Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey of Security Mechanism in Wireless AODV

Aarti Madan *
Research Scholar SKIET Department of Computer Sc & Engineering Kurukshetra University

Anu
Assistant Professor SKIET Department of Computer Sc & Engineering Kurukshetra University

Abstract—***Ad hoc networks exploit the processing, storage and wireless communication capabilities of mobile devices to create spontaneous and low-cost self-configuring networks. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. One of the principal routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol. The need of wireless network is to participating nodes to forward packets to other node for secure and reliable communication. There are presence of malicious node can harm networks In this paper we studied the details study of attack techniques.***

Keywords— AODV,Maneet,Black Hole Attack,Gray Hole Attack

I. INTRODUCTION

In wireless networks, transmission is done from node to node. Each node acts as a router for transmitting and receiving packets to/from other nodes. An ad-hoc network connection is temporarily created to transmit the data. If the network is established for a long time, it is called simple local area network (LAN). A wireless network uses a decentralized base station to which all nodes must communicate with. A peer-to-peer connection can increase the distance of the wireless network.

An ad hoc network dynamically forms a provisional network without using any existing network infrastructure. The characteristics of ad-hoc network routing protocol are:

1. Simple
2. Less storage space
3. Loop free
4. Short control message (Low overhead)
5. Less power consumption
6. Multiple disjoint routes
7. Fast rerouting mechanism

A number of routing protocols like Ad-hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR), Temporally Ordered Routing Algorithm (TORA) and Destination-Sequenced Distance-Vector (DSDV) have been implemented.

The area of wireless networking emerges from the combination of cellular technology, personal computing and the Internet through this we can access information and services electronically, regardless of their geographic position. We can access continuously changing information from anywhere, anytime due to the increasing interaction between computing and communication. Wireless networks have become popular in the computing industry. The applications of the ad-hoc network are vast and interested reader may refer [2].

Wireless ad-hoc network is without any fixed infrastructure. Nodes are free to move randomly and generate random topology. The neighbors change due to the random movement of nodes. Ad-hoc networks are more appropriate in situations where a fixed infrastructure is not possible.

II. RELATED WORK

In this paper [1] authors(**JATHE S.R. AND DAKHANE D.M.**)communicating without a network infrastructure. Due to security vulnerabilities of the routing protocols, however, wireless ad hoc networks may be unprotected against attacks by the malicious nodes. 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 [1]. In this attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. In this paper we studied the details about black hole attack, and comparison of different black hole attack techniques.

The information about the network, con-cept of wired and wireless network, why use of wireless network., we also see the introduction about MANET and various character-istics and application of MANET . In this paper we have studied about the blackhole attack, wormhole and DOS attack, and ana-lyzed different Intrusion Detection Systems in MANET

.Intrusion-Detection Systems aim at detecting attacks against computer systems and networks, or, in general, against information sys-tems. IDS can be viewed as a guard system that automatically detects malicious activities within a host or network. This paper also analyzes comparison between the different intrusion detec-tion systems in the MANET.
In this paper [2] authors(**Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall** Nygard) Mobile ad hoc networks (MANETs) are extensively used in military and civilian applications. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks. we address the problem of coordinated attack by multiple black holes acting in group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack.
The AODV protocol is vulnerable to the well-known black hole attack. A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole does not have to check its routing table, it is the first to respond to the RREQ in most cases..However, the proposed method cannot be applied to identifying a cooperative black hole attack involving multiple nodes. In this paper, we develop a methodology to identify multiple black hole nodes cooperating as a group. The technique works with slightly modified AODV protocol and makes use of the Data Routing Information (DRI) table in addition to the cached and current routing tables.
In this paper [3] authors(**Mr. Rajdipsinh Vaghela M,r. Divyesh Yoganand ,Mrs. Monika Changela)** The need of wireless network is to participating nodes to forward packets to other node for secure and reliable communication.There are presence of malicious node can harm networks. In mobile ad hoc network these attacks shown their significance in the terms of network worms which can attack, alter or modify the root definitions of network across all administrative and participating domains. This paper reviews the full study to eliminate thread of black hole attacks in MANET". We also address to the solution against the threat of black hole attack in MANET. In Black Hole Attack a malicious node advertises itself as having the shortest path to the node whose packets it wants to intercept. We are proposing a technique to identify attack and a solution to discover a safe route for secure transmission. We are proposing here a Secure Ad-hoc On-Demand Distance Vector routing protocol (SAODV) to detect the single black hole node as well as co-operative black hole.
The challenges in routing security and related issues are discussed. However there is no such standard exist to secure the MANET. There are many techniques to detect the black hole. In this paper an approach using SAODV protocol detect the black hole using CRRT and timer table. The source node has to wait for all RREP packets from the nodes. If there is a route path is same occur more than one time then it is a safe path for data packet. If not then taken a random path which reach to the destination.
In this paper [4] authors(**SUSHIL KUMAR CHAMOLI, SANTOSH KUMAR DEEPAK SINGH RANA)** Wireless mobile ad hoc network (MANET) is a self-configuring network which is composed of several movable mobile nodes. These mobile nodes communicate with each other without any infrastructure. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In Black Hole attack, a malicious node falsely advertises shortest path to the destination node and absorbs all data packets in it. In this way, all packets in the network are dropped. In this paper, performance of AODV is evaluated in presence of black hole attack (malicious node) and without black hole attack with cbr traffic under different scalable network mobility. For this analysis RWP model is used.
Analyze the performance of AODV with and without black hole (malicious node) attack 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 black hole attack and therefore, it is vital to have an efficient security functions in the protocol in order to avoid such attacks.

III Attack Type

1. Passive Eavesdropping

An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to infer the network topology to understand how nodes are located or are communicating with another. Therefore, it can gather intelligent information about the network before attacking. It may also listen to the information that is transmitted using encryption although it should be confidential belonging to upper layer applications.
Eavesdropping is also a threat to location privacy [6]. An unauthorized node can notice a wireless network that exists within a geographical area, just by detecting radio signals. To combat this, traffic engineering techniques have been developed.

2. Selective Existence (Selfish Nodes)

This malicious node which is also known as *selfish node* and which is not participating in the network operations, use the network for its advantage to enhance performance and save its own resources such as power. To achieve that, selfish node puts forth its existence whenever personal cost is involved. Therefore these selfish node behaviors are known as *selective existence attacks.* [7]. For instance, selfish nodes do not even send any HELLO messages and drop all packets even if they are sent to itself, as long as it does not start the transmission. When a selfish node wants to start a connection with another node, it performs a route discovery and then sends the necessary packets. When the node no longer needs to use the network, it returns to the "silent mode" After a while, neighboring nodes invalidate their own route entries to this node and selfish node becomes invisible on the network.

Actually, dropping packets may be divided into two categories according to the aims of the attacking node. Attacker may want to drop the packets of only the other nodes that it will attack later. To do that it must look at the packet to see whether it comes from this node. If attacker looks at the content of all packets aggregating from the network, it spends CPU resource and naturally battery life. This is not desirable behavior for selfish nodes because it spends battery life. Therefore attackers are not interested in the content of the packets if its aim is not to consume its own resources. First category of dropping packets cannot be evaluated as a selfish node behavior. Thus selectively dropping messages is not a selfish node behavior mentioned in [8]. Selective existence is kind of a passive attack, nodes just do not participate in the network operations and they do not change the content of packets.

3. Gray Hole Attack (Routing Misbehavior

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack.

If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior. [5]

Dropping packets is also one of the behaviors of failed or overloading nodes [6]. One should not evaluate every dropping packet action as a selective existence, gray or black hole attack. Actually most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception. [4]

4 Black Hole Attack

The difference of Black Hole Attacks [1] compared to Gray Hole Attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network.

If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

Gray hole attacks against one or two nodes in the network to isolate them, where as black hole attack affects the whole network. Moreover, the malicious node that attempts gray hole attacks cannot be perceived easily since it does not send false messages. Behavior of failed or overloaded nodes may seem like selfish nodes attacks or gray hole attacks due to dropping of messages. But, since failed nodes cannot fabricate a new control message, they cannot form a black hole attack although they will drop the message later.

5. Modification Attack

Control massages are used to establish the shortest and true path between two nodes. But malicious nodes want to route packets to the direction that they want, modifying content of the control messages (e.g. RREQ, RREP and RERR). Modification means that the message does not carry out its normal functions.

Route information such as hop count, sequence number, life time etc. are carried along with control messages. This information has a big role in establishing a true route. Modifying these fields in the control messages, malicious node can perform its own attacks. impersonation is not one of these kinds of attacks; impersonation is only performed by modifying source address to pretend as another node in the network. But changing route information in control messages is performed to mislead the victim or intermediate node and this modification is generally against the replay messages.

For example; by changing hop count or sequence number in the RREP messages, malicious node wants to change route information of victim node. In this attack type; malicious node decreases its sequence number in the RREP message, first capturing it, and finally sending it to the claimed node. When victim node receives this false message it chooses the costly route in the network. Malicious node intends to perform this attack to affect the network performance, or its intension may be selfish, it does not want to route the packet. This attack can be performed by adding a number of virtual nodes and decreasing hop count field of the RREP messages. This attack is also known as detour attack. [7]

Another attack is performed by changing destination IP field in any control message. Thus, messages are not forwarded to relevant node and the communication is broken. 19 At the same time the malicious node may send all messages to the victim node to perform denial of service (DoS) attack or to another malicious node to collect the aggregated network dump. To perform the latter one; more than one malicious node should be located in the network and one of them should be located in the middle of the network to collect messages. This way; collaborative malicious nodes can obtain all information about the network.

6.Attack Against The Routing Tables

Every node has its own routing table to find other nodes easily in the network. At the same time, this routing table draws the network topology for each node for a period (max. 3 seconds, duration of ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol). If malicious node attacks against this table, attacked nodes do not find any route to other nodes whom it wants to connect. This attack is always performed by fabricating a new control message. Therefore it is also named fabricating attack.

There are many attacks against routing tables. Each one is done by fabricating false control messages. For example; to attempt a black hole attack, malicious node first invades into the routing table of the victim, sending false RREP message. Malicious node also spreads false RERR messages to the network so that valid working links are marked as broken [6]. Another attack type against the routing table is to attempt to create lots of route entries for non-existent nodes, using RREQ messages. As a result, routing table of the attacked node is full and does not have enough entry to create a new one. This attack type is known as routing table overflow. [3]

Attacks against the routing tables also affect the network integrity, changing the network topology established in the routing tables. Incorrect control messages are disseminated quickly in the network due to route discovery process and influence the network integrity in a wide area. Therefore attacks against the routing table are known as Network Integrity Attacks. [6].

IV CONCLUSIONS

Securing AODV is still an open area for research work This attack periodically drop packets that they are expected to forward. We studied black hole attack, gray hole attack, Modification attack etc. We studied the defense mechanism for different types of attacks. This type of attack may lead to degrade the performance of the network

REFERENCES

[1] JATHE S.R. AND DAKHANE D.M. "A REVIEW PAPER ON BLACK HOLE ATTACK AND COMPARISON OF DIFFERENT BLACK HOLE ATTACK TECHNIQUES" International Journal of Cryptography and Security ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-22-26.

[2] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks " IEEE 2011

[3] Mr. Rajdipsinh Vaghela Mr. Divyesh Yoganand Mrs. Monika Changela "A Survey on Approaches towards the Black Hole Attack in Manet" INDIAN JOURNAL OF RESEARCH Volume : 1 | Issue : 12 | December 2012.

[4] DEEPAK SINGH RANA Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks"IJCTA july 2012

[8] Ming-Yang Su1 , Kun-Lin Chiang "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks "International Symposium on Parallel and Distributed Processing with Applications 2011

[5] Payal N. Raj, Prashant B. Swadas "DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET" IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[6] Ashok M.Kanthe, Dina Simunic and Marijan Djurek" Denial of Service (DoS) Attacks in Green Mobile Ad–hoc Networks" MIPRO 2012, May 21-25,2012, Opatija, Croatia

[7] Maha Abdelhaq1, Sami Serhan2, Raed Alsaqour3 and Rosilah Hassan"A Local Intrusion Detection Routing Security over MANET Network" 2011 International Conference on Electrical Engineering and Informatics 17-19 July 2011, Bandung, Indonesia.

[8] Nidhi Purohit, Richa Sinha and Khushbu Maurya" Simulation study of Black hole and Jellyfish attack on MANET using NS3" INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 08-10 DECEMBER, 2011.

