Performance Analysis of Black Hole Attack in VANET

Kirti Kaushik[1], Sandeep Tayal[2]

[1]Mtech, Student, [2]Associate Proffesor

Department of Electronics and Communication.

Vaish College Of Engineering, Rohtak, Haryana, India.

Abstract

Vehicular Ad-hoc Network systems (VANETs) are a particular type of the Mobile Ad-hoc Networks systems (MANETs) to provide communications among nearby vehicles. VANET is mostly planned to make available safety related information by warning drivers about road conditions, accidents and traffic management by helping drivers to discover the best available path to their destination. A number of distinctive properties make VANETs vulnerable for attackers to exploit and to decrease the normal performance of the networks. Black hole attack in Vehicular Ad Hoc Network is the most severe problem associated with the field of computer networking where the black node absorbs all the data packets in the network. In Black hole attack, a malevolent node utilizes its routing protocol in order to announce itself for having the direct path to the destination node. The main target of the paper is to measure the impact of Black hole attack on the VANET's AODV routing protocol. Measurements of several parameters with inclusive analysis and comparisons are presented.

Introduction

Vehicular Ad-hoc Network systems (VANETs) are the network with no fixed infrastructure. VANET facilitate various other applications [1] in the domain of vehicular communication. Vehicular ad hoc network has many unique features [2]. The distinctive characteristics [3] of a VANET atmosphere are a area under discussion of significance for many. Thus characteristics of VANET create both network design challenges [4] and opportunities in achieving security goals. These are the dynamic wireless network where the nodes move randomly. Any node can come and move in and outside of the network in a dynamic manner. VANETs are an open transmission and communication media without any safety means. This makes it more complex and also makes it more prone to attacks. .As the traffic increases over the VANET it will leads to number of troubles i.e. congestion and packet loss .This congestion control[5] and packet loss problems occurs due to the attack in VANET. Black hole attack is one of the security threats where the black node collects all packets by falsely declaring a fresh route to the destination node and absorbs them without forwarding them to destination. As a result some packet loss over the network slows the communication process.

In this paper we present the performance analysis of the black hole attack in Vehicular Ad Hoc Network. The performance metric is taken for the evaluation of attack which depends on Generated packets, Received packets, Dropped packets, Average End-to-End Delay and Routing overhead values for no black hole and multiple black holes. In VANET different types of routing protocols [6] have been recommended. But here these parameters are compared for AODV routing

protocol both using with black hole attack and without black hole attack. The main security requirements for VANETS [7] [8] are also considered. Simulation shows that AODV has high performance in terms of these parameters in absence of black node. Simulation is carried using Network Simulator (NS2) 2.35. An introduction of black hole in VANET with NS2 (2.35) is done, after applying the detection technique result reflects the performance. The simulation setup comprises of 27 Vehicular nodes moving with constant packets transmission rate of 0.1Mb.

Black Hole Attack

A black hole is an area in the network where either there is no node in that area or the nodes residing in that area refuse to participate in the network. In a black hole attack, a malevolent node introduces itself for having the direct path to the destination node and thus, cheats the routing protocol. As a result, the attacker node is able to intercept the data packet or retain it. When the forged route is successfully established, it depends on the malicious node whether to drop or forward the packets to wherever it wants.

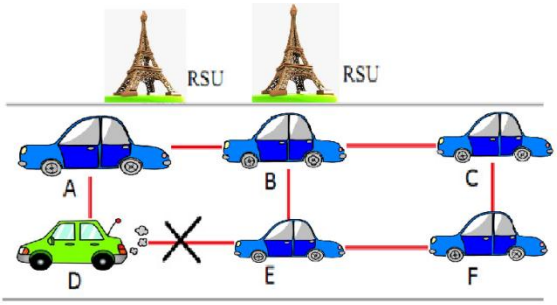

Fig.1 Black Hole Attack

Fig. 1 demonstrates an example where the node A wishes to send data packets to node F but, it is not be familiar with the route to F. Therefore, A starts the route discovery process. As a malicious node, D claims that it has active route to F and acts to be next-node if A wants to send packets to F.

Simulation Environments

The aim of this paper is to study the impact of Black hole attack on the performance of VANET All of the simulation is carried out by Network Simulator (NS2) 2.35

AODV network performances are as follow:

1. **Generated Packets**

This represents the total number of packets generated by all nodes in the network.

2. **Received Packets**

This represents the total number of packets received by all nodes in the network.

3. **Dropped Packets**

This represents the total number of packets discarded by all nodes in the network.

4. **Average End-to-End Delay**

This is the average time that a packet takes to traverse from the source node to the destination node in a network.

5. **Routing overhead**

Routing overhead is the number of control packets that are needed (for route discovery/maintenance) to transport data packets to their destinations successfully.

Simulation and Results

We have used the Network Simulator (NS2) 2.35 in our evaluation. In our scenario we simulate 27 nodes and it distributes over 2010*1010 Terrain areas in NS2. Number of nodes was kept constant and number of Black nodes was varied. CBR traffic is sent in form of packets over the UDP connection. The simulation starts at 10.0ms and stops at 420ms and again starts at 600ms and stops at 820ms. Here the packet Size is 1000 and packets are sent at rate of 0.1Mb. Two Ray Ground model is used for communication as Propagation model to describe the movement pattern of mobile users which includes their location, acceleration and mobility change over time. Under this, the different performance parameter considered here are Dropped packets, Average End-to-End Delay and Routing overhead values for AODV with no black hole and AODV with multiple black holes.

Simulation Parameters Setup

Here the various Simulation parameters are defined.

TABLE 1 Simulation parameters

Parameters	Values
No. of Nodes	27
Simulation Time	1000.0
Maximum X-coordinate value	2010
Maximum Y-coordinate value	1010
Propagation model	Two Ray Ground
Channel type	Wireless Channel
Routing Protocols	AODV
Data Traffic Rate	CBR
Network interface type	Wireless Phy
MAC type	802_11
Antenna model	Omni Antenna
Attack Type	Black hole Attack

Comparative analysis of performance of AODV and AODV with black hole attack

Generated Packets:

This shows the total number of packets generated by all nodes in the network.

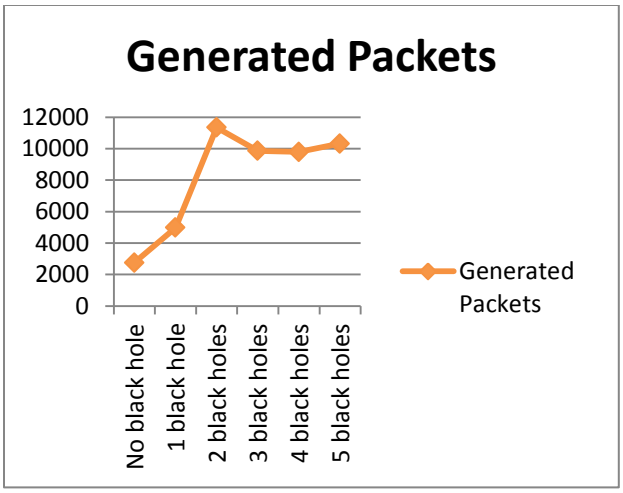

Fig. 2 of Generated Packets of AODV and AODV with multiple black holes

The above graph shows the values of Generated Packets of AODV and AODV with increasing number of black holes. It is clear from the graph that the number of generated packets is less in absence of black holes, but when the black nodes get introduced in network then it severely affect the security of vehicular communication. **This black node introduced itself for having the direct path to the target node and thus claims to be the genuine source**.

As the number of black hole increases, number of sources also increases. So there is an increase in number of generated packets with increase in number of black holes. But after certain limit the number of generated packets remains same due to chaos in the network. Fig. 2 shows that as the black holes are introduced, the number of generated packets increases.

Received Packets:

This represents the total number of packets received by all nodes in the network.

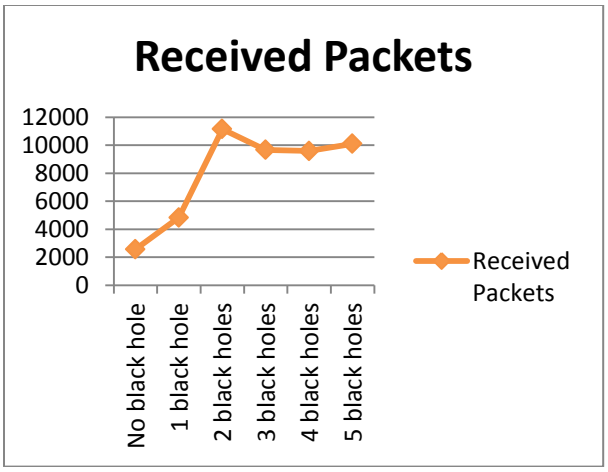

Fig. 3 Received Packets of AODV and AODV with multiple black holes

The above graph shows that the number of received packets is less for no black hole condition. The introduction of black nodes in the network results in generation of more and more packets. As the number of black hole increases, number of sources also increases so there is an increase in number of received packets with increase in number of black holes. But after certain limit the number of received packets remains same due to heavy traffic in the network. Since the generated packets increases more packets are received by the nodes as shown in fig. 3.

Dropped Packets:

This represents the total number of packets discarded by all nodes in the network.

The black nodes mislead the routing protocol. The malicious node collects the packets from other sources. As a result, the attacker node was capable to seize the data packet or retain it. When the fake route was successfully established, the malevolent node could either drop or forward the packets to wherever it wants.

Fig.4 shows that when there is no black hole attack then the number of dropped packets is very less. When the number of malicious nodes increases then it results in dropping of more and more packets.

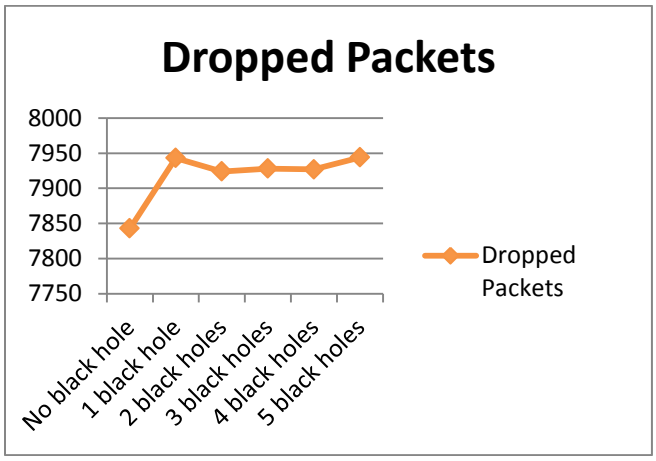

Fig. 4 Dropped packets of AODV and AODV with multiple black holes

Average End-to-End Delay:

This is the average time that a packet takes to traverse from the source node to the destination node in a network.

In VANETs, the communication takes place among various nodes. These nodes communicate by sending data in form of packets. The communication between adjacent nodes is quite simple as it requires transmission of packet to its neighbouring node. Difficulty arises when communicating nodes are far apart and there are a number of nodes in their path. In such a case usually the packet is delivered from the source to destination by passing it through the intermediate nodes which comes into its way to the target node. Thus the packet is received at the target node after some time and this delay in reception is termed as Average End to End Delay.

When there is no malicious node in the network then the value of this delay is small. As the number of black nodes increases in the network the Average End to End Delay increases. The presence of black nodes in the network enhance the Average End to End Delay of AODV because the malicious nodes sometimes hold the packets with them and forward these packets whenever they want. Fig. 4.5 shows the Average End to

End Delay of AODV and AODV with multiple black holes.

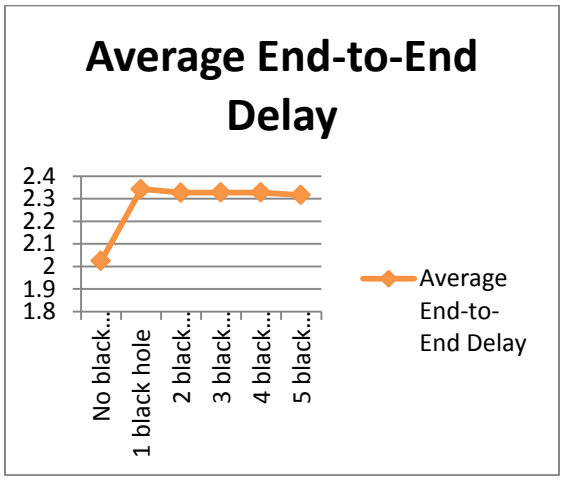

Fig. 4.5 Average End to End Delay of AODV and AODV with multiple black holes

Routing overhead:

Routing Overhead is defined as the total number of control packets that has been transmitted per data packet. It is obtained by dividing the total number of control packets sent by the total number of data packets received by destination.

When data is send in form of packets over the channel then some additional information is also send along with the useful information. This additional information is sent in the control packets. The control packets tell the receiver about number of number of data packets that are actually transmitted by the sender node and it also carry the acknowledgements that are conveyed by the receiver back to the sender for assuring the reception of data packets. Thus the control packets consume the bandwidth that is reserved for transmission of data packets.

Routing overhead help us to know how many control packets are required (for route detection/maintenance) to move data packets to their destinations effectively. It specifies the amount of traffic in entire network. It shows the total data traffic in bits per seconds received by the whole network from higher layer acknowledged and queued for communication. As the number of nodes increases, path discovery becomes more complex and large quantity of overhead is added in communication.

When there is no black hole attack in the vehicular communication network then the value of Routing overhead obtained after simulation is small. But when the black hole attack is introduced, then the problem starts. As the number of black nodes increases the routing overhead value increases.

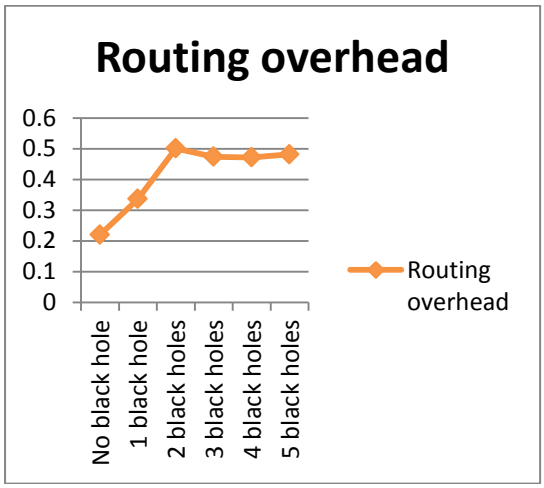

Fig. 4.6 Routing Overhead of AODV and AODV with multiple black holes

It is shown in fig.4.6 that the Routing Overhead of AODV with no black node is comparatively lesser than the AODV with black hole attack. The existence of a number of black node increases the Routing Overhead.

Conclusion & Future Scope

VANET is an attack prone methodology which meets attack at every instance of time. . In this work we studied how attackers could endanger the secure vehicular communication. In this paper we examined the most fundamental problem of black hole

attack regarding security of VANETs. We implemented the most dangerous black hole that pretends itself for having the shortest path to the target node. We examined the impact of the presence of black nodes on secure communication. We examined that when there is no malicious node in vehicular network then the communication was secure but the presence of malevolent node has disturbed the network operations by increasing the number of the various performance parameters. In the future, extensive complex simulations could be carried out, in order to gain a more in-depth performance analysis of the different black hole removing routing protocol. The efforts will be needed to develop new modified protocol which will also perform better with energy consumption metric, fewer overheads and compare its performance with existing protocol. Other new protocol performance could also be studied.

References

[1] Elmar Schoch, Frank Kargl, and Michael Weber, "Communication Patterns in VANETs" IEEE Communications Magazine , November 2008.

[2] Jie Luo Xinxing "MI-VANET: A New Mobile Infrastructure Based VANET Architecture for Urban Environment" 1-4244-3574-6,2010 IEEE

[3] T. H. Tee, Alex C. R. Lee "Survey of Position Based Routing for Inter Vehicle Communication System"

[4] Nur Diana Mohd. Nuri, Halabi "Strategy for Efficient Routing in V ANET" 978-1-4244-6716-711, 2010 IEEE

[5] Lars Wischhof and Hermann Rohling "Congestion Control in Vehicular Ad Hoc Networks" 0-7803-9435-6, 2005 IEEE.

[6] Harsh Trivedi, Prakash Veeraraghavan, Seng Loke, Aniruddha Desai, "Routing Mechanisms and Cross-Layer Design for Vehicular Ad Hoc Networks: A Survey" 2011 IEEE Symposium on computers and Informatics

[7] Vinh Hoa LA, "SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY" International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014

[8] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux "Secure Vehicular Communication Systems: Design and Architecture"