A Review Paper on Secure Routing Technique for MANETs

Sonali Sharma[1], Simranjit Kaur[2]

[1]*M.Tech student, Dept. of Electronics & Communication Engineering, Sri Sai College of Engineering and Technology(Badhani), Punjab,India*

[2]*Assistant professor, Dept. of electronics & Communication Engineering, Sri Sai College of Engineering and Technology(Badhani), Punjab,India*

---***---

Abstract - *The mobile adhoc networks are the decentralized type of network in which mobile nodes can join or leave the network they want. Due to self configuring nature of network, active and passive attacks are possible in the network. The active attacks are those which reduce network performance in terms of various parameters. The jelly fish is the active type of attack which reduce network performance and in this paper various secure routing techniques are reviewed and discussed*

***Key Words*: AODV, DSR, MANET**

1.INTRODUCTION

In day-to-day communication wireless networks plays a prominent role. There are many applications where it is widely used like military applications, industrial applications and in personal area networks. Due to its simplicity of installation, scalability, flexibility it is very popular in other applications also. In the case of wired network it has fixed infrastructure like cell phones, microwave and RADAR etc.

Wireless network has further two categories: Infrastructure and Infrastructure less. In Infrastructure wireless networks, the base stations are fixed, the mobile node can move while communicating. Moreover when nodes go out of the range of one base station it comes to the range of other base stations. In infrastructure less network or an adhoc network, base station is not fixed and router moves in any direction during communication. So this network makes their own route for flu using routing protocol.

In coming generation, MANET will be widely used in various applications due to its independent nature. It can join and leave network any time. Topology of the network changes dynamically and covers wide geographically area of network for communication.

Because of its decentralized nature its scalability is better than infrastructure network. In any crucial scenarios such as military conflicts, natural disasters etc, ad-hoc network provides better performance due to the minimum configuration and quick operations.

Ad-hoc networks can be classified into three categories depending on their applications: Mobile Ad-hoc Networks (MANETs), Wireless Mesh Networks (WMNs) and Wireless Sensor Networks (WSN).

1.1 MANET

MANET is a self configuring network, in which topology is dynamic. These nodes are struggling to cope with the normal effect of radio communication channels, multi-user interference; multi-path fading etc. The design of an optimum routing protocol for MANET is highly difficult. To determine the connectivity of network organizations, there is a need of an efficient algorithm link scheduling, and routing in such dynamic scenarios, becomes very important. The efficiency of a routing algorithm depends on the proficient and winning route computation. Usually the shortest path algorithm is a successful method to calculate the optimal way in static networks. But this idea is not possible in MANET platform. There are many factors which can be considered for routing. Networks should adaptively change their routing paths depending on scenarios at any instance to improve any of these affects.

1.2 MANET Architecture

A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. All available nodes are aware of all other nodes within range. The entire collection of nodes is organized in a number of ways. As shown in Fig 1.2 there are more than one path from one node to another . The nodes in a MANET can be of untrustworthy capabilities. Mobile phones, laptop computers and Personal Digital Assistants (PDAs) are some examples of nodes in ad-hoc networks. In MANETs nodes are frequently movable but it can consist of fixed nodes as well such as access points to Internet.

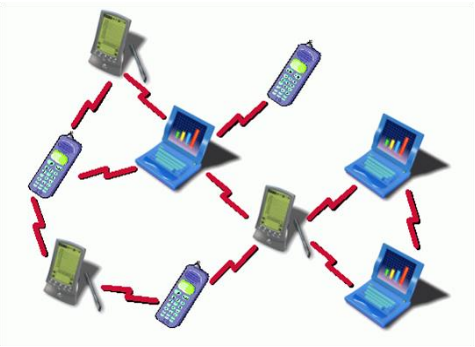


Fig.1- A Simple Mobile Ad Hoc Networks

The nodes in MANETs are interrelated using the multi-hop communication paths. Simply it mentions that all the nodes in the hop must be prepared to contribute in the procedure of deliver a packet by forwarding it from source to destination. Packets are travel through multiple paths. A single file is divided into several data packets, and then these packets are forwarded through different paths. At the destination node, all these packets are combined in sequence to generate the original file.

1.3 Ad Hoc Routing Protocols

The principle objective of these protocols is to create an optimal pathway with minimal number of intermediary nodes between source and destination, the route should have less overhead and reasonable bandwidth consumption in order to transmit the message on time.

The protocol should be able to perform in an effective &efficient manner throughout the networking environment consisting of heterogeneous ad hoc networks i.e., from small to large Multi-hop networks. There are three categories of these routing protocols, which include proactive routing protocols, reactive routing protocols and hybrid routing protocols with respect to the routing topology used in MANET. Proactive routing protocols constantly retain the updated state of the network topology and are typically table-driven. The Proactive routing protocols includes DSDV, OLSR routing protocols. The second category includes reactive routing protocols also known as source-initiated on-demand routing protocols, these are demand driven reactive protocols. Therefore the do not follow the procedure creating & updating routing tables with routing information at regular intervals. As they are on demand routing protocols, so they start route discovery only when they are asked to. DSR & AODV are example of these types of routing protocols. Hybrid protocols are the one which utilizes the advantages of both reactive and proactive approaches. It includes Zone Routing Protocol.

1.3.1 Proactive Routing Protocol

These routing protocols constantly retain the updated state of the network topology by creating a routing table and having the routing information before it is needed. Therefore they are also called as Table Driven protocols. All the nodes present in the network creates& maintains routing information to every other node in the network which is kept in the routing tables and is updated periodically as the network topology changes. These protocols maintain various tables and are not suitable for a larger network because the memory required maintaining node entries for each and every node in the routing table of every node will raise an issue regarding cost, overhead and consumption of more bandwidth.

1.3.2 Reactive Routing Protocol

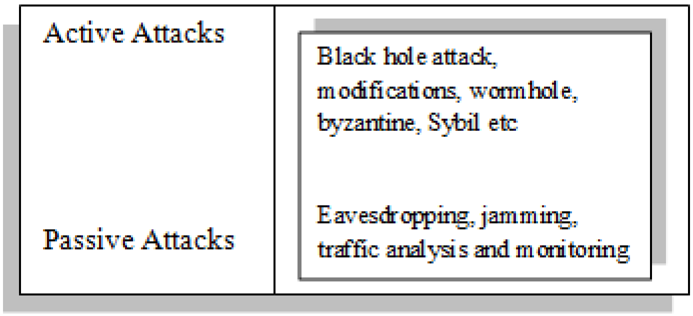
These protocols are also known as source-initiated on-demand routing protocols, these are demand driven reactive protocols. Therefore they do not follow the procedure creating & updating routing tables with routing information at regular intervals. As they are on demand routing protocols, so they start route discovery only when they are asked. In order to send a packet to another node in the network using this protocol, then this protocol initiates a route discovery process for finding the suitable route to the destination and establishing the connection in order to transmit and receive the packet. In this process the RREQ packet is broadcasted throughout the network which adds a significant amount of control traffic to the network due to query flooding.

1.3.3 Hybrid Routing Protocol

These types of protocols make use of the strengths of both the previously discussed protocols by combining them together to obtain better results. In the initial stage routing is done with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The basic idea is that each node has a pre-defined zone centred at itself in terms of number of hops and for the nodes which lie within the zone, the protocol used to maintain routing information in the network is proactive. The nodes which lie outside its zone, it does not maintain routing information in a permanent base. Instead, reactive routing strategy is adopted when inter- zone connections are required.

1.4 Attacks in MANET

There are a variety of attacks possible in MANET. The attacks can be classified as active or passive attacks, internal or external attacks, or different attacks classified on the basis of different protocols. A passive attack does not disrupt the normal operation of the network. The attacker only snoops the data exchanged in the network without altering it. It includes Eavesdropping, jamming and traffic analysis and monitoring. In case of active attacks, the attacker attempts to alter or destroy the data being exchanged in the network. This attack disrupts the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks .The ultimate goals of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, authentication, non-repudiation, and availability to mobile users. The various possible attacks are



Active Attacks	Black hole attack, modifications, wormhole, byzantine, Sybil etc
Passive Attacks	Eavesdropping, jamming, traffic analysis and monitoring

Fig 2. Classification of attacks in MANET

1.5 Jelly Fish Attack

JellyFish attack is concerned with transport layer of MANET stack. The JF attacker disrupts the TCP connection which is established for communication. JellyFish (JF) attacker wishes to intrude into forwarding group and then it delays data packets unnecessarily for some amount of time before forwarding them. Due to JF attack, high end to end delay takes place in the network. So the performance of network (i.e.throughput etc) decreases substantially. Application i.e. file transfer requires reliable and congestion controlled delivery. It is provided by Transmission Control Protocol (TCP). JF attacker disrupts the whole functionality of TCP, so performance of real time applications become worse. JF attack is further divided into three categories- JF Reorder Attack, JF Periodic Dropping Attack, JF Delay Variance Attack.

Jelly fish attacks are targeted against closed-loop flows. The goal of jellyfish node is to diminish the good put, which can be achieved by dropping some of packets. When a malicious nodes launches forwarding rejection attacks it also may comply with all routing procedures. The Jellyfish attack is one of those kinds. A malicious node launching Jellyfish attacks may keep active in both route discovering and packet forwarding in order to prevent it from detection and diagnosis, but the malicious node can attack the traffic via itself by reordering packets, dropping packets periodically, or increasing jitters. The Jellyfish attack is especially harmful to TCP traffic in that cooperative nodes can hardly differentiate these attacks from the network congestion. Reference also described that malicious nodes may even abuse directional antenna and dynamic power techniques to avoid upstream nodes to detect their misbehaviors of dropping packets. This attack mainly targets closed-loop flows as such flows respond to network conditions like packet loss and packet delay. It targets TCP's congestion control mechanism. The main goal of the Jellyfish nodes is to reduce the good put of all the flows to near-zero by either reordering the packets or dropping a small fraction of packets.

2. LITERATURE SURVEY

Author	Year	Description	Outcome
S.S. Tyagi, R.K. Chauhan	2010	Performance analysis of ProActive and ReActive routing protocols for ad hoc networks	AODV and DSR are proved to be better than DSDV.
K. Pandey, A. Swaroop	2011	A Comprehensive Performance Analysis Of Proactive, Reactive and Hybrid MANETs Routing Protocols	In terms of throughput, AODV performance is better than other protocols. Furthermore, DSDV performances poorly from time to time.ZRP throughput does not change even with a change in mobility or pause time because of its hybrid nature
Mohammad Wazid, Vipin Kumar and RH Goudar	2012	Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under JellyFish Attack	Under JF attack DSR protocol shows maximum time efficiency and TORA protocol shows highest throughput.
ManjotKaur , Malti Rani, AnandNayyar	2014	A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks	JellyFish Attack exploits the end to end congestion control mechanism of Transmission Control Protocol (TCP).
S. Mohseni, R. Hassan, A. Patel, and R. Razali	2010	Comparative Review Study of Reactive and Proactive Routing Protocols in MANETs	While it is not clear that any particular algorithm. Each protocol has definite advantages as well as disadvantages and is well suited for certain situations.

3. CONCLUSIONS

In this work, it has been concluded that due to decentralized nature of the mobile adhoc network, malicious nodes enter the network which trigger various type of active and passive attacks. The secure and efficient routing techniques has been reviewed in this paper. In future technique will be proposed which detected and isolate malicious nodes from the network.

REFERENCES

[1] S.S. Tyagi, R.K. Chauhan, "Performance analysis of ProActive and ReActive routing protocols for ad hoc networks", International journal of computer applications, Vol. 1No.-14, 2010, pp. 27-30

[2] K. Pandey, A. Swaroop, "A Comprehensive Performance Analysis Of Proactive,Reactive and Hybrid MANETs Routing Protocols", International Journal of computerScience Issues, Vol. 8, Issue 6, No 3, November 2011, pp. 432-441.

[3] Internet Engineering Task Force, MANET working group charter.Available from IETF MANET group Character Sector , Jan. 2010.

[4] K. Majumder and S.K. Sarkar, "Performance analysis of AODV and DSR Routing Protocols in Hybrid Network Scenario", Proc. IEEE transactions on networking, Dec. 2009, pp. 1-4.

[5] Mohammad Wazid, Vipin Kumar and RH Goudar, "Comparative Performance Analysis of Routing Protocols in Mobile Ad Hoc Networks under JellyFish Attack", 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, 2012

[6] ManjotKaur , Malti Rani, AnandNayyar, "A Comprehensive Study of Jelly Fish Attack in Mobile Ad hoc Networks", , International Journal of Computer Science and Mobile Computing, Vol.3 Issue.4, April- 2014, pg. 199-203

[7] S.A. Ade1& P.A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in MANET", International Journal of Information Technology and Knowledge Management, Vol. 2, No. 2, , Dec. 2010, pp. 545-548

[8] S. Mohseni, R. Hassan, A. Patel, and R. Razali, "Comparative Review Study of Reactive and Proactive Routing Protocols in MANETs", 4th IEEE International Conference on Digital Ecosystems and Technologies 2010 IEEE, Apr. 2010, pp.- 304-309.

[9] S.S. Tyagi, R.K. Chauhan, "Performance analysis of ProActive and ReActive routing protocols for ad hoc networks", International journal of computer applications, Vol. 1No.-14, 2010, pp. 27-30

[10] T.P. Singh, Dr. R.K. Singh, J. Vats, "Effect of quality parameters on energy efficient Routing protocols in MANETs", Vol. 3 No-7, July 2011,pp. 2620-2626.

[11] W. Kiess, M. Mauve, "A survey on real-world implementations of mobile ad-hoc networks", Vol. 5, Issue 3, Apr. 2007, pp 324-339.

[12] X. Hong, K. Xu, M. Gerla, " Scalable routing protocols for mobile ad hic networks",Network IEEE, Vol. 16, Issue 4, july 2002, pp. 11-21.