ISSN: 2321-7782 (Online)
Special Issue, December 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Survey in Handling Routing Attacks over MANETs

Shakila. M[1]
PG student
Department of Computer Science and Engg
Velammal Engineering College
Chennai - India

Prittopaul. P[2]
Faculty
Department of Computer science and Engg
Velammal Engineering College
Chennai - India

Abstract: ***Mobile Ad-hoc networks do not have any centrally controlled monitor points to oversee the formation of the networks or the communication. They are dynamic in nature and do not need an infrastructure to create a network. Due to these behaviors, these networks are more vulnerable for attacks. The attacks can end in data loss or data corruption. Without any prior notice, nodes can join or leave network without any set frequency. In order to learn and create loop-free paths, the process of routing plays the most important role. In this paper, issues related to MANET in handling the attack with the responses through different systems are analyzed with their reactive and proactive protocols. Hence in order to provide more accurate response in the process of attack handling, we have evaluated risk through Fuzzy multi-level security and Mathematical theory of evidence.***

Keywords: Mobile Ad Hoc Networks, Routing Protocols, Attacks, Security Issues in MANETs.

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a self-configuring infrastructure-less network of mobile devices connected by wireless [10]. It is a collection of nodes, which forms temporary network without any centralized system, access points or base station. These nodes generally have limited transmission range, so that each node needs the assistance of its neighboring nodes to forward packets. Devices in a MANET are free to move independently in any direction, and can change their links to other devices frequently. The devices forward traffic unrelated to its own, and therefore can be acting as a router. Routing is the process of selecting best paths in a network [9]. It is necessary to perform the functions like, to act as a gateway, learn and advertise loop free paths based on routing protocols.

The major challenge in establishing a MANET is maintain devices to continuously sustain the information required to properly manage the route traffic. Such networks shall be able to operate among them or even be connected to the larger Internet.

Application places spread across like: emergency and rescue operations, conference or campus settings, car networks, personal networking, etc.

II. ISSUES IN MANET

Mobile Ad hoc Networks (MANET) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Although there are many attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. Routers believe their neighbors. If its neighbors lie, Router can be deceived about the proper route thus allowing eavesdropping, Hijacking, Denial of Service etc., The malicious node(s) causes attacks in MANET using different paths, like sending fake messages numerous times, passing fake routing information, advertising the fake links to disrupt routing methods. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail.

Types of Attacks:

ATTACK	DESCRIPTION
Flooding attack	In flooding attack, attackers exhaust the network resources like bandwidth and to consume a node's resources, like computational power and battery power or to disrupt the routing operation to cause severe decrease in network performance
Black-hole attack	In black-hole attack, a malicious node send fake routing information to claim that it has an optimum route and cause other nodes to send data packets via the attacker
Wormhole attack	A wormhole attack is one of the most sophisticated and severe attacks in MANETs. Pair of colluding attackers record their packets at one location and replay them at another location by a private high speed networks
Colluding mis-relay attack	In colluding mis-relay attack, multiple attackers work in collusion to modify and drop routing packets to disrupt routing in MANET
Denial of service attack	In denial of Service attack, node generate frequent unnecessary route request to make network resources unavailable to other nodes.

III. EXISTING SYSTEMS AND CHALLENGES

As already stated, the specific characteristics of MANETs impose many challenges to network protocols on layers of the network protocol.

Types of routing protocols [11]:

Routing protocol	Description
Table-Driven(pro-active)	Periodically updated routing tables maintain destination routes
On-Demand (reactive)	Routes are set up on demand during transmission.
Flow-oriented routing	This type of protocols finds a route on demand by following present flow
Hybrid (both proactive and reactive)	Combines the advantages of proactive and reactive routing
Hierarchical routing protocols	Choice of proactive and of reactive routing depends on the hierarchic level in which a node resides

Physical layer should deal with rapid changes in link architectures. The media access control (MAC) layer should be allowing fair access, try to minimize the packet collisions and should deal with the hidden as well as exposed terminals. At the network layer, nodes need to cooperate to calculate paths. While transport layer must be in a stance to handle packet loss and also the delay characteristics that may differ from wired networks.

Applications should handle possible scenarios of disconnections and reconnections. Moreover, all network protocol developments need to integrate with traditional networks and take into account possible security problems. In the following sections, technological challenges and possible solutions related to routing, security and node cooperation are covered in more detail.

Routing in mobile ad hoc networks are characterized by a multi-hop network topology that can change frequently. Efficient routing protocols are needed to establish communication paths between nodes, avoiding excessive control traffic overhead or computational burden on the power constrained devices a large number of solutions have already been proposed, some of them being subject to standardization within the Internet Engineering Task Force (IETF).

To this end, these protocols exchange routing control information periodically and on topological changes. These protocols, which are called proactive routing protocols, are typically modified versions of traditional link state or distance vector routing protocols encountered in wired networks, adapted to the specific requirements of the dynamic mobile ad hoc network environment.

IV. LITERATURE REVIEW

A. *Routing Security in Mobile Ad Hoc Networks*

In the entire wireless network, we can see the routing process plays the most important role. The problem of security in MANET is a well-known and a traditional problem. In this paper [1], we concentrate on solution for one of the attack type "Black-Hole Attack" which is proven to be easily deployable in On-demand Distance Vector Routing Protocol.

AODV is Ad hoc on-demand routing protocol that creates routes only when desired by the source node. It initiates a route discovery process and maintains routes. In black hole attack, a malicious node can advertise itself as having the shortest path to the node. The malicious node can easily misroute in the entire network traffic, disrupting the correct functioning of the protocol.

One possible solution is to disable the reply from intermediate nodes and making all the reply sent out only by destination

B. *Optimized Link State Routing Protocol(OLSR)*

It provides optimal routes in terms of number of hops that are available immediately whenever needed. It is best suitable for big and complex networks. OLSR is based on Link State routing algorithm and is a pro-active routing protocol (table-driven) using periodic exchange [2]. Optimal routes provided in terms of number of hops. Figure 2 below shows the multipoint relay selection around node N. Retransmissions overhead is reduced by using the Multipoint Relays (MPR), the messages are broadcasted only to MPR nodes.

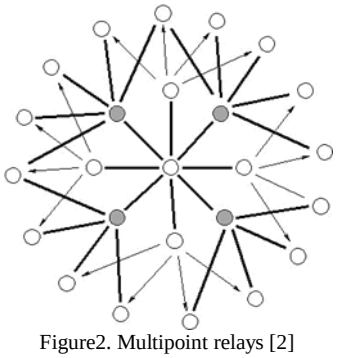

Figure2. Multipoint relays [2]

C. Secure Efficient Distance Vector Routing For Mobile Ad Hoc Networks(SEAD)

This is a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. It is used to support use with nodes of limited CPU processing capability, and to defend against Denial of-Service attacks in which an attacker causes other nodes to consume excess network bandwidth and processing time. One-way hash functions are used to be efficient

Secure Efficient Ad hoc Distance vector routing protocol (SEAD), is robust against multiple uncoordinated attackers[3]. It supports nodes with limited CPU processing capability to guard against the common Denial of-Service attacks. It is used in part with Destination-Sequenced Distance-vector for designing trusted environment. In distance vector routing, each router maintains a routing table.

D. ARIADNE

Secure On-Demand Routing Protocol for Ad Hoc Networks The design and performance evaluation of a new secure on-demand ad hoc network routing protocol called Ariadne is proposed in this paper [4]. It prevents attackers or compromised nodes from tampering with the uncompromised routes that consist of uncompromised nodes. This also prevents many types of Denial-of-Service (DOS) attacks. In addition to this, ARIADNE is even efficient by using only highly efficient symmetric cryptographic primitives.

E. Secure Wireless Ad Hoc Routing

This reviews attacks performed on ad hoc networks and discusses the current available approaches to establish cryptographic keys in ad hoc networks. When a powerful wormhole attack is applied against an on-demand routing protocol, they can be mounted by tunneling each ROUTE REQUEST packet directly to the target node of the REQUEST. This type of attacks prevents any node from discovering their routes that are more than two hops long.

Hence in this study we make use of specifically two types of packet leashes namely "geographical" and "temporal". The main idea is by authenticating any one, a precise timestamp or location information combined with a loose timestamp can be achieved. So a receiver can determine if the packet has travelled a unrealistic range

Given the precise time synchronization, some efficient broadcast authenticators based entirely on symmetric primitives is constructed [5]

Private-key distribution is more challenging than public-key distribution because protocols for key distribution must ensure the secrecy of such keys. It expects the cooperation between two attacking nodes. One attacker records routing traffic at one point and tunnels it to another point in the network .Then selects and injects tunnel traffic back into the network. This attack prevents any node from discovering routes more than two hops long. A solution to this attack is Packet leashes. It uses timed efficient Stream Loss-Tolerant Authentication Protocol (TESLA) for authenticating routing messages.

F. Strategies for enhancing routing security in protocols for mobile ad-hoc networks

The absence of any central authority makes MANETs more vulnerable to various forms of attacks. Potential attacks against routing fall into two groups:

- Passive attacks-monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks.
- Active attacks-attacker tries to bypass or break into secured systems.

This approach [6] comprises of two systems the "External attack prevention system" (EAPS) and "Internal Attack Detection and Correction System" (IADCS)

- Proactively prevents external attacks by using an authentication scheme
- It assumes mutual trust among all network nodes
- Enables ease of key distribution and authentication
- The nodes are computationally powerful
- IADCS performs by having mutual suspicion among nodes
- It assumes, compromised nodes do not work in team
- Each node has some knowledge to detect Misbehavior

G. Fuzzy Multi-Level Security

There is always inherent uncertainty and risk in access control decisions. This concept details by showing how the Bell–Lapadula model based, Multi–Level Security (MLS) access control model can be used to develop a risk-adaptive access control model.

Access control is one of the mechanisms used to manage the risk. Multi–Level Security (MLS) access control model used to develop a risk-adaptive access control model. It addresses [7] inherent uncertainty and risk in access control decisions. Risk associated with its access is quantified by Fuzzy MLS model. Quantified Risk–Adaptive Access Control in figure 3 below is used to determine the probability and the value of damage. (QRAAC)

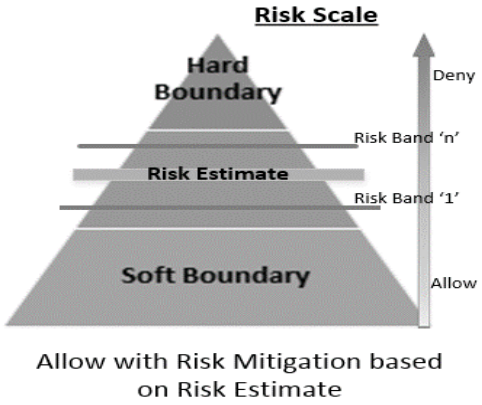

Figure3. QRAAC

H. Mathematical Theory of Evidence

None of the formal methods are able to provide a solution to the problem of representing the security concerns faced by the MANETS. Dempster Shafer theory of mathematical evidence is the only appropriate approach [8] that can be used to formally represent the security concerns in MANETS. Hence, a hybrid approach involving D-S theory of mathematical evidence can be deployed in this domain.

Dempster-Shafer mathematical theory of evidence [13] enables us to present subjective knowledge (retrieved from previous experience) and objective evidence (obtained from observation) with probable reasoning.

The probability that "the detected attack is X" is indicated by a "confidence interval",

$$[\text{Belief}_i(X), \text{Plausibility}_i(X)] \qquad (1)$$

The lower bound of the confidence interval is the belief confidence, which accounts for all evidence Ek that supports the given proposition "attack X".

$$\text{Belief}i(X)=\sum^{m} i(E_k) \qquad (2)$$
$$E_k \subseteq X$$

The upper bound of the confidence interval is the plausibility confidence, which accounts for all the observations that do not rule out the given propagation.

$$\text{Plausibility}i(X)=1-\sum^{m} i(E_k) \qquad (3)$$
$$E_k \cap X=\varphi$$

The main disadvantages behind this theory are as follows:

- Associative: The order of the received information does not impact the result.
- Non-weighted: All evidences are trusted equally.

V. CONCLUSION

The MANET is an emerging research area with many practical applications .However this presents a greater security problem due to its fundamental characteristics like open medium , distributed cooperation, dynamic topology, constrained capability and absence of central system. Routing security plays an important role in the entire network. But it is still a nontrivial problem.

In this paper, the routing security issues of MANET have been studied and several attacks are discussed that can be employed against MANET and a plausible solution is proposed.

References

1. H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks,"IEEE Comm. Magazine,vol. 40, no. 10, pp. 70-75, Oct. 2002,vol. 40, no. 10, pp. 70-75, Oct. 2002.
2. T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol,"Network Working Group,2003.
3. Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks, Vol. 1, no. 1, pp. 175-192, 2003.
4. Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, Vol. 11, no. 1, pp. 21-38, 2005.
5. Y. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing,"IEEE Security and Privacy Magazine,vol. 2, no. 3, pp. 28-39, May/June 2004.
6. L. Venkatraman and D. P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks," J. Parallel Distributed Comp., 2002.
7. P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger, "Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control,"Proc. 28th IEEE Symp. Security and Privacy,2007.
8. G. Shafer,A Mathematical Theory of Evidence.Princeton Univ., 1976.
9. http://en.wikipedia.org/wiki/Routing
10. http://en.wikipedia.org/wiki/Mobile_ad_hoc_network
11. http://en.wikipedia.org/wiki/List_of_ad_hoc_routing_protocols
12. http://en.wikipedia.org/wiki/Optimized_Link_State_Routing_Protocol
13. https://www.google.co.in/search?q=2-77-1372411735-5.+Eng-Intelligent&oq=2-77-1372411735-5.+Eng Intelligent&aqs=chrome..69i57j69i59.1659j0j9&sourceid=chrome&espv=210&es_sm=93&ie=UTF-8

