Detection and Prevention of Black hole Attack in MANET

Abhilasha Arya¹, Asst. Prof. Namrata Sharma²,
¹, ²Sushila Devi Bansal College of Engineering, Indore (M.P.)

Abstract: - MANET (Mobile Ad Hoc Network) could be a collection of self configurable mobile nodes wherever every node acts as a router for different nodes, which permits knowledge to travel, utilizing multi-hop network paths. MANETs are vulnerable to various attacks in the least layers, because the design of most MANET routing protocols assumes as if there is no malicious intruder node within the network. The main aim of this work is to develop routing protocols for knowledge transmission below black hole attack in MANET. The proposed protocols should be efficient in terms of Packet Delivery ratio, End-to-End Delay, Residual Energy and Throughput. Based on the motivations to produce new security measures to be incorporated in popular routing protocols DSDV, the aim has been implement secure routing (MDSDV) protocols for data transmission in MANET. Detect black hole node in MANET scenario using MDSDV protocol. Prevent the network from black hole attack and improve the packet delivery fraction, throughput and end-to-end delay, Residual Energy even with the presence of black hole attacks. The results of both DSDV and MDSDV compare to analyze that of those 2 types of protocols provides higher performance.

Keywords: - Mobile ad hoc network, NS-2.35, black hole attack, DSDV and MDSDV routing protocol

I. INTRODUCTION

A wireless ad-hoc network consists of a collection of mobile nodes in which nodes are communicating with each other without help from a fixed infrastructure. Routers and hosts are used to form wireless networks. A wireless ad hoc network is a decentralized type of wireless network. A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Mobile hosts are used to form mobile ad hoc network. There is no fixed infrastructure or base station for communication in MANET. Two nodes can communicate with each other when they are within the transmission range but need cooperation of intermediate nodes by forwarding packets when they are multi hop away from each other [1]. In MANET each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network [2]. Routing protocols in ad hoc wireless networks can be classified into three broad categories. This classification is based on the routing information update mechanism. They are Proactive (or table-driven) protocols, Reactive (or on-demand) protocols, and Hybrid routing protocols [3]. These are further divided into sub categories. Routing protocols are vulnerable to routing attacks [3]. There are various routing attacks in ad hoc wireless networks like Attacks using Impersonation, Modification, Fabrication, Replay, and Denial of Service (DoS). In this paper, we focus on black hole attack that belongs to category of fabrication attacks.

There are three main routing protocols proposed for MANET [4]: Ad hoc On-demand Distance Vector (AODV) routing, Dynamic Source Routing (DSR), and Destination Sequence Distance Vector (DSDV) routing protocols. AODV and DSR belong to on-demand routing protocols and DSDV is a table-driven routing protocol. These protocols are vulnerable to different security attacks. In this paper, we use DSDV routing protocol because the DSDV protocol is vulnerable to the black hole attack. So we have simulated the behaviour of black hole attack on DSDV in MANET.

DOI: 10.23883/IJRTER.2017.3563.IJEST
II. DSDV ROUTING PROTOCOL

Destination Sequenced Distance Vector Routing (DSDV)

Destination Sequence Distance Vector (DSDV) is a proactive routing protocol and is based on the distance vector algorithm. In proactive or table-driven routing protocols, each node continuously maintains up-to-date routes to every other node in the network. Routing information is periodically transmitted throughout the network in order to maintain routing table consistency. The routing table is updated at each node by finding the change in routing information about all the available destinations with the number of nodes to that particular destination. Also, to provide loop freedom DSDV uses sequence numbers, which is provided, by the destination node. In case, if a route has already existed before traffic arrives, transmission occurs without delay. However, for highly dynamic network topology, the proactive schemes require a significant amount of resources to keep routing information up-to-date and reliable.

As a result, all the packets through the malicious node are simply consumed or lost. The malicious node can be said to form a black hole within the network, and that we call this the black hole problem. During this way the malicious node will simply misroute lots of network traffic to itself, and will cause an attack to the network with very little efforts on its part.

III. PROPOSED ALGORITHM

Opinions among nodes modification dynamically with the increase of successful or unsuccessful communication times. once and how to update trust opinions among nodes can follow some policies. we derive as follows:

Step 1: Nodes are connected with each other for relaying messages in mobile ad-hoc network. Every node is initialized with Trust index=0.5.

Step 2: Source node transmits the route request packet to its neighbor nodes for relaying messages to the destination.

Step 3: Neighbor node first checks the route in its cache memory, if it exists, then it sends a route reply to the source node. Otherwise, intermediate nodes send same route request to its neighbors and further to other intermediate nodes until the destination is found.

Step 4: When a route reply message is received from the neighbor nodes. Source node first checks sequence number and trust index of replying nodes, and select the highest reputed node for relaying messages.

Step 5: Source node transfers the message through the selected neighbor nodes.

Step 6: If a message is delivered correctly then the trust value of the neighbor is increased If not delivered then the trust value is decreased.

Step 7: All the nodes having trust index less than 0.5 are termed as Black hole and these nodes are black listed.

IV. IMPLEMENTATION AND RESULT ANALYSIS

1. SIMULATION RESULTS FOR PACKET DELIVERY RATIO

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Packet delivery ratio under Black hole attack detection and its prevention through Trust based mechanism i.e. Attack, pre (prevent) and without attack for the various node density.

Packet Delivery Fraction = \( \frac{\text{Total No. of Packet Receive}}{\text{Total No. Packet Send}} \)
2. SIMULATION RESULTS FOR THROUGHPUT

This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Throughput under black hole attack detection and its prevention through Trust based mechanism i.e. Attack, pre and without attack for the various node density.

\[
\text{Throughput} = \frac{\text{Total No. of Successfully Received Packet}}{\text{Total Simulation Time}}
\]

3 SIMULATION RESULTS FOR END TO END DELAY

This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes. Figure and table shows the End to End Delay under Black hole attack detection and its prevention through Trust based mechanism i.e. Attack, pre and Without attack for the various node density.

\[
\text{E2E Delay} = \text{Receiving Time} - \text{Sending Time}
\]
4 SIMULATION RESULTS FOR RESIDUAL ENERGY
It is the total amount of remaining energy by the nodes after the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation than the energy consumption by that node is 30%. The unit of it will be in Joules. Figure and table shows the Residual Energy under Black hole attack detection and its prevention through Trust based mechanism i.e. Attack, pre and without attack for the various node density.

\[
\text{Residual Energy} = \text{Total Energy} - \text{Consume Energy}
\]

5. CONCLUSION AND FUTURE WORK
MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment, the detection and prevention of black hole attack in the network exists as a challenging task. In this work analyzed the effect of black hole attack in the performance of DSDV protocol and prevent the network from black hole attack using MDS DV protocol. The simulation has been done using the network simulator (NS-2.35). The performance metrics like packet delivery ratio, energy, throughput and average end to end delay has been measured and analyzed with the variable node density. From the simulation results it is clear that when the black hole node exists in the network, it can be affected and decreased the performance of DSDV routing protocol.
As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory, mobility, increasing number of malicious node, increasing number of nodes and also focusing on resolving the problem of multiple attacks against DS/DV.

REFERENCES


II. Hizbullah Khattak and Nizamuddin, Fahad Khurshid,” Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash” 2013 IEEE.

III. Seryvuth Tan, Kheecheon Kim,” Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETS” in 7/2013 IEEE.

IV. Ms Monika Y. Dangore and Mr Santosh S. Sambare,” Detecting And Overcoming Blackhole Attack In manet” 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies

V. Ketan S. Chavda and Ashish V.Nimava,” REMOVAL OF BLACK HOLE ATTACK IN AODV ROUTING PROTOCOL OF MANET” 4th ICCCNT – 2013 July 4 -6, 2013, Tiruchengode, India

VI. jilpa khamar and avani Dadhania “An Performance Enhancement of AODV Routing Protocol in Manets”in IJAERD volume 1,Issue 6,june e-ISSN: 2348


XI. Nital Mistry, Devesh C Jinwala, Member, IAENG, and Mukesh Zaveri, “Improving AODV Protocol against Black hole Attacks”, IMECS2010


XVIII. Bo-Cang Peng and Chiu-Kuo Liang”Prevention techniques for flooding attack in Ad Hoc Networks”, IEEE , 2006


XXI. Fan-Hsun Tseng1, Li-Der Chou1and Han-Chieh Chao2,3,4” A survey of black hole attacks in wireless mobilead hoc networks”.

XXII. NishantSitapara ,Prof. Sandeep B. Vanjale”Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks”.