IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

A Review: AODV & DYMO Protocols Effects of Black Hole Attack in MANET

Manju[1], Mr. Kapil Kaswan[2]

M.Tech, CSE, CDLU, Sirsa, India [1]

Asst Professor (CSE), CDLU, Sirsa, India [2]

Abstract: Wireless mobile ad hoc networks (MANETs) are self configuring, dynamic networks in which nodes are free to move. A major performance constraint comes from path loss and multipath fading Many MANET routing protocols exploit multi paths to route packets. The probability of successful packet transmission on a path is dependent on the reliability of the wireless channel on each hop. Rapid node movements also affect link stability, introducing a large Doppler spread, resulting in rapid channel variations. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. Black hole attack is one of many possible attacks in MANET. Black hole attack can occur when the malicious node on the path directly attacks the data traffic and intentionally drops, delay or alter the data traffic passing through it. This attack can be easily lessen by setting the promiscuous mode of each node and to see if the next node on the path forward the data traffic as expected. The implementation of AODV, OLSR and DYMO routing protocol and their comparison based on the performance metrics will be detailed in the Research Paper. The Proposal has been explained in this paper.

Keywords: AODV (Ad hoc On-Demand Distance Vector); OLSR (Optimized Link State Routing); Dynamic Manet on demand (DYMO), MANET (Mobile Ad Hoc Networks).

I. INTRODUCTION

Wireless Technology is an amazing new technology that will allow users to access information and services electronically, regardless of their geographic position. The black hole attack is an active insider attack, it has two Properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. In other terms, a malicious node uses the routing protocol to advertise as having the shortest path to nodes whose packets it wants to intercept. In the case of AODV protocol, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised, if the reply from malicious node reaches to the requesting node before the reply from the actual node, a fake route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to form a denial- of-service attack.

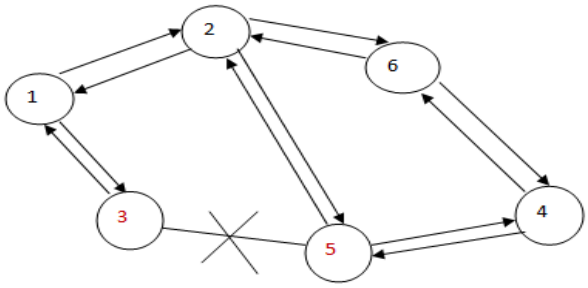


Figure 1: Black Hole Attack

Wireless Networks enable users to communicate and transfer data with each other without any wired medium between them. One of the reasons of the popularity of these networks is widely penetration of wireless devices. Wireless applications and devices mainly emphasize on Wireless Local Area Networks (WLANs). This has mainly two modes of operations, i.e. in the presence of Control Module (CM) also known as Base Stations and Ad-Hoc connectivity where there is no Control Module. Ad-Hoc networks do not depend on fixed infrastructure in order to carry out their operations. The operation mode of such network is stand alone, or may be attached with one or multiple points to provide internet and connectivity to cellular networks.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

A wireless network is one of the most discussed and frequently studied topics these days. As the name suggests it is a network which has limited boundaries and least cost of wiring. Users can communicate and send data to each other without any wired boundary. Among these wireless networks MANETs are gaining popularity day by day. When a computer device wants to communicate with another device, the destination device must lays within the radio range of each other. Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation. Let's discuss the detail some characteristics of wireless networks:

1. Undoubtedly wireless networks are easy to use and easy to configure.
2. Users don't have to stick to one place for using the network; they can easily move and still remain connected to the network.
3. Since it is wireless all the troubleshooting related to wires the cost, the configuration etc are reduced.
4. Wireless networks can be configured in both ways either small or large network as per the users need.

Attacks on MANETs:

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET). This chapter describes Black Hole attack and other attacks that are carried out against MANETs. Since nodes in mobile network can move freely, the network tends to change its topology very frequently. This mobile nature of the nodes may create many security and other issues in MANETs –

a. Lack of Centralized Management - Since MANETs forms a random network and even the nodes are mobile so there is no centre management. Due to lack of centralized management the detection of attacks is very difficult.

b. Infrastructure less - MANETs infrastructure less nature brings difficulty in detecting any malicious node or faults in the network.

c. Dynamic Topology – Since MANETs have a dynamic topology because the nodes are ever changing this may weaken the relationship among nodes.

d. Packet Loss – There are many reasons of packet loss problem in MANETs. Packet loss may happen due to mobility of nodes, bit rate error, due to interference.

e. No network boundary – Since MANETs have no network boundary because the nodes are movable this may lead to increase in number of attacks on them. Any node may enter the network and may hinder the network communication.

There are different types of attacks which are vulnerable to MANETs and which are active at different layers of network. Few of them are discussed below –

1. Blackhole Attack – The black hole attack is active at the network layer. It has two properties. First is that the attacker sends fake routing information, claiming that it has the valid route to the destination, due to which other nodes in the network route the data packets through the malicious one. Second, the malicious node targets the routing packets, drops them instead of normally forwarding them.

2. Wormhole Attack – It is another network layer attack where the attacker forms a tunnel from one location in the network to another. All the routing packets are tunneled; this tunnel is referred to as a wormhole. In wormhole attack, the attacker gets themselves in strong strategic location in the network. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network. When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network. When the attackers are in such position the attack is known as out of band wormhole. The other type of wormhole attack is known as in band wormhole attack. In this type of attack the attacker builds an overlay tunnel over the existing wireless medium. This attack is potentially very much harmful and is the most preferred choice for the attacker.

II. LITERATURE REVIEW

[1] A. Kumar Sharman and N. Bhatia (2011), "Behavioral study of MANET routing protocols by using NS-2", IJCEM. Author has studied the MANET routing protocols using NS-2 simulator. A Mobile Ad-hoc Network (MANET) consists of a number of mobile wireless nodes, among which the communication is carried out without having any centralized control. MANET is a self organized, self configurable network having no infrastructure, and in which the mobile nodes move arbitrarily. In this work a study has been carried out on the behavioral aspect of three different MANET routing protocols i.e. AODV (Ad Hoc On-Demand Distance Vector), DSDV (Destination Sequenced Distance-Vector) and DSR (Dynamic Source Routing Protocol) using the NS-2 simulation tool. The performance of these routing protocols is analyzed in terms of their average throughput; average delay & maximum packets in queue and their results are shown in graphical forms. The main objective of this study is to create a choice guide of routing protocol for a given network scenario, based on the relative performance of the protocols under various scenarios.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

[2] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma (2011), "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing. Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. The absence of a central management agency or a fixed infrastructure is a key feature of MANETs. These nodes communicate with each other by interchange of packets, which for those nodes not in wireless range goes hop by hop. Due to lack of a defined central authority, securitizing the routing process becomes a challenging task thereby leaving MANETs vulnerable to attacks, which results in deterioration in the performance characteristics as well as raises a serious question mark about the reliability of such networks. In this paper they have attempted to present an overview of the routing protocols, the known routing attacks and the proposed countermeasures to these attacks in various works.
[3] Manveen Singh Chadha, Rambir Joon, Sandeep(2012),"Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs", International Journal of Soft Computing and Engineering (IJSCE). ISSN: 2231-2307, Volume-2, Issue-3, July 2012. The author has been explained the MANTE,A Mobile Ad-hoc Network and the existing protocols of this category. Author has been considered the AODV, DSR, etc protocols for compare the features of these protocols. They explained that the MANET is a dynamic wireless network that can be formed without the need for any pre-existing infrastructure in which each node can act as a router. Mobile ad hoc network (MANET) is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. These nodes change position frequently. The main classes of routing protocols are Proactive, Reactive and Hybrid. A Reactive (on-demand) routing strategy is a popular routing category for wireless ad hoc routing The design follows the idea that each node tries to reduce routing overhead by sending routing packets whenever a communication is requested. They compare the performance of three prominent on demand reactive routing protocols for MANETs, Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) protocols and Ad-hoc On-demand Multipath Distance Vector Routing (AOMDV).
[4] Devendra Singh, Vandana Dubey, Shipra Sharma,(2012),"Performance Analysis of DSR and AODV in Manets: Using WLAN Parameters", International Journal of Computer Applications (0975 – 888). Security is one of the main issues in the MANET in particular with respect to size and complexity of the network. The aim of the author is to discuss special security aspects of MANET and relative study of the routing protocols such as AODV and DSR. The Author has explained the routing protocols with consideration of large network and concluded that the AODV routing protocols is efficient for the huge network as compare to the DSR. They show the impact of routing protocols on a typical MANET performance. The simulation results give a clear view of which routing protocols perform best in a given situation. The simulation results provide a clear view for implementing a MANET routing protocol, for example in particular AODV can perform well in medium size networks. In terms of reactive routing protocols, according to the results, DSR is best recommending for small networks, AODV for Medium networks.
[5] Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava,(2013),"Simulation And Analysis Of Performance Parameters For Black Hole And Flooding Attack In MANET Using AODV Protocol", International Journal Of Scientific & Technology Research, Volume 2, Issue 7, July 2013, ISSN 2277-8616. The author has explained the security issues in routing protocols and compare them by consider the different parameters and attacks on AODV. They explained that the each device in a MANET is free to move independently in any direction, linking to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. They describe the features, application, flooding attack and black hole attack in the MANET implemented on AODV protocol. The simulation work is carried out in Network Simulator (NS2.34). The performance analysis is done for 3, 5 and 10 nodes. The average delay, routing overhead, packet drop rate and packet delivery rate are calculated. They simulated and has been evaluated that in flooding attack the routing overhead is more as compared to the black hole attack. A comparative study is also done on these parameters.
[6] A.Moravejosharieh, H.Modares, Rosli Salleh (2013),"Performance Analysis of AODV, AOMDV, DSR, DSDV Routing Protocols in Vehicular Ad Hoc Network", International Science Congress Association. The author has been assimilated the knowledge about Vehicular Ad Hoc Network (VANET) and routing protocols is implemented on the VANET. There is the concept of efficiency in connectivity for the vehicles either through vehicle-to-vehicle or vehicle-to-infrastructure communication that enables the Intelligent Transportation Systems (ITS). In order to design a suitable and efficient routing protocol in VANET, they implemented the comprehensive study on popular VANET tool and routing protocols must be considered as a real need. The author have been exploited routing protocols AODV, AOMDV, DSR, DSDV and is compared in terms of routing performance based on vehicle velocity and vehicle density.

III. OBJECTIVES

To render the network function normally in the presence of misbehaving nodes is a challenging task and demands it necessary to consider "fault tolerance" as a main objective at the design level of routing protocols. It seems imperative to provide a simulation study that measures the impact of misbehaving nodes in order to provide protocol designers

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

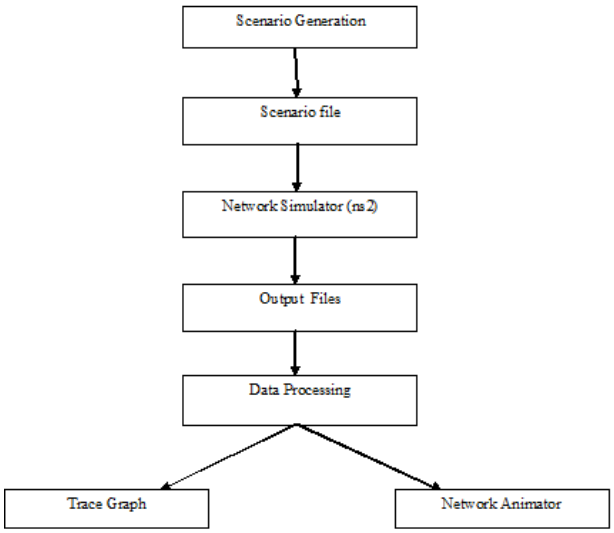
with new guidelines that help in the design of fault tolerant and attack tolerant routing protocols for MANETs. The objective of Research work is to study the affect of Attacks in Routing Protocols. The Objectives of Research Work is explained as:

1. Literature review of MANET Routing protocols.
2. Analyse the selected protocols through simulation via ns2.34 and verify it on the basis of literature review.
3. Review and understanding of black hole attack on routing Protocols.
4. To implement black hole attack on DYMO and AODV routing protocol.
5. To evaluate and conclude the result of the proposed work using different parameters.
6. To conclude which protocol between AODV and DYMO works better under the effect of attack.

IV. PROPOSED METHODOLOGY

The Proposed Steps has been followed in Research work and will be implement in the Research Scenario. MAC layer gives a positive sign to send the packet on to the channel, it fetches the packet form the queue and hands it over to network interface which in turn sends the packet to radio channel. This packet is copied and sent to all network interfaces. Each network interface stamps the packet with its properties and invokes the radio propagation channel. If the packet is received error free, then it is sent to the mobile entry point. Below figure 4.2 explains the simulation with ns. It consists of generating the following input file to network simulator:

A file that describes the movement pattern of nodes and the traffic in the network called scenario file. This file is then used for the simulation and as a result of it a trace file is generated as output. The trace file can then be scanned and analyzed for the various parameters that we want to measure.



V. CONCLUSION AND FUTURE WORK

In this we have studied the performance parameters and work flow of our proposed work of the routing protocols i.e. AODV, DYMO and OLSR and tool proposed ns-2 simulator. In Future Work, The different parameters will be analyzed and detailed in the research paper. The above work will be conducted at the real time platform and it should also be tested on cross layer. The tool will be used NS-2 Simulator.

REFERENCES

[1] A. Kumar Sharman and N. Bhatia (2011), "Behavioral study of MANET routing protocols by using NS-2", IJCEM.
[2] Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma (2011), "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing.
[3] Manveen Singh Chadha, Rambir Joon, Sandeep(2012),"Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs", International Journal of Soft Computing and Engineering (IJSCE). ISSN: 2231-2307, Volume-2, Issue-3, July 2012.
[4] Devendra Singh, Vandana Dubey, Shipra Sharma,(2012),"Performance Analysis of DSR and AODV in Manets: Using WLAN Parameters", International Journal of Computer Applications (0975 – 888).
[5] Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava,(2013),"Simulation And Analysis Of Performance Parameters For Black Hole And Flooding Attack In MANET Using AODV Protocol", International Journal Of Scientific & Technology Research, Volume 2, Issue 7, July 2013, ISSN 2277-8616.
[6] A.Moravejosharieh, H.Modares, Rosli Salleh (2013),"Performance Analysis of AODV, AOMDV, DSR, DSDV Routing Protocols in Vehicular Ad Hoc Network", International Science Congress Association.