CLASSIFICATION OF SECURITY ATTACKS IN MANET

Pankaj Chaudhary*1, Sachin Chaudhary*2

*Department Of CSE, J.B.Institute Of Technology, Dehradun, Shankarpur, Dehradun(India)
*‘DIT University, Makkawala Green, Rajpur road, Dehradun(India)

ARTICLE INFO

Corresponding Author: Pankaj Chaudhary
Department Of CSE, J.B.Institute of Technology, Dehradun, Shankarpur, Dehradun India

Keywords: - MANETS, Security, Cryptography, Active,passive

ABSTRACT

Mobile ad hoc networks (MANETs) is defined as a collection of large number of mobile nodes that build temporary network without aid of any existing network infrastructure or central access point. Each node participating in the network acts both as host and a router and must therefore is willing to forward to packets for other nodes. The characteristics of MANETs such as: dynamic topology, node mobility, provides large number of degree of freedom and self-organizing capability of that make it completely different from other network. Due to the nature of MANETs, to design and development of secure routing is challenging task for researcher in an open and distributed communication environments.

INTRODUCTION

Wireless cellular system has been in use since 1980s. Wireless system operates with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to other. In wireless system the device communicate via radio channel to share resource and information between devices.

Due to presence of a fixed supporting structure, limits the adaptability wireless system is required easy and quick deployment of wireless network. Recent advancement of wireless technologies like Bluetooth [3], IEEE 802.11 [4] introduced a new type of wireless system known as Mobile ad-hoc network (MANETs) [1, 2, 5, 6], which operate in the absence of central access point. It provides high mobility and device portability's that enable to node connect network and communicate to each other. It allows the devices to maintain connections to the network as well as easily adding and removing devices in the network. User has great flexibility to design such a network at cheapest cost and minimum time.

MANETs has shows distinct characteristics, such as:
- Weaker in Security
- Device size limitation
- Battery life
- Dynamic topology
- Bandwidth and slower data transfer rate

MANETs has shows distinct security goals, such as:
- Authentication
- Integrity
- Confidentiality
- Non-Repudiation

A mobile ad hoc network has following features:

A. Autonomous Terminal

In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other, since there is no background network words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.

B. Distributed Operation

For the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

C. Multihop Routing

Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multi hop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

D. Dynamic Network Topology

Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly.

E. Light-weight Terminal

In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.

APPLICATION

With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining
importance with the increasing number of widespread applications. Ad hoc networking can be applied anywhere where there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use.

Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment.

It includes:
- Military Battlefield
- Sensor Networks
- Commercial Sector
- Medical Service
- Personal Area Network

Fig 1: Application of MANETs

ROUTING IN MANETS

Routing in mobile ad hoc networks faces additional problems and challenges when compared to routing in traditional wired networks with fixed infrastructure. There are several well-known protocols in the literature that have been specifically developed to cope with the limitations imposed by ad hoc networking environments. The problem of routing in such environments is aggravated by limiting factors such as rapidly changing topologies, high power consumption, low bandwidth and high error rates. Most of the existing routing protocols follow two different design approaches to confront the inherent characteristics of ad hoc networks, namely the table-driven and the source-initiated on-demand approaches. The following sections analyze in more detail these two design approaches, and briefly present example protocols that are based on them.

- Table-driven Ad hoc Routing Protocols
- Destination-Sequenced Distance-Vector Routing (DSDV)
- Optimized Link State Routing (OLSR)
- Source-initiated On-demand Ad hoc Routing Protocols
- Ad hoc On-demand Distance Vector Routing (AODV)
- Dynamic Source Routing (DSR)

PRACTICAL IMPLEMENTATIONS OF MANET DESIGNS

Mobile Adhoc Networks can be practically classified into four major categories:
- Table-Driven (Proactive)
- On-Demand (Reactive)
- Dynamic Source Routing Protocol
- Adhoc On-Demand Distance Vector Routing

SECURITY PROBLEM WITH EXISTING AD HOC ROUTING

PROTOCOLS The main assumption of the previously presented ad hoc routing protocols is that all anticipating nodes do so in good faith and without maliciously disrupting the operation of the protocol [19]. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like ad hoc networks. In ad hoc network the routing function can be disrupted by internal or external attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes [14]. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Internal attackers having capability to complete access the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers.

A. Security Goals
- Authentication
- Confidentially
- Integrity
- Availability
- Non-repudiation
- Access Control

VULNERABILITY IN MANETS Malicious and selfish nodes are the ones that fabricate attacks [14] against physical, link, network, and application layer functionality. Current routing protocols are exposed to two types of attacks:
- Active attacks
- Passive attacks

A. Active Attacks

Spoofing, Fabrication, Wormhole Attack, Modification, Denial of Service, Sinkholes, Sybil Attack Eavesdropping, traffic analysis, monitoring Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. These attacks can be classified into further following types:

1. Spoofing: Spoofing occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather [2].
2. Fabrication: The notation “fabrication” is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [5].
3. Wormhole Attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols.
4. **Modification:** The attacker performs such attacks targeted to integrity of data, by altering packet or modifying packets.

5. **Denial of Service:** This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks.

6. **Sinkholes:** In a sinkhole attack, a compromised node tries to attract the data to it from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on Adhoc networks such as AODV by using flaws such as maximizing the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate. The problem of sinkhole attack can be much.

7. **Sybil Attacks:** Malicious nodes in a network may not only impersonate one node, they could take up the identity of a group of nodes, and this attack is called the Sybil attack. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from point A to point B. A consequence of this is that attackers have harder time to destroy the integrity of information. However, if a single malicious node is able to represent several other nodes, the effectiveness of these measures is significantly degraded.

   The attacker may get access to all the data or may alter all packets in the same transmission so that the destination node/s cannot detect the change in packets anymore. In trust-based routing environments, representing multiple identities can be used to deliver fake recommendations about the trustworthiness of a certain party, hereby attracting more traffic to it; in ideal starting point for further attacks. Amplified if the malicious node exists within or around the centre of the network so that it hears every communication happening inside the network. However, in the case of Multipath protocols which send data redundantly, not relying on one path only, the problem of sinkholes can be reduced. Probabilistic protocols which measure the trustworthiness of a network can help detecting sinkholes within the network.

B. **Passive Attacks** In passive attacks the attacker does not perturb the routing protocol, instead try to extract the valuable information like node hierarchy and network topology from it. Passive attack is in nature of eavesdropping on, or monitoring of, transmission. The goal of opponent is to obtained information that is being transmitted [5]. Passive attacks are very difficult to detect because they do not involve any alteration of data.

C. **Other Advanced Attacks** We will now discuss several specific attacks that can affect the operation of a routing protocol in ad hoc network.

- Black hole attack
- Byzantine attack
- Rushing attack
- Replay attack
- Location disclosure attack

VII. **SECURE AD HOC ROUTING**

There exist several proposal that attempt to architect a secure routing protocol for mobile ad hoc network, in order to offer protection against the attacks mentioned in the previous section. There are several solutions proposed by researcher they are either completely new stand-alone protocol or in some cases incorporation of security mechanism into existing one like DSDV and AODV [17]. Since routing is an essential function for ad hoc networks, the integrated security procedures should not hinder its operation. Another important part of analysis is the examination of assumption and the requirements that each solution depend on. Although a protocol might be able to satisfy certain security constraints, its operational requirements might thwart its successful employment. In order to analyze exiting solution in structure way we have classified them into three categories: Solution based on Symmetric cryptography, solution based on Asymmetric cryptography and Hybrid solution. However, this classification is only indicative since a lot of solution can be classified into more than one category.

A. **Symmetric Cryptography Solutions**
- Secure Efficient Ad hoc Distance Vector (SEAD)
- Secure Routing Protocol (SRP)
- Ariadne
B. Asymmetric Cryptography Solutions
- Authenticate routing for ad hoc network (ARAN)
- SAR C. Hybrid Solutions
- Secure Ad hoc On-demand Distance Vector (SAODV)

REFERENCES