. 30-Apr. 3,IEEE Xplore Press, pp: 1976-1986. DOI: 10.1109/INFCOM.2003.1209219

7.Hu, Y.C., A. Perrig and D.B. Johnson, 2003b. Rushing attacks and defense in wireless ad hoc network routing protocols. Proceedings of the 2nd ACM Workshop on Wireless Security, Sept. 19-19, ACM Press, San Diego, CA, USA., pp: 30-40. DOI: 10.1145/941311.941317

8.Mangai, S. and A. Tamilarasi, 2011. An improved location aided cluster based routing protocol with intrusion detection system in mobile ad hoc networks. J. Comput. Sci., 7: 505-511. DOI: 10.3844/jcssp.2011.505.511

9.Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Aug. 06-11, ACM Press, Boston, Massachusetts,U.S.,pp:255-265.DOI: 10.1145/345910.345955

10.Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computer Systems and Applications, Feb. 25-26, IEEE Xplore Press, New Orleans,LA.,pp:90-100.DOI:10.1109/MCSA.1999.749281

11.Su, X. and R.V. Boppana, 2007. On mitigating in-band wormhole attacks in mobile ad hoc networks.Proceedings of the IEEE International Conference on Communications, Jun. 24-28, IEEE Xplroe Press,Glasgow,pp:1136-1141.DOI:10.1109/ICC.2007.193

12.Tseng, C.Y., P. Balasubramanyam, C. Ko, R.Limprasittiporn and J. Rowe et al., 2003.

13.A specification-based intrusion detection system for AODV. Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Oct. 27-30, ACM Press, Washington, DC, USA., pp: 125-134. DOI: 10.1145/986858.986876.

14.Vigna, G., S. Gwalani, K. Srinivasan, E.M. Belding-Royer and R.A. Kemmerer, 2004. An intrusion detection tool for AODV-based ad hoc wireless networks. Proceedings of the 20th Annual Computer Security Applications Conference, Dec. 6-10, IEEE XplorePress,pp:16-27.DOI: 10.1109/CSAC.2004.6

15.Viswanatham, V.M. and A.A. Chari, 2008. An approach for detecting attacks in mobile adhoc networks. J.Comput.Sci.,4:245-251.DOI: 10.3844/jcssp.2008.245.251

16. Weerasinghe, H. and H. Fu, 2007. Preventing cooperative black hole attacks in mobile ad hoc networks:Simulationimplementationand evaluation. Future Generat. Commun. Netw., 2: 362-367. DOI: 10.1109/FGCN.2007.184

17.Xiao, Y., X. Shen and D. Du, 2007. Wireless Network Security. 1st Edn., Springer, New York, ISBN-10:0387280405, pp: 422.

18.Zapata, M.G., 2002. Secure ad hoc on-demand distance vector routing. ACM Mobile Comput. Commun. Rev., 6: 106-107. DOI: 10.1145/581291.581312