International Journal Of Latest Technology In Engineering & Management (IJLTEM)
Volume 8 - Issue 5 {September 2023} {Page: 52-55}

Security Issues in Mobile Ad-Hoc Networks Routing Algorithms

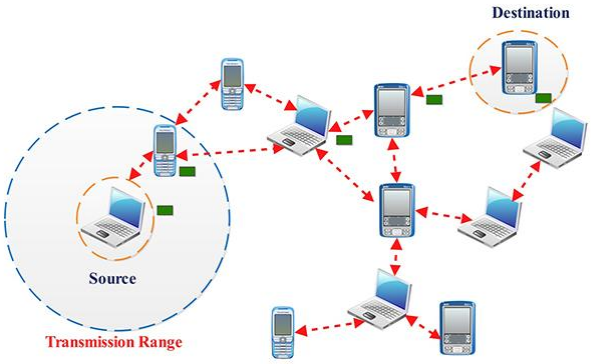
Channakeshava RN
Assistant Professor, HPPC Government First Grade College, Challakere, India

Abstract: *Transporting data through the networks has many techniques, and these techniques have their own advantages and disadvantages, depending on the networking structure, physical medium, power constraints, types of services the network providing, appropriate routing protocol is chosen. Different protocols chosen may provide some specific advantage, but at the same time due to concentrating on particular issue, the vulnerabilities in the protocols may rise which may be exploited by culprits to breach the network data. As per our research work done there may not be a single best routing algorithm which gives fastest, reliable, secured, efficient, routing algorithm but we can list out the issues associated with the algorithms and probable solutions. The main objective of the research is to study the security issues that may arise in different routing protocols, and thereby to find out the possible solutions or precautionary measures to be taken in different routing algorithms.*

Keywords: *AODV, Communications, MANETs, Routing, Security*

1. INTRODUCTION

Mobile Ad Hoc Networks (MANET) are the networks crated Ad Hoc, the network topology keeps on changing as the devices in the MANETs are mobile devices. Military communication systems, rescue setup in a disaster site, etc are the major applications of the MANETs.



Networks used for transmission between mobile devices are designed without keeping security in mind and all the devices are treated to be friendly. After implementing MANETs security has to be introduced in mobile Ad Hoc networks in two systems. One is to secure data to be transmitted and second is to secure the routing protocols so that networking resources are not wasted.

Security can be forced in different layers. But implementing security in network layer for routing algorithms mainly concentrates on identifying right person to receive data and right person has transmitted data. Routing algorithms are always designed to route the packets from source to destination with least delay, maximum throughput, and with least energy consumed at nodes, but while optimizing these things the routing algorithm will have to minimize accommodations for some security features.

The nodes in the Ad Hoc networks are exposed to; easy theft and tampering of nodes. And nodes have limited computational abilities and limited battery power.

2. BACKGROUND

A black hole problem in AODV protocol can be solved by restricting the reply message by any of the intermediate node and all the reply messages must be sent by destination but this increases delay greatly. An alternative method is to trust the intermediate node who is telling it has the shortest path, by checking whether it can reach that node by an alternative path [1]. A Secured Ad Hoc On-demand Distance Vector or SADOV is an extension of AODV makes every node to use a digital signature to sign the whole message. Every neighboring node can verify that digital signature [2]. For the security

issues associated with Ad Hoc networks [3] has provided countermeasures, security measures with Preventive mechanism using cryptography and reactive mechanism by detecting the transmission against pattern of well known attacks. 6LoWPAN protocol is used in IOT devices which also has mobile devices most of them runs over batteries, so the protocols securities are discussed in the paper [4]. 6LoWPAN uses compressed IPSec for security at Network layer which takes care of the security using encryption.

3. ROUTING ALGORITHMS

MANETs; Mobile Ad-Hoc Networks established for mobile nodes, which are challenges of current trends, the protocols have to accompany routing for mobile devices which may change access points randomly due to their mobility. Two major types of routing are possible Table-driven and On-demand. Table Driven routing algorithms periodically checks for the neighboring devices to update its routing information in the form of routing tables. And any change in the network topology is updated in the next periodic check. On-demand routing algorithms attempt to discover the route only when a source initiates transmission. Three Routing protocols are widely used in mobile Ad-Hoc networks; DSDV Destination Sequenced Distance Vector Routing Protocol, AODV Ad Hoc On-demand Distance Vector Protocol, and DSR Dynamic Source Routing Protocol.

DSDV is a table driven routing algorithm whose tables are updated periodically or every tome network infrastructure changes. Routing table in each node consists of new sequence number, the destination address, the number of hops for the destination, and the sequence number of the destination.

AODV is the most used protocol for MANETs: this protocol detects routing tables as and when required, and routes are saved as long as they are required, obsolete routes are discarded. Once started detecting routes to destination multiple routes are produced but AODV keeps only the shortest one. Sequence numbers are used to prevent loops in the routing tables.

DSR Dynamic Source Routing Protocol initiates a route discovery whenever source wants to transfer to destination.

4. SECURITY ISSUES IN ROUTING ALGORITHMS

Attacks on a network are passive or active. Passive attack just attempts to listen into the network system but doesn't disrupt original transmission. A passive attack is very difficult to detect. An active attack will try to disrupt the transmission by inserting false packets into the data stream. Active attacks are further divided into internal and external. Internal attacks are done by compromising nodes inside the network. External attacks are done by the nodes not belonging to the network.

Nodes in a network may misbehave in two types Selfish nodes and malicious nodes. Selfish nodes use the network for their own use but they will not help others in communication in order to save their batteries. Malicious nodes in any other way to Routing has many issues, out of them two of them are to be mentioned;

Some types of attacks that are easily performed on a MANET are;

Black hole: in this type of attack the malicious node pretends to having shortest path to the destination of whose packets it wants to intercept.

Denial of Service: In a typical form of DOS attack the malicious node floods the packets into the network so that maximum bandwidth of the network is utilized and any other nodes will not be able to use the network. Example: A malicious node generates frequent and unnecessary route requests, so that other nodes cannot use the network.

Routing table overflow: Goal of this type of attack is to create routes to nonexistent nodes. Routing table is filled with all fake routes which lead to nonexistent nodes. Creating new route for actual existing node will be denied as the routing table will be full.

Impersonation: A malicious node impersonates as other node while sending control packets which leads in to faulty updating of routing tables.

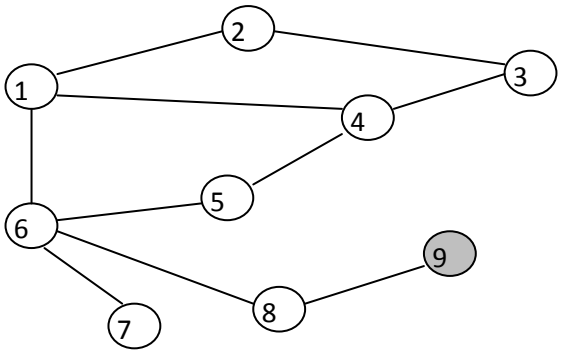
Energy Consummation: MANETs are mainly comprised battery operated nodes, which in turn tries to save energy by transmitting only when necessary. An attacker tries to send unnecessary packets to nodes to drain their energy.

Information Disclosure: in a network, addresses of some nodes may be confidential. A compromised node will reveal this information or any other confidential information to the attackers.

5. SECURITY MECHANISMS

Implementation of network watch dog for detecting routing table overflow and impersonation.

Work of the network watchdog is to keep a watch on the activities of all the nodes in the network, Messages sent by any of the node are verified with some pre defined patterns and thus identifies the malicious node. First all nodes are warned about the malicious node, once it is confirmed to stop activities to and from the malicious node for certain period.



Any node in the network can act as watchdog. In this example node 9 is acting as a network watchdog. It simply asks for the routing tables with each of the other 8 nodes periodically. Maximum of the routing tables will have the same path for the destinations, and a very few will vary. Based on the available routing tables each destination is attempted to reach. If a destination is unreachable by using certain path, the sender of the path is identified. If number of such cases increases from a particular node, that node is identified as a malicious node.

Traditional forms of network watchdogs are used to block certain patterns of traffic or certain nodes to participate in transmission. But using a specialized form of network watch dog we can manage a network. As the number of nodes increases workload on the network watchdog increases. Increasing the number of watchdogs is also an idea. Deciding the scope of each network watch dog will also become additional burden. What happens if the node working as watch dog gets infected? A hierarchical model has to be created and the centralized node should be monitored manually and automatically both. As the nodes in the MANETs are supposed to move how to create a hierarchical model will also becomes a new challenge.

6. CONCLUSION

Implementing a network watchdog for a MANET with small number of nodes will not be a challenging but implementing the technique for a network with millions of nodes is really challenge, but this can be simplified by adopting a hierarchical model. Implementation of this model is little bit risky but the same model can also be used for monitoring other attacks too. Attempts to discover routing table of each node regularly also makes the node acting as watchdog busy.
As it is not necessary for network watchdog to be immediate next node for every node, there is a possibility of routing table information from a node is routed through a malicious node, hence appropriate encryption and keys are to be used.

REFERENCES

[1] *Routing Security in Wireless Ad Hoc Networks, Hongmei Deng, Wei Li, and Dharma P. Agrawal, University of Cincinnati, October-2002, IEEE Communications Magazine.*

[2] *Secure Ad hoc On-Demand Distance Vector Routing, Manel Guerrero Zapata, Mobile Computing and Communications Review, Volume 6, Number 3*

[3] *Security issues in routing protocols in MANETs at network layer, Praveen Joshi, WCIT-2010, 1877-0509, 2010 Published by Elsevier Ltd.*

[4] *Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis, Christine Hennebert and Jessye Dos Santos, October-2014, IEEE Internet of Things Journal, vol. 1, no. 5,*

[5] *Routing Security in Ad Hoc Networks, Janne Lundberg, 2000, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.144.7589&rep=rep1&type=pdf*

[6] *A Performance Comparison of Wireless Ad Hoc Network Routing Protocols under Security Attack, Su Mon Bo, Hannan Xiao, Aderemi Adereti, James A. Malcolm and Bruce Christianson, 2007, IEEE Third International Symposium on Information Assurance and Security*

[7] *Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols, YihChun Hu, Adrian Perrig, David B. Johnson, September2003, WiSe 2003, San Diego, California, USA*

[8] *The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, Frank Stajano and Ross Anderson, 1999, https://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf*

[9] *"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," S. Marti et al., 6th Int'l. Conf. Mobile Comp. Net., Aug. 2000,.*

[10] *Intrusion Detection in Wireless Ad-Hoc networks, Y. Zhang and W. Lee Aug-2000, 6th International conference, mobile Corp.net*

[11] Security in Ad Hoc Networks: A General Intrusion Detection Architecture Enhancing Trust Based Approaches P. Albers et al., 2002 Enterprise Info Systems 4th International Conference,

[12] Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks,, L. Venkatraman and D. P. Agrawal, 2002.