A survey: Mobile Adhoc NETworks using Security Attacks in routing mechanism

K.RANGASWAMY [1] P.BHARATH KUMAR[2]
1. Assistant Professor, Anantha Lakshmi Institute of Tech & Sciences, Anantapur.
2. Assistant Professor, Anantha Lakshmi Institute of Tech & Sciences, Anantapur.

ABSTRACT

Security is a major concern for safe communication between mobile nodes in an alien environment. In alien environments, attackers can bunch active and passive attacks against imperceptible routing in routing message and data packets. In this, we focus on significant security attacks in Mobile ad hoc networks. MANET has no clear immunity so; it is available to both legitimate users and malicious attackers. In the existence of malicious nodes, one of the main objectives in MANET is to design the robust security solution that can protect MANET from various routing attacks. However, these solutions are not correct for MANET resource constraints, i.e., battery power and limited bandwidth. Mobile ad-hoc network can operate in isolation or in coordination with a wired infrastructure. This flexibility along with their self organizing facilities is some of MANET's biggest strengths, as well as their biggest security vulnerabilities. In this paper different routing attacks, such as active (black hole, spoofing, wormhole, flooding,) and passive (traffic monitoring, traffic analysis, eavesdropping) are described.

Black hole node or malicious node sends the Route Response (RREP) to the sender which having a shortest path to reach to the destination and when sender starts the communication with that black hole node, that node drops all packets. Now a day, there are many detection and prevention techniques available to protect the network form the black hole attack. This paper is shortly explains the detection techniques of the black hole attack in MANET.

Keywords: MANET, DOS, AODV, Data Traffic, Attacks, Security.

1. INTRODUCTION

An ad hoc network is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. Such a network may work in a standalone way, or may be connected to the larger Internet. A mobile ad hoc network [2] is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. So the functioning of Ad-hoc networks is dependent on the trust and co-operation between nodes. Nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. Hence in addition to acting as hosts, each mobile node does the function of routing and relaying messages for other mobile nodes [3]. A MANET is particularly vulnerable due to its fundamental characteristics [4], [5], such as open medium, dynamic topology, distributed cooperation, and constrained capability.

2. Security Challenges in MANET

Security is a major concern in all forms of communication net-works, but ad hoc networks face the greatest challenge due to their inherent nature. As a result, there exist a slew of attacks that can be performed on an Ad hoc network. [3]. Challenges to MANET are discussed as follows-

Confidentiality- It ensures that classified information in the net-work is never disclosed to unauthorized entities. In MANETs, this is more difficult to achieve because intermediates nodes (that act as routers) receive the packets for other recipients, so they can easily eavesdrop the information being routed. Sensitive information, such as strategic military decisions or location information requires confidentiality. Leakage of such information to enemies could have devastating consequences.

Availability- Availability is the most basic requirement of any network. It assures that the services of the system are available at all times and are not denied to authorized users.

Integrity- It guarantees that a message being transferred between nodes is never altered or corrupted and the message must be genuine. Data can be altered either intentionally by malicious nodes in the network or accidentally because of benign failures, such as radio propagation impairment or through hardware glitches in the network.

Authenticity- Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes.

Non-repudiation- It ensures that the information originator cannot deny having sent the message. Non-repudiation is useful for detection and isolation of compromised nodes.

Access Control- To prevent unauthorized use of network ser-vices and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

3. Routing Approaches in MANET

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. Following are the categories of routing protocols in MANET.

Table-driven or Proactive Protocols- Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network. As the resulting information is usually maintained in tables, the protocols are some-times referred to as table-driven protocols. Representative proactive protocols include- Destination-Sequenced Distance- Vector (DSDV) routing, Optimized Link State Routing Protocol (OLSR).

On-demand or Reactive Protocols- A different approach from table-driven routing is reactive or on-demand routing. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually

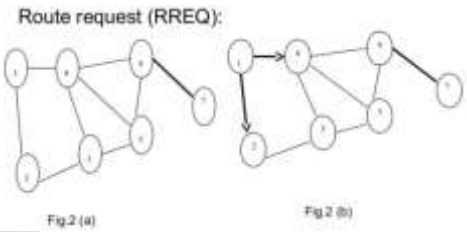
initiated by the source node through discovery process within the network. Once a route has been established, it is maintained by the node until either the destination becomes inaccessible or until the route is no longer used or has expired. Reactive routing protocols include- Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) routing protocol.

Hybrid Routing Protocols- Purely proactive or purely reactive protocols perform well in a limited region of network setting. How-ever, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently.

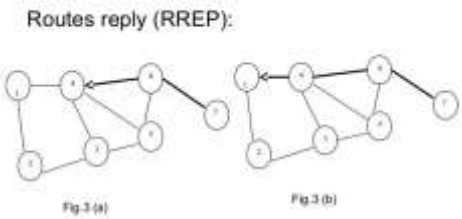
AODV: AODV, source node and intermediate nodes store the next hop information corresponding to each flow for data packet transmission.

- On-demand routing protocol, the source code floods the RouteRequest packet in the network when a route is not available for the desired destination.
- It may obtain multiple routes to different destinations from a single RouteRequest.
- AODV uses a destination sequence number DestSeqNum to determine an up-to-date path to the destination.
- A node updates its path information only if the DeptSeqNum of the current packet received is greater than the last DeptSeqNum stored at the node.
- A RouteRequest carries source identifier (SrcID), the destination identifier (DestID), the source sequence number (SrcSeqNum), destination sequence number (DestSeqNum), the broadcast identifier (BcastID), time to live (TTL) field.
- DestSeqNum indicates the freshness of the route that is accepted by the source.
- Validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the RouteRequest packet.
- If RouteRequest is received multiple times, indicated by BcastID-SrcID pair, the duplicate copies are discarded.
- A timer is used to delete this entry in case RouteReply is not received before the timer expires.

Route discovery Process on AODV protocol



Route discovery Process on AODV protocol



4. SECURITY ISSUES

Security in Mobile Ad-Hoc Networks is an important concern for the network functioning.

MANET often experience different security attacks because of its following features: Dynamically changing network topology, lack of central monitoring, cooperative algorithms and absence of a certification authority and etc [3, 4]. These features are explained below:

1) *Dynamically changing network topology*: Nodes are free and they can move arbitrarily. So the network topology changes unpredictably and frequently, which results in change in routes, frequent partitioning of network and loss of packets.

2) *Lack of centralized monitoring*: MANETs does not have any established infrastructure and centralized administration. MANET works without any preexisting infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management.

3) *Cooperative algorithms*: In MANET the routing algorithms need to have trust between their neighboring nodes.

4) *Bandwidth constraint*: Wireless links have lower capacity as compared to the infrastructures networks.

5) *Limited physical security*: Mobility of nodes results in higher security risks, which increases the possibility of spoofing, eavesdropping and masquerading and DoS attacks.

6) *Energy constrained operation***:** The only energy means for the mobile nodes in Ad-Hoc network is the battery power. And they also have a limited storage capacity and power.

Characteristics of MANET

- No Centralized Administration – Each node in the MANET has its own communication capabilities for forwarding the data over [1] the network and adjusts the topology.
- Flexibility- MANET enables fast organization of the ad hoc network. When a node is joining the network, it should have the limited wireless communication range.
- Peer to peer connectivity of the nodes- In MANET, the nodes set communication link to which request response messages are flooded.
- Resource constraints- The node may have finite energy, so this may affect the functionality of the network.
- Dynamic Network topology-A node discovers the service of a nearby node using the service discovery protocol.
- Heterogeneous Nodes – In MANET architecture, any node can participate in forwarding the packets. The node may be Personal Computers, smart phones, smart tablets, embedded systems etc.

Applications

As Mobile ad hoc network has dynamic network and fewer infrastructures so it is gaining popularity. Ad hoc networks can be established [1] anywhere where the nodes have connectivity with other nodes and can join and leave the network at any time. The applications are as followed:

Military: The communication among the soldiers, headquarters of military and vehicles can be possible as this area do not have the proper establishment of the base station for the communication.

Emergency Services: Ad hoc can be used in emergency operations such as search and rescue, recovery from disasters for e.g. Fire, flood, volcano earthquake, eruption etc.

Commercial environments: Ad hoc networks can autonomously link an instant in business so as to share the daily updates of office.

5. Types of Security Attacks

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from inside i.e. network itself. Ad hoc network are mainly subjected to two different levels of [4] attacks. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level tries to damage the security mechanisms employed in the network.

5.1. Internal Attacks

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. These attacks may broadcast wrong routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more reliable nodes. The inaccurate routing information generated by malicious nodes is difficult to identify.

5.2. External attacks

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc [2]. External attacks prevent the network from normal communication and producing additional overhead. External attacks can divided into two categories:

5.2.1 Passive attacks

MANETs are more susceptible to passive attacks. The passive attack does not alter the data transmitted within the network. But it includes the unauthorized “listening” to the network traffic. Passive attacker does not alter the operation of a routing protocol, but attempts to discover the important information from traffic. Detection of passive attacks is difficult since the operation of network itself doesn’t get affected. In order to overcome these attacks, powerful encryption algorithms are used to encrypt the data being transmitted.

5.2.2 Active Attacks

Active attacks are very severe attacks on the network that prevent message flow between the nodes. Active attacks can be internal or external. Active external attacks can be executed by outside sources that do not belong to the network. Active Internal attacks are malicious nodes which are part of the network. Internal

attacks are more rigid and hard to detect than external attacks. These attacks generate illegal access to network that helps the attacker to make changes such as packets modification, DOS and congestion etc.

6. LITERATURE REVIEW

[1] Mobile Ad hoc network (MANET) is infrastructure-less network. The nodes are free to move in the network and also wireless topology may change rapidly. For the security concerned, it is very important to protect communication between mobile nodes. There are many attacks in MANET and one of them is Blackhole Attack. The blackhole attack is degraded the network's performance and reliability. Blackhole node or malicious node sends the Route Response (RREP) to the sender which having a shortest path to reach to the destination and when sender starts the communication with that blackhole node, that node drops all packets. Now a day, there are many detection and prevention techniques available to protect the network form the blackhole attack. This paper is shortly explains the detection techniques of the blackhole attack in MANET.

[2] A mobile Adhoc network is an autonomous network that consists of nodes which communicate with each other with wireless channel. Due to its dynamic nature and mobility of nodes, mobile Adhoc networks are more vulnerable to security attack than conventional wired and wireless networks. In MANET, A routing protocol plays important role to handle entire network for communication and determines the paths of packets. A node is a part of the defined network for transferring information in form of packets. If all packets transferred from source to destination successfully, it has been assumed that the routing protocol is good. But, an attacker turns this dealing as a speed breaker and turning point of a highway. One of the principal routing protocols AODV used in MANETs. The security of AODV protocol is influence by malicious node attack. In this attack, a malicious node injects a faked route reply claiming to have the shortest and freshest route to the destination. However, when the data packets arrive, the malicious node discards them. To preventing malicious node attack, this paper presents PPN (Prime Product Number) scheme for detection and removal of malicious node.

[3] Vehicular Ad hoc Network (VANET) needs security to implement the wireless environment and serves users with safety and comfort applications. Attackers generate different attacks in vehicular network. In this paper, first phase implementation of attacker node in AODV routing protocol in VANET and in second phase identify malicious node with watchdog intrusion detection system. Once the attacker node is identified we will prevent it to communicate with other neighbor nodes in network with the help of Beyesian network theory. From Beyesian network theory find probability of the neighbouring node being attacker node. To make secure AODV connection with generate new Route Request Packet (RREQ) in VANET.

[4] Ad-hoc networks are emerging technology, due to their spontaneous nature, are frequently established insecure environments, which makes them vulnerable to attacks. These attacks are launched by participating malicious nodes against different network services. Ad hoc On-demand Distance Vector routing (AODV) is a broadly accepted network routing protocol for Mobile Ad hoc Network (MANET). Black hole attack is one of the severe security threats in ad-hoc networks which can be easily employed by exploiting vulnerability of on-demand routing protocols such as AODV. In this paper, a review on different existing techniques for detection of pooled or co-operated black hole attacks with their defects is presented.

[5] An ad hoc network is a collection of mobile nodes that dynamically form a temporary network. It operates without the use of existing infrastructure. One of the principal routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack. This paper analyze the black hole attack which is occurs in ad hoc network. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. By doing this, the malicious node can deprive the traffic from the source node In order to prevent this kind of attack, it is crucial to detect the abnormality occurs during the attack. In this paper we have propose a watchdog mechanism which first detect the black hole attack and then give new route to this node.

CONCLUSION AND FUTURE WORK

There is no fix mechanism to detect or prevent the blackhole attack; researcher finds new methods to detect blackhole attack. And also new methods will come because blackhole attack is active research area. To detect multiple blackhole attack there is one or combinations of two methods are used. As discussed above methods are implementing in AODV or in DSR routing protocol. The proactive based method gives higher packet delivery ratio but it creates more overhead. Whereas, reactive based method gives lower overhead but the packet loss is higher. So hybrid method is solution of that problem. Combining both proactive and reactive method we get the better results.

A security protocol has been proposed that can be utilized to identify malicious nodes in a Manet and thereby identify a secure routing path from a source node to a destination node avoiding the malicious nodes (i.e Prime Product Number (PPN) scheme is proposed to mitigate the adverse effects of misbehaving nodes. The basic idea of the PPN scheme is that, each node in the network has a specific prime number which acts as Node Identity and this identity must not be changed). As future work we intend to include that the proposed security mechanism may be extended so that it can defend against the malicious nodes which are present inside the clusters. The next step is to simulate more scenarios in which more complicated misbehaviors exist and other metrics need to be measured such as latency and end-to-end delay.

I analyze the performance of AODV with and without malicious node under the circumstances of different parameters. Simulation results show, that when a node become as a malicious node it will effect on the AODV performance. The route discovery process in the AODV is susceptible to malicious node and therefore, it is vital to have an efficient security functions in the protocol in order to avoid such attacks.

First perform the solution for the malicious node and other attacks like blackhole, gray hole or other and apply this for AODV and measure different QoS (Quality of Service) parameter. For detect unauthorized accesses to a computer system or a network Watchdog is implemented in AODV with blackhole attack.

We analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in NS-2. Moreover, we also implemented a solution that attempted to reduce the Black Hole effects in NS-2 is black hole AODV protocol. Watchdog mechanism AODV tries to eliminate the Black Hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes start communication of data packets.

Finally we have compared the two protocol for various design metrics and comes to conclusion that black hole AODV proves to better than AODV in presence of black hole node.

REFERENCES

[1] Radhika K. Vyas, Dr. K. H. Wandra "A Review: Blackhole Attack Detection/Prevention Techniques in MANET" Volume-2, Issue-5, May-2015

[2] Nusrat Inamdar, Aliya Inamdar "PPN: PRIME PRODUCT NUMBER BASED MALICIOUS NODE DETECTION SCHEME FOR MANETS"

[3] Nishant P Makwana, Sunil K Vithalani, Jayesh D Dhanesha "Intrusion Detection-Watchdog: For Secure AODV Routing Protocol in VANET" Volume4Issue5- May 2013

[4] "A Review Paper on Pooled Black Hole Attack in MANET "Sonia, Abhishek Aggarwal

[5] SURANA K.A.*, RATHI S.B., THOSAR T.P. AND SNEHAL MEHATRE "SECURING BLACK HOLE ATTACK IN ROUTING PROTOCOL AODV IN MANET WITH WATCHDOG MECHANISMS"

AUTHORS

K.RANGA SWAMY **MSC, M.TECH** As an Assistant Professor in the department of computer science and engineering, **ALTS**, Anantapuramu. He received MSC **(COMPUTER SCIENCE) from, S.K UNIVERSITY** in the year of **2000**. He received **M.Tech** degree in Computer Science and Engineering from **JNTU-Hyderabad** in the year of 2**014**

P.BHARATH KUMAR **M.Tech [SE], IRPM (HR), MISTE, IAENG, UACEE, CSTA**

As an Assistant Professor in the department of computer science and engineering, **ALTS**, Anantapuramu. He received from **B.Tech** Degree in the Department of Computer Science and Engineering, **JNTU-Anantapuramu** from **2007-2011**. He received from **M.Tech** degree in Software Engineering Specialization from **SVIST**, Madanapalle from **2012-2014**. He received from **IRPM (HR)** Diploma, **SV University** from **2014-2015**.

Technical Memberships

1. Member of Computer Science Teachers Association **(MCSTA)**
2. Member of International Association of Engineers **(MIAENG)**
3. Associate Member of Universal Association of Computer and Electronics Engineers **(UACEE)**

REVIEW MEMBER

The board of ***JETIR*** grants that ***P.BHARATH KUMAR*** is an active "***REVIEW MEMBER***" journal of emerging technologies and innovative research ***(JETIR)*** approved by ***ISSN & UGC***

IMPACT FACTOR: 5.87
MEMBER SINCE: 13-NOVEMBER-2018
ISSN NUMBER: 2349-5162
MEMBER ID: 113903

He Received **10** International Journals **2** UGC Approved Journal, **2** international workshops and **3** International Conferences From various Organizations. His **Research** area is **Cryptography and Network Security, Networking using simulation tool**