Black Hole Attack in MANET Detection and Prevention

Arshdeep Kaur[1], Jaspreet Kaur[2]

[1]Arshdeep Kaur department, Dept of computer science Engineering, Punjab, India, Professor [2]Jaspreet Kaur, Dept of Electronics and Communication Engineering, Punjab, India.

Abstract : Users want wireless connectivity irrespective of their geographic position. Black hole attack in which the traffic is redirected to such a node that actually does not exist in the network. MANET must have a secure way for transmission, communication with one another nodes. In order to provide secure communication and transmission, researcher worked specifically on the security issues in MANET. Many secure routing protocols and security measures in to the networks were propose. The scope of this thesis is to study the Black hole attack in MANET. State Routing and Reactive routing protocol Ad Hoc on Demand Distance Vector. The impact of Black Hole attack on the performance of MANET is finding out which protocol is more vulnerable for attack and how much is the impact of the attack on network.

Key Word : (Black Hole, Protocol, MANET, Ad Hoc)

INTRODUCTION

MANET is stands for Mobile ad hoc network also called as wireless ad hoc network. MANET nodes are moves randomly as the network topology changes automatically. Each node is doing well to connect the different network in to one. MANET is just a part of larger internet. The challenge for the MANET is to equipped each device to continuously maintain the information required to properly route traffic.

Characteristics of MANET

Dynamic Topologies: network topology which is typically multi hops, it is changeable topology which can be linked with other networks.

Bandwidth constrained, variable capacity links:

Wireless links usually have lower reliability, efficiency, stability, and capacity as compared to wired network.

Autonomous behaviour: Each node can act as a host and router, which shows its autonomous behaviour.

Energy: as some or all the nodes rely on batteries or other usage means for their energy. Mobile nodes are connected with less memory power and space in the connection of the network. Wireless network are more prone to security, routing, and host configuration.

MANET face various threats like attacks that perform against them to interrupt the normal performance of the networks. In these attacks, black hole attack is one type of attack which occurs in Mobile Ad hoc network. Here I need to described black hole attack and other attacks that act against mobile ad hoc network. The routing method is complicated analysis. In black hole attack, a harmful node uses its routing technique to be able to promote identify. In this paper, performance of one of the most efficient solutions for preventing single black hole attack in MANET. This paper explain the introduction ground of the study, research objectives and questions, the scope of the study and its primary objectives.

Literature survey

Narender et al. [1] (a) Detection and Removal of Black Hole Attack in Vehicular Ad-Hoc network Using secure AODV Routing Algorithm.

(b) He suggests some ways like route discovery and route maintains.

Musau et al. [2] PREVENT BLACK HOLE ATTACK IN MOBILE AD-HOC network. (a) He explain the attacks on MANET and also detected it.

Balamurugan et al. [3] Black Hole Detection in AODV Using Hexagonal Encryption in MANET's.

V. Pawar et al. [4] Intrusion Detection and Prevention in WSN and MANET using Machine Learning Techniques and Existing Challenges.

Mwangi et al. [5] Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in MANETs Using NS-3.

M. Yaseena et al. [6] Enhanced AODV Protocol for Avoiding Black Holes in MANET

Kulkarni et al. [7] Prevention of Black Hole Attacks in AODV Based Manets Using Secure Route Discovery.

Begum1 et al. [8] An Efficient & Secure Timer Based Baiting Approach to Detect Black Hole Attacks in MANET

F. Taylor et al. [9] Mitigating Black Hole Attacks in Wireless Sensor networks Using Node-Resident Expert Systems.

Alee et al. [10] Analysis of Black hole Attack in Ad hoc On-Demand Distance Vector (AODV) Routing Protocol: Vehicular Ad-hoc networks (VANET) Context.

D Sheela et al. [11] Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor networks using Mobile Agents with Several Base Stations.

Bhalerao et al. [12] Detection of Blackhole Nodes Categories Based on Trust Values for Securing Wireless Sensor Network Using Matlab.

S. Joshi et al. [13] Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach.

Reddy et al. [14] Semantic Probabilistic Modelling of novel routing Protocol with Implication of Cumulative Routing Attack in Mobile ad hoc network.

Problem Formulation

According to the all software programming there is machine learning is the best processing language for problem formulation of black hole Attack in Mobile Ad hoc network. With these empirical studies I have studied that the relationship between machine learning and NS2.

They both detected the attack with the very fine way and these simplification techniques and their methods. The black hole attack are easy to verified after they shared their methods. Mwangi et al. [5] Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in Mobile Ad hoc network Using NS-2. when Ever I went through all of these methods really appreciate the (Reddy et al. [14] Semantic Probabilistic Modelling of novel routing Protocol with Implication of Cumulative Routing Attack in Mobile ad hoc network) with his method I cleared about the black hole attack because this attack is held between user and network.

But I thought that probability is not free from errors and they will not justify the way we found to simplify the black hole attack identify and solve.

The challenge is raised how to fix the probability routing attack in the Mobile Ad hoc network.

Objectives

1. Black hole attack is one of the different types of attack for detection and prevention upon the mobile ad hoc network.

2. The study on the software of Jupyter notebook for detection and prevention of the black hole attack. In this study we are going to find the relationship between probable attack in ad hoc network and black hole attack in MANET.

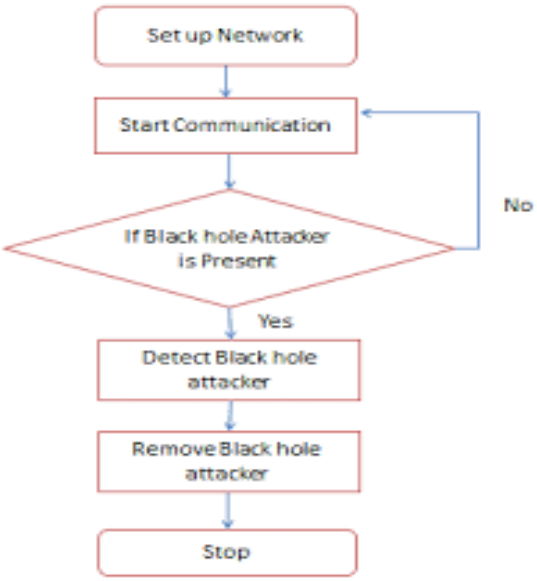
3. After knowing all those effects their best way for exception handling is showing in Graphs and execution the source code.

4.Black hole attack is exception and solution is catch with using Jupyter notebook server Backend as console.

5. Study on different Ad hoc network attack removing ways. To study and compare the output of the Attack before and after conditions in.

6.The error perdition can be more in detail. In this paper required conducting the open source like Jupyter notebook.

Methodology Followed



CONCLUSION

In the current study I discussed that the weakness of AODV routing protocol of black hole attack. The important analysis is to be mentioned here is that all these techniques are well working under single black hole attack.

Research Gap

It is a big problem is how to identify the black hole attack in MANET and how to simplify it and correct it in an easiest way by using different methods.

The main problem in black hole attack is it is not secure and not even trustful after all researchers because the research gap between the black hole attack is not secure.

Comparison of Results

In April 2020 a research work for Black Hole Attack Prevention in Mobile Ad-hoc network connection (MANET) Muhammad Aslam [15] In that research the Authors achieved 512 Throughputs and 200 packets loss with 8 numbers of nodes.

REFERENCES

1) Kumar et al. [1] (A) Detection and Removal of Black Hole Attack in Vehicular Ad-Hoc network Using secure AODV Routing Algorithm.
2) (B) He suggests some ways like route discovery and route maintains.
3) MUSAU et al. [2] PREVENT BLACK HOLE ATTACK IN MOBILE AD-HOC network. (a) He explain the at Ant Colony Optimization Technique optimization was presented by the two authors Imran Muja did Rabbani*, Maitakes on MANET and also detected it.
4) Balamurugan et al. [3] Black Hole Detection in AODV Using Hexagonal Encryption in MANET's.
5) V. Pawar et al. [4] Intrusion Detection and Prevention in WSN and MANET using Machine Learning Techniques and Existing Challenges.
6) S. Bansal et al. [5] Optimized Trust-Based DSR Protocol to Curb Cooperative Blackhole Attacks in MANETs Using NS-3.
7) M. Yaseena et al. [6] An Enhanced AODV Protocol for Avoiding Black Holes in MANET.
8) Kulkarni et al. [7] Prevention of Black Hole Attacks in Word-based Manets Using Secure Route Discovery.
9) Begum1 et al. [8] An Efficient & Secure Timer Based Baiting Approach to Detect Black Hole Attacks in MANET.
10) F. Taylor et al. [9] Mitigating Black Hole Attacks in Wireless Sensor networks Using Node-Resident Expert Systems.
11) Alee et al. [10] Analysis of Black hole Attack in Ad hoc On-Demand Distance Vector (AODV) Routing Protocol: Vehicular Ad-hoc networks (VANET) Context.

12) D. Sheela et al. [11] Mollifying the Effect of Cloning, Sink Hole and Black Hole Attacks in Wireless Sensor networks using Mobile Agents with Several Base Stations.
13) Bhalerao et al. [12] Detection of Blackhole Nodes Categories Based on Trust Values for Securing Wireless Sensor Network Using MATLAB.
14) Chang et al. [13] Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach.
15) Reddy et al. [14] Semantic Probabilistic Modelling of novel routing Protocol with Implication of Cumulative Routing Attack in Mobile ad hoc network.
16) Rabani et al. [15] Black Hole Attack Prevention in Mobile Ad-hoc network Using Ant Colony Optimization Technique optimization.