A Survey – Secure Routing in Mobile Ad hoc network

N.Saravanan[1], K.Pazhanisamy[2]
[1]Department of IT, Thiruvaluvar College of Engg. And Tech., Tamilnadu, India.
[2]Department of CSE, University college of Engineering Villupuram, Tamilnadu, India.
Email:kpsamy09@gmail.com

ABSTRACT - Security in MANET is the most vital concern for the basic functionality of network. One of the most important challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different type of mechanisms has been proposed using different cryptographic techniques to countermeasure the routing attacks against MANET. In this paper we study the routing security issues of MANETs and analyses in detail for different type of attacks.

Keywords - Ad hoc networks, Securing Routing, MANET Security, Routing topology, Attacks

I. INTRODUCTION FOR ROUTING PROTOCOLS

There are different type of routing protocols [10] are used to discover routes and locate the MAC addresses between Ad- hoc wireless nodes. The main goal of ad-hoc network routing protocol is to make optimum and best route establishment between mobile nodes so that message reached to the destination in time. The best route in Ad-hoc wireless communication is that in which bandwidth spending and overhead is less. In ad-hoc networks, there is lack of topology information so that nodes have to discover the topology by transfer hello messages within the network. When new node enters the topology it announces its presence within the network and listens to broadcast announcements from its neighbors.

Routing algorithms have to:

- Maintain routing table reasonably small.
- Select best route for given destination includes fastest, reliable, highest throughput.
- Keep table up-to-date when nodes leave, join or move.
- Little amount of messages/time is required to converge.

II. OVERVIEW OF MANETS ROUTING PROTOCOLS

Mobile Ad-Hoc Network [2] is the rapid increasing technology from the past twenty years. The growth in their popularity is because of the easily deployment, infrastructure less and their dynamic nature. Mobile Ad-Hoc Networks created a new set of demands to be implemented and to provide proficient better end-to-end communication. Mobile Ad-Hoc Networks works on TCP/IP structure to provide the means of communication between communicating work stations. The work stations are mobile and they have limited resources, therefore the traditional TCP/IP model requests to be refurbished or modified, in order to compensate the MANETs mobility to give efficient functionality. Therefore the key research part for the researchers is routing in several network. Routing protocols in MANETs are complicated and attractive tasks, researchers are giving great amount of attention to this key area.

The most important features of MANET are listed some as below:

- MANET can be created without any preexisting infrastructure.
- It follows dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network. It does have mostly limited physical security, and thus increasing security is a main concern.

- Every node in the MANET can support in routing of packets in the network.
- Limited Power and Limited Bandwidth.

Routing protocols can be divided into reactive, proactive and hybrid protocols depending on the routing topology *(Papadimitratos and Haas, 2002)*. Proactive protocols are either distance vector protocols or table-driven. In such protocols, the nodes periodically refresh the existing routing information so that every node can immediately operate with consistent and up-to-date routing tables *Papadimitratos and Haas, 2002*. On the contrast, source-initiated or reactive on demand protocols do not periodically update the routing information *(Hubaux et al., 2001)*. Thus, they create a big overhead when the route is being determined, since the routes are not automatically up-to-date when required. The Hybrid protocols make use of both proactive and reactive approaches. They typically offer the means to switch dynamically between the reactive and modes of the protocol *(Hubauxetal. 2001)*. The hierarchy of these protocols is give bellow.

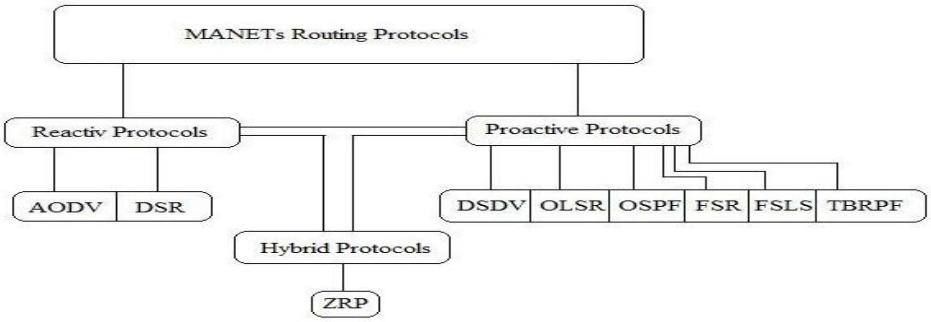

Fig. 1 MANETs Routing Protocols

III. ROUTING ATTACKS IN MANET

The malicious node(s) can attacks in Mobile Ad-Hoc Network using different ways, such as transfer fake messages many times, fake routing information, and advertising fake links to disrupt routing operations. In the following paragraph, current routing attacks and its countermeasures against Mobile Ad-Hoc Network protocols are discussed in detail below.

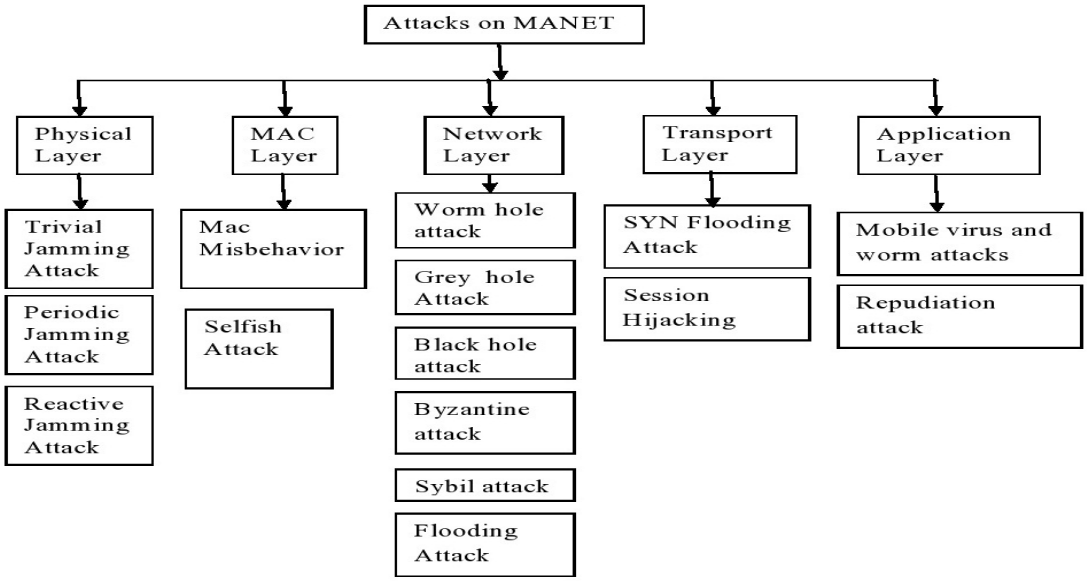

Fig. 2 Classification of attacks on MANET

A. Rushing Attack

It is an unfamiliar attack [1], in which the attacker attempts to be part of routing path to cause the denial of service attack. The attack is directed to reactive protocol only. This attack exploits the property that each node processes just the route request packet for specified identity once.

When rushing attack launched during the route discovery, only a route not longer than two hops is found. As shown in Fig. 3 the source S starts by forward packet to the destination D. The malicious node M when received the route request to D it quickly broadcasts the request to one of the destination neighbor N without any checking for request demand. Finally, the destination received the request from N. So this route request is selected and other discards since each node must process one route request.

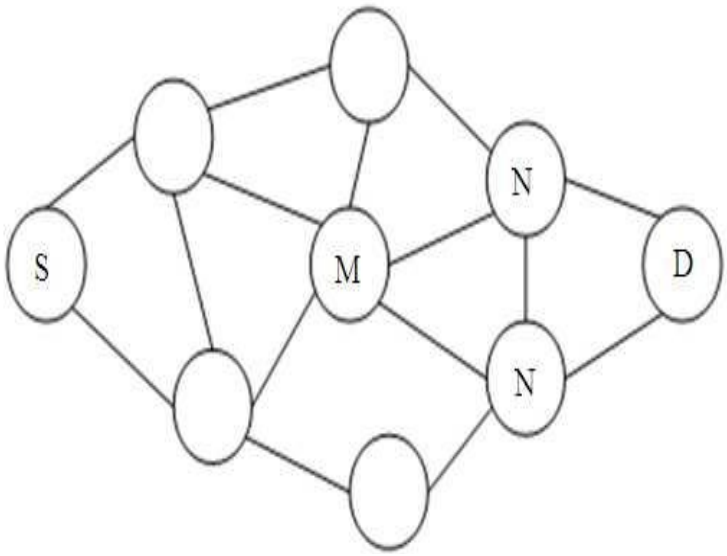

Fig. 3 Rushing Attack

B. Blackhole Attack

In a black hole attack [9] a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be made-up to divert network traffic through the malicious node for eavesdropping, or just to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

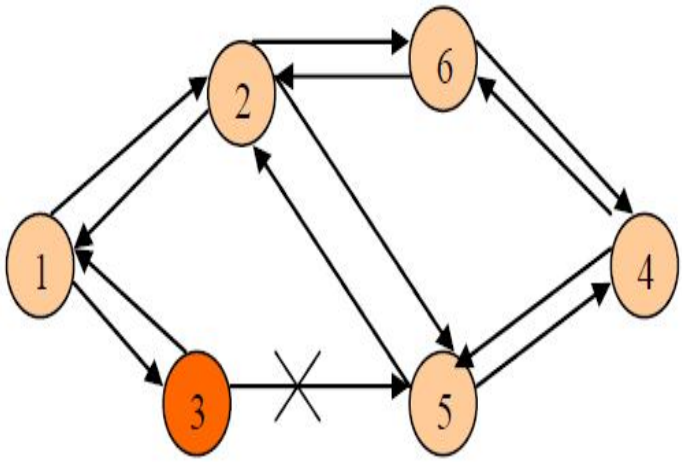

Fig. 4 Black hole attack

Protocol Name	Routing topology	Security requirements	Advantage	Disadvantages	Rushing attack	Black hole attack	Wormhole attack	Jellyfish attack
TARP	Reactive	Availability	Save resources	need to combine to one of the security protocols	Yes	Yes	Yes	Yes
MOSAR	Reactive	Authentication integration and no repudiation	Can balance between security performance and power consuming	The problem of security level classification	No	Yes	Yes	Yes
AODVSEC	Reactive	integration	No computation due to lack of cryptography	Cannot protect request packet	Yes	No	Yes	Yes
SRP	Reactive	Integrity, authentication	no overhead computation in intermediate nodes	Can be attacked with nodes colluding	No	No	Yes	Yes
Ariadne	Reactive	Integrity, authentication	Immune to the wormhole attack	Based on time synchronization which is difficult to implement	No	No	Yes	Yes
SecMR	Reactive	Authentication	Secured multipath route	Overhead for computation in each intermediate nodes	No	No	Yes	Yes
SEDYMO	Reactive	Authentication integration	Prevent attack of modified the hop counts and the non altered field	Overhead for computation in each intermediate nodes	No	No	Yes	Yes
SERA	Reactive	Authentication and integration	Prevent modified attacks for hops number and sequence number	Require loosly synchronization, distribution for authentication vow	No	No	Yes	Yes
APPALLS	Reactive	Integrity, Authentication	Can isolate the misbehaving nodes	Can have problem of wormhole attack	No	No	Yes	Yes
ASRP	Reactive	Authentication and integration	Apply Strong Authentication	Cannot prevent from wormhole attack and selfish node can halt protocol	No	No	Yes	Yes
UBSOR	Reactive	Authentication and integration	strong privacy protection	Cannot handle worm hole attack	No	No	Yes	Yes
SEAD	Proactive	Authentication	Attacker creating routing loops can be prevented	Does not cope with wormhole attacks	No	No	Yes	Yes
Secure OLSR	Proactive	Authentication	Prevent play attacks and modified the routing path	Vulnerable to wormhole attack	No	No	Yes	Yes
SMRR	Proactive	Integrity and confidentiality	Depend on Trust nodes to relay the packets	Can not apply in low density network	No	No	Yes	No
STOP	Reactive	Authentication integration and no repudiation	Can select path depends on performance	Need key management and overhead for encrypt the packets	No	No	No	No

Table 1 Summary for secure routing protocols properties

C. Jellyfish Attack

In jellyfish attack [2], the attacker attacks in the network and introduce unwanted delays in the network [7]. In this type of attack, the attacker node first get access to the network, once it get into the network & became a division of the network. The attacker then proposed the delays in the network by delaying all the packets that it receives, once late are propagated then packets are released in the network. This enables the attacker to produce highly end-to-end delay,

high delay jitter and considerably affect the performance of the network. So above provide table 1 for a few analyses of secure routing protocols properties [1] and attacks within the MANETs.

D. Wormhole Attack

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then maintain on hearing the network, record the wireless data. Shows the two attackers placed themselves in a strong strategic location in the network.

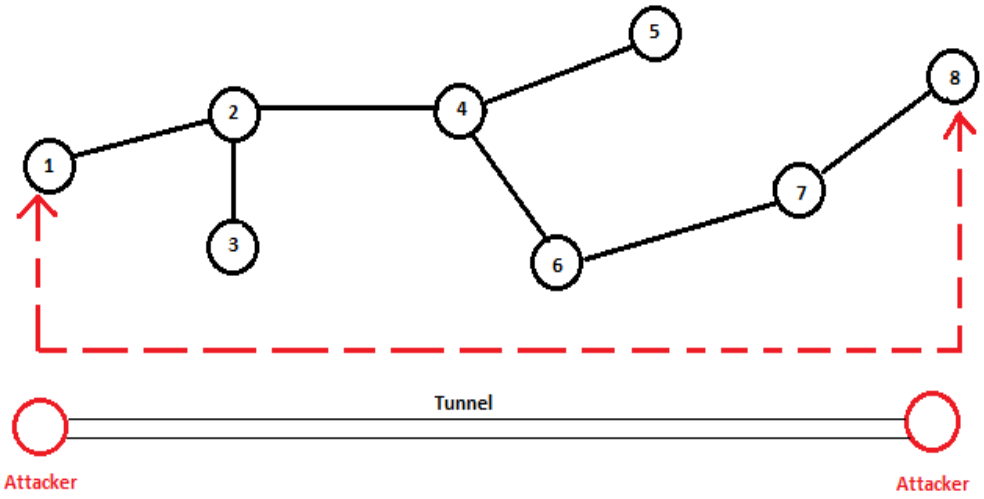

Fig. 5 Wormhole attack

In wormhole attack [2], the attacker gets themselves in strong strategic location in the network. They make the use of the position i.e. they have shortest path between the nodes as shown in the Fig. 5 above. They advertise their path letting the other nodes in the network to know they have the shortest path for pass on their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network [6].When the attacker nodes create a direct link between each other note in the network, wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such location the attack is known as out of band wormhole [7].

The other type of wormhole attack is identified as in band wormhole attack [7]. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. Band wormhole attack is potentially very much harmful and is the most preferred choice for the attacker.

IV. CONCLUSIONS

This paper discusses common possible attacks on different type of protocols being used in MANETs. We have tried to evaluate them so as to prevent the attacker to intrude in wireless networks. There are many of techniques with which, one can easily detect most of the attacks. One can select them in accordance with the protocol being used in the network. However, no protocol is fully secure from attacks being encountered in the MANETs. Hence, one should choose a combination of techniques intelligently to avoid any attack and make the network fully secure.

Future research work should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a Mobile Ad-Hoc Network environment. Furthermore, each proposed solution can work only with a specific attack and is still vulnerable to unexpected attacks.

REFERENCES

1. Salwa Aqeel Mahdi, Mohamed Othman, Hamidah Ibrahim, Jalil Md. Desa and Jumat Sulaiman" Protocols For Secure Routing And Transmission In Mobile Ad Hoc Network: A Review" Journal of Computer Science 9 (5): 607-619, 2013.
2. IRSHAD ULLAH, SHOAIB UR REHMAN" Analysis of Black Hole attack on MANETs Using different MANET routing protocols"sep 2010
3. M .Nasir Iqbal, Junaid A.Khan, Farooq Umer, Nadeem Javaid, Izhar-ul-Haq, Mustafa Shakir" Security Enhancement of Pro-active Protocols in Mobile Ad-hoc Networks"2013
4. Rashid Hafeez Khokhar, Md Asri Ngadi & Satria Mandala" A Review of Current Routing Attacks in Mobile Ad Hoc Networks" 2006
5. Shekhar Saini, Rajesh Kumar" *Comparison of layerwise attacks in MANETs" 2013*
6. H.L.Nguyen, U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks", International Conference on System and Networks and International Conference on Mobile Communications and Learning Technologies (ICN/ICONS/MCL 2006), pp.149-149, April, 2006.
7. V.Mahajan, M.Natue and A.Sethi,"Analysis of Wormhole Intrusion attacks in MANETs", IEEE Military Communications Conference, pp. 1-7, Nov, 2008.
8. F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing", Vol. 35, pp. 22-26, Apr, 2002
9. Sarvesh Tanwar, Prema K.V**. "**Threats & Security Issues in Ad hoc network: A Survey Report"Jan2013
10. M .Nasir Iqbal, Junaid A.Khan, Farooq Umer, Nadeem Javaid, Izhar-ul-Haq, Mustafa Shakir" Security Enhancement of Pro-active Protocols in Mobile Ad-hoc Networks"2013
11. P.A.R Kumar, S.Selvakumar, "Distribute Denail-of-Service (DDoS) Threat in Collaborative Environment – A survey of DDoS Attack Tools and Traceback Mechanism" IEEE International Advance Computing Conference (IACC 2009), pp. 1275-1280, March, 2009.
12. L.Zonglin, H.Guangming, Y.Xingmiao, " Spatial Correlation Detection of DDoS attack" International Conference on Communication, Circuits and System (ICCCAS 2009), pp. 304-308, July, 2009.
13. X.Y.Zhang, Y.Sekiya, Y.Wakahara, "Proposal of a method to detect black hole attack in MANET", international Syposium on Autonomous Decentralized System (ISADS 2009), pp. 1-6, March, 2009
14. Jeremy J. Blum, Andrew Neiswender and Azim Eskandarian,"Denial of Service Attacks on Inter-Vehicle Communication Networks" in 11th IEEE conference on Intelligent Transportation Systems, 2008, pp 797-802
15. Nikos Komninos, Dimitris Vergados, Christos Douligeris" Layered security design for mobile ad hoc networks" 2006