Manet : Overview

Sandip Shirgave [1]
(MECSE First Year)
[1] Department Of Computer Science ,SKN Sinhgad College Of Engineering ,Korati ,Maharastra,
Dist : Solapur 413 304 India

Abstract
Mobile Ad hoc networks, also known as MANETs. Mobile Ad hoc Networks (MANET) are having dynamic nature of its network infrastructure and it is vulnerable to all types of attacks. Among these attacks, the routing attacks getting more attention because its changing the whole topology itself and it causes more damage to MANET. Even though there exist several intrusion response techniques to mitigate such critical attacks, existing solutions typically attempt to isolate malicious nodes based on binary or naı¨ve fuzzy response decisions. In this paper, I classify the architectures for intrusion detection systems (IDS) that have been introduced for MANETs. Current IDS's corresponding to those architectures are also reviewed and compared. I then provide some directions for future work.[1]
.

Keywords: MANET, Wireless Networks, Ad hoc Networking, Routing Protocol**.**

1. Introduction

In the recent years, one could assist to a spectacular growth in the use of wireless equipments. The number of mobile devices such as PDAs, mobile phones laptops, is also tremendously increasing. To ensure the connectivity between all these devices, ad hoc networks appear to be a promising solution. An ad hoc network is a collection of wireless mobile nodes, which communicate together without the assistance of any fixed nor central infrastructure. MANET an autonomous collection of mobile nodes forming a dynamic wireless network. The administration of such a network is decentralized, *i.e.* each node acts both as host and router and forwards packets for nodes that are not within transmission range of each other. A MANET provides a practical way to rapidly build a decentralized communication network in areas where there is no existing infrastructure or where temporary connectivity is needed, *e.g.* emergency situations, disaster relief scenarios, and military applications. There exist many intrusion response mechanisms for routing attacks. The existing techniques usually attempt to isolate the malicious nodes from the topology there by causing the partition of network topology. Methods such as binary responses may result in the unexpected network partition,

causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET.

A MANET with the characteristics described above was originally developed for military purposes, as nodes are scattered across a battlefield and there is no infrastructure to help them form a network. In recent years MANETs have been developing rapidly and are increasingly being used in many applications, ranging from military to civilian and commercial uses since setting up such networks can be done without the help of any infrastructure or interaction with a human such as search-and-rescue missions, data collection, and virtual classrooms and conferences where lap tops, PDA or other mobile devices share wireless medium and communicate to each other. As MANETs become widely used, the security issue has become one of the primary concerns. For example, most of the routing protocols proposed for MANETs assume that every node in the network is cooperative and not malicious
Therefore, only one compromised node can cause the failure of the entire network.

.

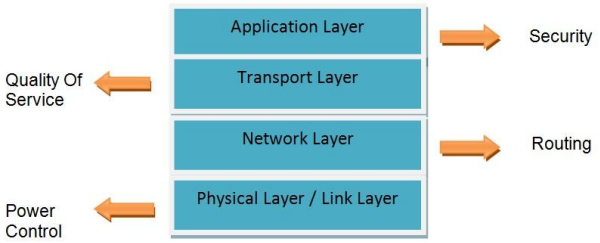
2.Characteristics Of MANET

1.Network is not depending on any fix infrastructure for its operation.
2.Multi-hop routing
3. Dynamic network topology
4. Device heterogeneity
5.Bandwidth constrained variable capacity links
6.Limited physical security
7. Network scalability
8.Self-creation, self-organization and self-administration.[2]

.

3. MANET Challenges

The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design.



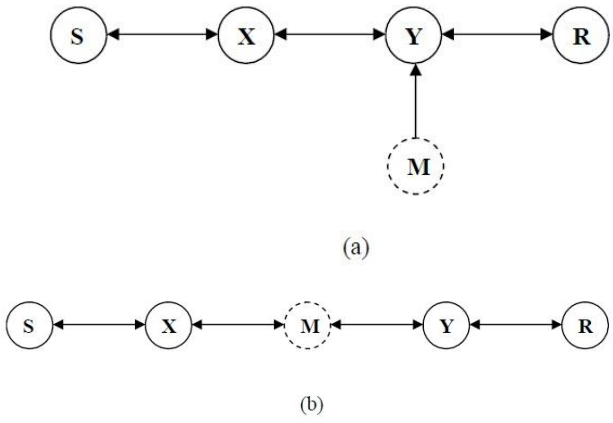


FIG: ROUTING ATTACK

Challenges

A. Absence of Infrastructure
B. Lack of Centralized monitoring
C. Security and Reliability
D. Poor Transmission Quality
E. Dynamically changing network topology
F. Power Consumption
G. Limited physical security

4.Security Threats in Network Layer

In MANET, the nodes also function as routers that discover and maintain routes to other nodes in the network. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network.

A number of attacks in network layer have been identified and studied in security research. An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow. For example, as shown in the following *(a) and (b)* in the next page, a malicious node ***M*** can inject itself into the routing path between sender ***S*** and receiver ***R***.

Attacks on Particular Routing Protocol

1) **AODV {** Ad-hoc On-demand Distance Vector (AODV) }
2) **DSR {** Dynamic Source Routing (DSR) }
3) **ARAN {** Authenticated Routing for Ad-hoc Networks (ARAN) }

5. Other Advanced Attack[3]

A. Blackhole Attack

An attacker creates forged packets to impersonate a valid mesh node and subsequently drop packets. The attracting packets involve advertising routes as low-cost. In networking, black holes refer to places in the network where incoming traffic is dropped without informing the source that the data did not reach its intended recipient. In Black hole. Attacks a node uses the protocol and advertises itself as having the shortest path to the destination node where the packet is destined to.

B. Greyhole Attack

Grey Hole is a node that can switch from behaving correctly to behaving like a black hole. This is done to avoid detection. Some researchers discussed and proposed a solution to a black hole attack by disabling the ability for intermediate nodes to reply to a Route Reply (RREP); only the destination is allowed to reply.

C. Wormhole Attack

In a wormhole attack, an attacker forwards packets through a high quality out-of-band link and replays those packets at another location in the network.

For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric. It is also possible for the attacker to forward each

bit over the wormhole directly, without waiting for an entire packet to be received. An attacker can create a wormhole even for packets not addressed to itself, since it can hear them in wireless transmission and tunnel them to the attacker at the opposite end of the wormhole.

6.PROTOCOLS COMMONLY USED FOR MANET'S

A. Table-driven (proactive) routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. The main disadvantages of such algorithms are:

1. Respective amount of data for maintenance.
2. Slow reaction on restructuring and failures.

Examples of proactive algorithms are:

- B.A.T.M.A.N– Better approach to mobile AD-Hoc networking.
- OLSR Optimized Link State Routing Protocol RFC3626.
- BABEL, a loop-avoidance distance-vector routing protocol RFC 6126.

B. On-demand (reactive) routing

This type of protocols finds a route on demand by flooding the network with Route Request packets. The main disadvantages of such algorithms are:

1. High latency time in route finding.
2. Excessive flooding can lead to network clogging.

Examples of on-demand algorithms are:

- Admission Control Enabled On Demand Routing (ACOR)
- Ad Hoc On-Demand Distance Vector(AODV) (RFC3561)
- Dynamic Source Routing (RFC 4728)
- Flow State In The Dynamic Source Routing.
- Dynamic Manet On-Demand Routing (RFC 4728)
- Power-Aware DSR-based

C. Flow-oriented routing

This type of protocols finds a route on demand by following present flows. One option is to unicast consecutively when forwarding data while promoting a new link. The main disadvantages of such algorithms are:

1. Exploring new routes without prior knowledge takes a long time
2. May refer to entitative existing traffic to compensate for missing knowledge on routes.

Examples of flow-oriented algorithms are:

- IERP (Interzone Routing Protocol/reactive part of the ZRP)
- RDMAR (Relative-Distance Micro-discovery Ad hoc Routing protocol)

D. Hybrid (both proactive and reactive) routing

This type of protocol combines the advantages of proactive and reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice of one or the other method requires predetermination for typical cases. The main disadvantages of such algorithms are:

1. Advantage depends on number of other nodes activated.
2. Reaction to traffic demand depends on gradient of traffic volume.

Examples of hybrid algorithms are:

- ZRP (Zone Routing Protocol) ZRP uses IARP as pro-active and IERP as reactive component.

E. Hierarchical routing protocols

With this type of protocol the choice of proactive and of reactive routing depends on the hierarchic level in which a node resides. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding on the lower levels. The choice for one or the other method requires proper attributation for

respective levels. The main disadvantages of such algorithms are:

1. Advantage depends on depth of nesting and addressing scheme.
2. Reaction to traffic demand depends on meshing parameters.

Examples of hierarchical routing algorithms are:

- CBRP (Cluster Based Routing Protocol)
- FSR (Fisheye State Routing protocol)

F. AODV (Ad Hoc On-Demand Distance Vector Routing)

It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. When the valid route is not known by the source node, it initializes a route discovery process by broadcasting a Route Request (RREQ) to its neighbors. Each node discards Route Requests (RREQs) it has already seen by checking the Broadcast ID and the Sequence Number which had been included into the Route Request (RREQ) .

G. DSR (Dynamic Source Routing)

Determining source routes requires accumulating the address of each device between the source and destination during route discovery. The accumulated path information is cached by nodes processing the route discovery packets. The learned paths are used to route packets. To accomplish source routing, the routed packets contain the address of each device the packet will traverse .

H. Others

- IMEP (Internet Manet Encapsulation Protocol)
- MMARP (Multicast Manet Routing Protocol)

7.Future Directions

Significant research in MANET has been ongoing for many years, but still in an early stage. Existing solutions are well-suited only for specific attack. They can cope well with known attacks but there are many unanticipated or combined attacks remaining undiscovered. Resource consumption DoS attack is still unclear to the researchers. More research is needed on secure routing protocol, robust key management, trust based systems, integrated approaches to routing security, data security in different level and cooperation enforcement. Existing routing protocols are subject to a variety of attacks that can allow attackers to influence a victim's selection of routes or enable denial-of service attack. So, necessity of secure routing protocol is inevitable. Cryptography is one of the most common security mechanisms and its strength relies on the secure key management.

.

References

[1] Risk-Aware Mitigation for MANET Routing Attacks [Ziming Zhao, Student Member, IEEE, Hongxin Hu, Student Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, and Ruoyu Wu, Student Member, IEEE]2012

[2] Challenges in Mobile Ad Hoc Networks:Security Threats and its Solutions[Miss.Dhara N. Darji, Assistant ProfessorGanpat University]

[3] Survey of Attacks on Mobile Ad-hoc Wireless Networks-Vikas Solomon Abel[Information and Communications Department, University of Trinidad and Tobago, Trinidad 2011]

[4]Security Threats in Mobile Ad Hoc Network [Kamanshis Biswas and Md. Liakat Ali]

[5] A Study of Intrusion Detection Systems in MANETs[Umesh Prasad Rout C V Raman Computer Academy, Bhubaneswar, India]