ISSN:0975-9646

A Review on Reactive & Proactive Routing Protocols and Security Breaches and Remedies in MANETs

Mohammed Aziz Ahmed[1], Mohammed Sirajuddin[2], Nazia Kouser[3]

[1]*Department of CSE, Research Scholar,*

[2] *Department of CSE, Visiting Professor,*

[3]*Department of ECE, Research Scholar,*

[123] *Shri Venkateshwara University, Gajraula, Amroha (UP) India*

***Abstract*— In the Mobile Ad hoc Networks (MANETs), Routing protocols have a major role. Depending on the route discovery time the Routing Protocols have been classified into Two Major Categories as Reactive and Proactive. . We know today's popularity and more usage of MANETs in every field which also attracts the intruders to sabotage the privacy of the data and will attack on the security. This paper tries to provide the information about the day by day popularity and more usage of MANETs and overall security breaches and possible solutions.**

***Keywords*— MANETs, Security, Security Breaches, Remedies, Routing Protocols, Attacks.**

I. INTRODUCTION

In the MANETS all the autonomous nodes are configured dynamically without any pre-existing routes and without any centralized management system. Depending on the requirements at all the time a new route is established for each node and moreover the data moves freely among all the nodes without any centralized control system. The Nature of Decentralization and dynamic network or route establishment causes a vulnerable to various security attacks which are not common in wired networks. Due to the Dynamic and Temporary route establishment nature of MANETs many researchers have proposed several Safe and secure routing protocols, but the resistance of those proposed and secure routing protocols towards various types of security attacks and efficiency are primary points of concern at all the time in implementing these protocols. Wireless links make MANETs more susceptible to attacks. It is easier for hackers to eavesdrop and gain access to confidential information. It is also easier for them to enter or leave a wireless network because no physical connection is required. They can also directly attack the network to delete messages, inject false packets or impersonate a node. This violates the network's goal of availability, integrity, authentication and nonrepudiation. Compromised nodes can also launch attacks from within a network. Most proposed routing algorithms today do not specify schemes to protect against such attacks.

II. ROUTING PROTOCOLS

An ad hoc routing protocol is a convention, or standard, or set of rules that controls how nodes decide which way to route packets between routing devices in a mobile ad hoc network.

In the MANETs, all the nodes moves freely without knowing their networks topology, so they have to discover network topology on their own. Here every new node will announce about its inclusion in the network and will get the information about its neighbour's broadcast information too. Apart from that each new node will learn how to reach to nearby neighbour's and will provide the rout information about itself to all others.

In a wider sense all the routing protocols have been classified into the following categories.

- On-Demand Routing Protocol (Reactive)
- Table-Driven Routing Protocol (Proactive)
- Hybrid Routing Protocol (Both Proactive and Reactive)
- Hierarchical Routing Protocol (Proactive or Reactive)

A. On-Demand Routing Protocols (Reactive)

In this type of routing protocol the route is established when it is needed. Source node initiates the route discovery phase by flooding the network with Route Request Packets (RRP). When the packet forwarding process is finished then the route is terminated and route information is discarded from the routing table. Reactive protocol Examples are On Demand Distance Vector (AODV) [2], Dynamic Source Routing (DSR) [3], Flow State in the Dynamic Source Routing (FSDSR) and Power – Aware DSR based.

The main disadvantages of these routing protocols are

- Latency Time is very High to find the Route
- Flooding of RRPs may leads to the blocking of networks
- More RRPs from different nodes may cause congestion problem in the network columns.

Some of the existing Reactive/On Demand Routing protocols are:

- Ad-hoc On-demand Distance Vector routing (AODV)
- Dynamic Source Routing (DSR)
- Light-weight Mobile Routing (LMR)
- Associativity Based Routing (ABR)
- The Enhanced On Demand Multicast Routing Protocol (EODMRP)

B. Table-Driven Routing Protocol (Proactive)

The name itself indicates that in this protocol a routing table is maintained which contains the fresh routing information about the destinations and their routes which are updated periodically by the network. Whenever a node needs to communicate, an appropriate best path to the destination is selected for communication depending on the fresh information available in the routing table which is updated periodically. Some of the protocols which comes under this category are Optimized link State Routing Protocol (OLSR)[ ],Babel RFC 6126 and Destination Sequence Distance Vector(DSDV).

The main disadvantages of these routing protocols are

- Data should be maintained for route discovery
- Periodic updates are compulsory in the routing table
- Reaction is very slow on restructuring and failures

Some of the existing proactive/table driven routing protocols are:

- Destination Sequenced Distance Vector routing (DSDV)
- Wireless Routing Protocol (WRP) Cluster Gateway Switch Routing protocol (CGSR)
- Fisheye State Routing (FSR)
- The logical Hypercube-based Virtual Dynamic Backbone protocol (HVDB)

C. Hybrid Routing Protocols (Both Reactive and Proactive)

This type of protocols has the mixed behavior and the combination of advantages and disadvantages of both Reactive and Proactive protocols. Here the routing is initially established with proactive prospect to the nodes by getting the advantage of routing table information. In this way we can save the latency Time for searching the destination nodes. After that directly we can send the packets to the destination nodes. If we combine the two routing protocols then we can overcome the problems of both the routing protocols. The Example of this routing protocol is Zone Routing Protocol (ZRP) , ZRP uses IARP(Intra Zone Routing Protocol) as proactive and IERP(Inter Zone Routing Protocol) as Reactive protocols.
The main disadvantage of this routing protocol is

- Each protocol depends on the other in terms of advantage, disadvantage, delay, congestion etc.

Some of the existing hybrid routing protocols are:

- Temporally Ordered Routing Algorithm (TORA)
- Zone Routing Protocol (ZRP)
- Zone-based Hierarchical Link State (ZHLS)
- Sharp Hybrid Adaptive Routing Protocol (SHARP)
- Optimized Polymorphic Hybrid Multicast Routing Protocol (OPHMR)

D. Hierarchical Routing Protocols

This type of protocols depends on the hierarchy level of the nodes in which networks they resides. Here also the choice of the Reactive or Proactive protocol depends on the node area and situation. The routing is initially established with proactive prospect to the nodes by getting the advantage of routing table information. In this way we can save the latency Time for searching the destination nodes. After that directly we can send the packets to the destination nodes. But here it is compulsory that there should be a proper coordination between the initial levels of establishment and packet transmission. The Examples of these routing algorithms are Cluster Based Routing Protocols (CBRP) and Fisheye State Routing Protocol (FSR)

The main disadvantages of these algorithms are:

- Advantages depend on depth of nesting and addressing schemes.
- Traffic demand reaction depends on meshing parameters.

III. Security Breaches

Many Researchers have concentrated on security breaches and tries to find out the solutions for it. Here are the some solutions discussed by many researchers in view of routing protocol's privacy and security in MANETs.

MANETs Nature which causes the security breaches in routing Protocols [4], [5].

- In the network any node can acts as a router when needed
- There is no centralized control in MANETs
- Each Node can join or leave the network at any time without any restrictions which causes the security and privacy problems
- Capability of multi hop routing puts the network into congestion problem
- By nature MANETs are dynamic and wireless media, So When compare to wire networks wireless links are more vulnerable to many attacks such as spoofing, eavesdropping, Denial of service and black hole attacks etc.
- Because of limited transmission range, when the source and destination are not in range they have to rely on intermediate nodes which causes security breaches.
- Broadcast nature of wireless networks also causes many hidden and exposed security breaches particularly more vulnerable to many attacks.
- Mobility nature of MANETs makes the nodes to change the route frequently which causes routing problems.

IV. Security Attacks

According to the nature of the attacks broadly they are classified into two types of attacks [1].

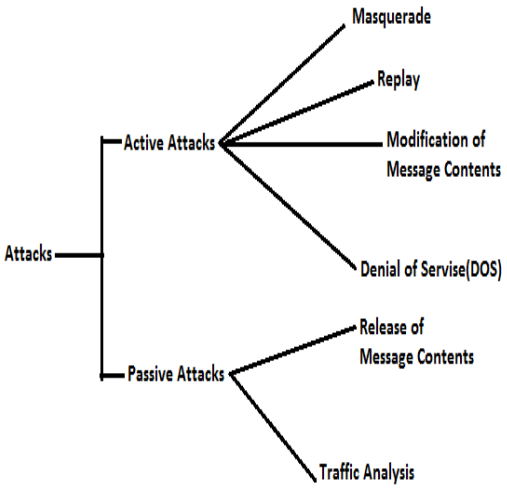

Fig. 1 Types of attacks

A. *Active Attacks*

These types of attacks are very dangerous and need to save the data from these types of attacks. In these types of attacks the data is read and modified according to the willingness of the attackers, and most of the time the functionality of the network goes down. Moreover these attacks are divided into Two Types.

- External attacks: These attacks are carried out by the External Nodes which does not belong to the same Networks.
- Internal attacks: These attacks are carried out by the internal malicious nodes which belong to the same network.

B. *Passive attacks*

In this type of attacks the system is monitored and the hackers will try to gain the information which is transmitted. Passive attacks are very hard to detect as there is no damage or change in the data. The data should be encrypted to avoid these types of attacks.

V. Possible Solutions on the Security Issues

A. *Distributed Operation*

The protocol should be distributed and should not be dependent on any centralized authority. This is beneficial because the nodes can enter and leave the network easily.

B. *Loop Free*

For the efficient functioning of the network, the routing protocol should guarantee that the routes are loop free. This avoids the wastage of bandwidth and computing power. Also, delays are reduced if the routes are loop free.

C. *Demand based Operation:*

To avoid the unnecessary wastage of bandwidth, computing power and battery, the routing protocol should react only when necessary. In other words, the protocol should be reactive.

D. *Unidirectional Link Support*

Unidirectional links are formed in the radio environment. The protocol should use these unidirectional links for the optimal performance of the protocols.

E. *Security*

Security is an important issue in MANETs. MANETs are susceptible to attacks like spoofing. To guarantee the desired behavior in ad hoc routing protocols some security measures are required. Security can be improved by applying encryption and authentication to the routing protocols.

F. *Quality of Service Support*

Quality of Service is an important parameter in the ad hoc routing protocols. The routing protocols should support various QoS. For instance, real time traffic should have low jitter. It should be noted that none of the proposed protocols have all these properties.

G. *Multiple Routes*

The protocol should have redundant routes, so when one link fails an alternative route can be used without initiating route discovery. Also, buffering multiple routes makes the protocol resistant to frequent topology changes.

H. *Power Conservation*

The nodes that form the ad hoc network have very limited resources. One such important resource which is limited is the battery power. The protocols should conserve the battery power of the mobile devices. They should switch to power saving or standby mode when not in use.

I. *Cryptography*

Often, the sender/receiver is an organization. The goal of cryptography is to split a cryptographic operation among multiple users so that some predetermined number of users so that some predetermined number of users can perform desired operation. In organizations, many security-related actions are taken by a group of people instead of an individual so there is a need for guaranteeing the authenticity of messages sent by a group of individuals to another group without expansion of keys and / or messages. To avoid a key management problem and to allow distribution of power, an organization should have one public key. The power to sign should then be shared, to avoid abuse and to guarantee reliability.

J. *Decentralized Authentication Of New Modes*

Two nodes authenticate each other using signed non forgeable certificates issued by virtual trusted CA. Multiple nodes will function collectively as a CA. Authority and functionality of an authentication server is distributed

across k nodes that collaboratively serve and provide authentication services.

K. *Per-Packet And Per-Hop Authentication*

A new node has to be initially authenticated by each of its neighbours to join the network. Once that has been accomplished, each packet sent by the node to its one-hop neighbour is authenticated by the neighbour using a packet authentication tag. The one-hop neighbour then replaces the tag with its own authentication tag and forwards the packet to its neighbour. This next neighbour verifies the new authentication tag as coming from its immediate neighbour and the process is repeated iteratively until the packet reaches its destination. Therefore, each packet is authenticated at every hop. This scheme has the advantage that is resistant to denial of service (DoS) attacks and sessions hijacking attacks such as man-in-the-middle attack.

L. Intrusion Detection In Manets

An effective IDS is a key component in securing MANETs [6], [7]. Two different methodologies of intrusion detection are commonly used: anomaly intrusion detection and misuse intrusion detection. Anomaly-detection systems are usually slow and inefficient and are prone to miss insider attacks. Misused detection systems can't detect new types of attack. Hybrid systems using both techniques are often deployed in order to minimize these shortcomings.

VI. CONCLUSIONS

In this paper we have given the complete overview on Routing protocols and tried to expose the problems and possible remedies in MANETs. . Due to the Dynamic and Temporary route establishment nature of MANETs many researchers have proposed several Safe and secure routing protocols, but the resistance of those proposed and secure routing protocols towards various types of security attacks and efficiency are primary points of concern at all the time in implementing these protocols. In future we will expose the security breaches and remedies in all the layers.

REFERENCES

[1] M.s.Supriya and Mrs.Manju Khari " MANET Security Breaches: Threat to a Secure Communication Platform" International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 2, pp. 45-52 April 2012 .

[2] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, 1999, pp. 90–100.

[3] D. B. Johnson, D. A. Maltz, and J. Broch, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," in In Ad Hoc Networking. Addison-Wesley, 2001, pp. 139–172

[4] Zaiba Ishrat "Security issues, challenges & solution in MANET", ISSN : 0976-8491 (Online) | ISSN : 2229-4333(Print) pp.108-112, IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011.

[5] Jameela Al-Jaroodi "Routing Security in Open/Dynamic Mobile Ad Hoc Networks" The International Arab Journal of Information Technology, Vol 4, No. 1, January 2007, pp. 17-26.

[6] Lidong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Networks Special Issue on Network Security, November/December 1999.

[7] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Adhoc Networks", in Proceedings of the 6th International conference on mobile computing