International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

A Probabilistic Black Hole & Gray Hole Attacks Detection Scheme for Vehicular Ad-Hoc Network

Arpita Rathod[1], Prof. Shreya Patel[2]

[1, 2]Grow More Faculty of Engineering Himatnagar, Gujarat, India

Abstract: ***Vehicular Ad-hoc Network is a technology which conduce the vehicle to interconnect with each other through a wireless network. So that it can way and locate other vehicles to manage road safety. Security is a major issue in vehicular ad-hoc network as it can be people's life in danger. The black hole attack is a pattern of a denial of service attack that makes a difference for data traffic in VANET. A gray hole attack is a technique in which the vindictive node just drops the packet from some decided node in the network and forwards all other packets to its destination. We will provide a suitable solution for a low solidity network where each car moves in a straight line and submit or assign packets to other neighboring cars using a routing protocol. NS2 is a simulation tool which is used to design and imitate our proposed method. I analyzed variable parameters like a packet delivery ratio(PDR) , delay and throughput.***

Keywords: VANET, RSU, black hole attack, gray hole attack

1. Introduction

- **VANET**

Vehicular Ad Hoc Network(VANET) is a technology which conduce the vehicle to interconnect with each other through a wireless network. Vehicular ad hoc networks (VANETs) are appoint by applying the principles of mobile ad hoc networks (MANETs) the spontaneous creation of a wireless network for data exchange to the domain of vehicles. It was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures will co-exist in VANETs to provide road safety, navigation, and other roadside services [1]. VANETs are a key part of the intelligent transportation systems (ITS) framework.

In VANET, There are many attacks harm the networking system. So the detection of that attacks we will using many different schemes. For my purposed method, I choose detection of black hole and gray hole nodes at the same time in a system using reactive routing protocols such as AODV. Then such purposed mechanism is below:

- **Attacks In VANET**

There are various types of attacks that can affect the entire system or can mortify the execution of system. These attacks can be marked into subsequent types:

1) Impersonation Attack
2) Denial of Service Attack
3) Routing Attack
   - Worm Hole Attack
   - Black Hole Attack
   - Gray Hole Attack
4) Sybil Attack
5) Timing Attack

a) Black Hole Attack

In this type of attack, the attacker firstly engage the nodes to transferring the packet through itself. When some malicious user enter into the system's network and stop along messages to next nodes by releases messages are called as black node.

When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node[3].

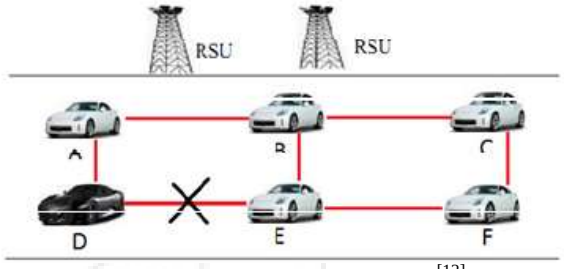


Figure (a): Black Hole Attack[12]

b) Gray Hole attack

This attack happen if some node dropping 50% of the packets and rest 50% is sending by transfering the message. In this way wrong data is broadcast. A Gray hole is a technique in which the spiteful node just drops the packet from some specific node in the network and forwards all other packets to its destination. This is the addition of black hole attack[3].

In this type of attack the malicious node behaves like a black node but it releases the packets selectively.

Figure (b): Gray Hole Attack[2]

2. Proposed Mechanism

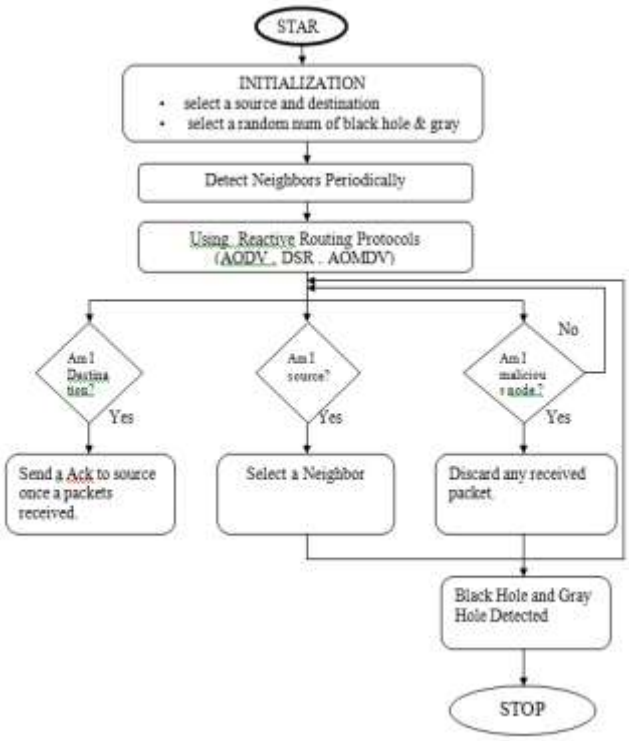


Figure 2: Flow Chart of Proposed Work

Algorithm Steps:

1. Begin(Start)
2. Select Source and Destination
3. Select Random Number of Black Hole and Gray Hole Nodes.
4. Detect Neighbors Periodically
5. Using Reactive Routing Protocols such as AODV , DSR , AOMDV
6. Sequence Number Identification
7. If the node is Destination than Send an acknowledgement to source once a packet received.
8. If the node is Source than Select a neighbor node.
9. And If finally the node is Malicious Node(Black hole node and Gray hole node) than Discard any received packet.
10. Otherwise again check the identification of nodes and above process is continue .
11. When Discard any Received packet in Network , After that Detect the Black Hole and Gray Hole Nodes.
12. End While.

3. Software Requirements:

Simulation : NS version 2.35
Language : TCL, AWK Script and C++
Operating System : Ubuntu 14.04 LTS 64-bit
Road Map and Mobility Generator : SUMO and MOVE

3.1 Experimental Setup

An Improved AODV protocol is designed by modifying iaodv.cc and iaodv.h files according to the proposed method and ns2 is rebuilt with newly added protocol in VANET.

Performance of the proposed IAODV is evaluated for the simulation settings as per the following simulation model and compared with original AODV. Metrics such as packet delivery ratio, Average End-to-End delay and control overhead are evaluated using awk script by analyzing trace file for the attacker scenarios.

Using the results obtained from awk script graph is plotted for performance metrics using graph tool available in ns2.

3.2 System Model

In Vehicular Ad Hoc Network, nodes N are moving in the road map model generated using SUMO and MOVE. Communication between source S Є N and Destination D Є N is established dynamically.

The routers between S and D are r1, r2, r3...rn where, n is the path length. Communication flow between source and destination pair is established dynamically.

The randomly chosen source-destination pairs are spread in the network.

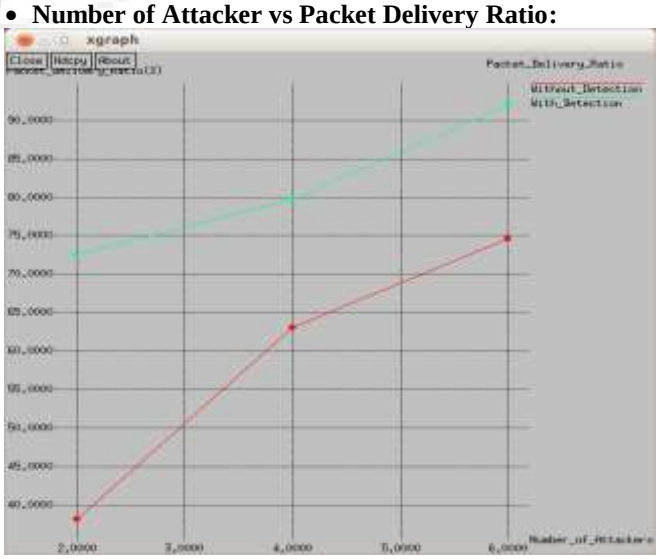
3.3 Simulation Model

Table 3: Simulation model

Simulator	Network Simulator 2
Number Of Nodes	60
Interface Type	Phy/ WirelessPhyExt
Mac Type	802.11Ext
Queue Type	DropTail / PriQueue
Queue Length	50 Packets
Antenna Type	Omni Antenna
Propagation Type	TwoRayGround
Routing Protocol	AODV
Transport Agent	UDP
Application Agent	CBR
Simulation Time	200 seconds
Packet Size	512
Network Area Size	600 * 600

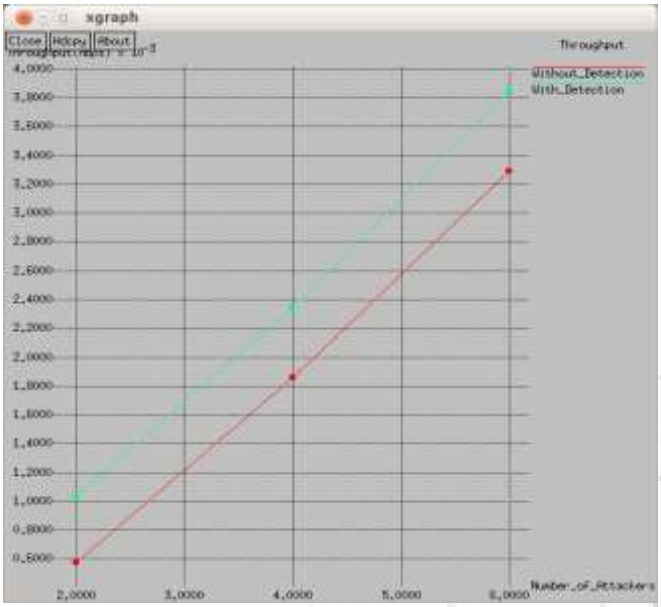
4. Comparison Graph:

- **Number of Attacker vs Packet Delivery Ratio:**



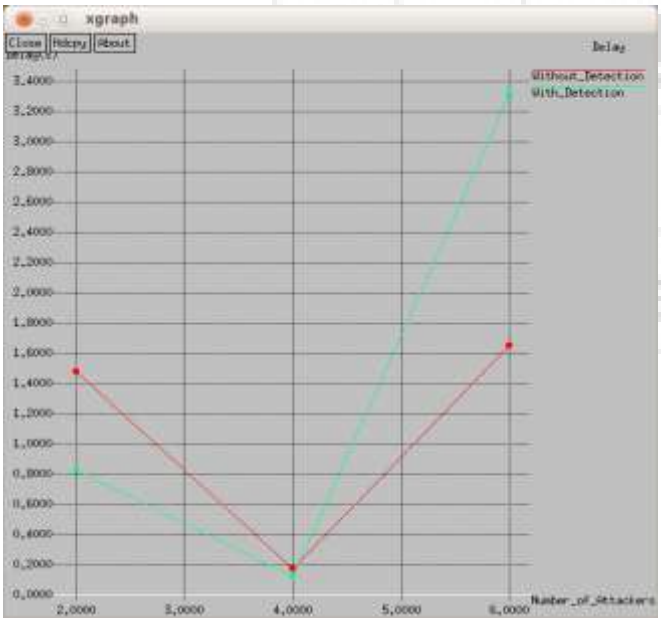
When the number of attackers are varied packet delivery ration is increased. With detection scheme provides better packet delivery ratio compared to existing without detection scheme.

- **Number of Attacker vs Throughput :**



When the number of attackers are varied throughput is increased. With detection scheme provides better throughput compared to existing without detection scheme.

- **Number of Attacker vs Delay:**



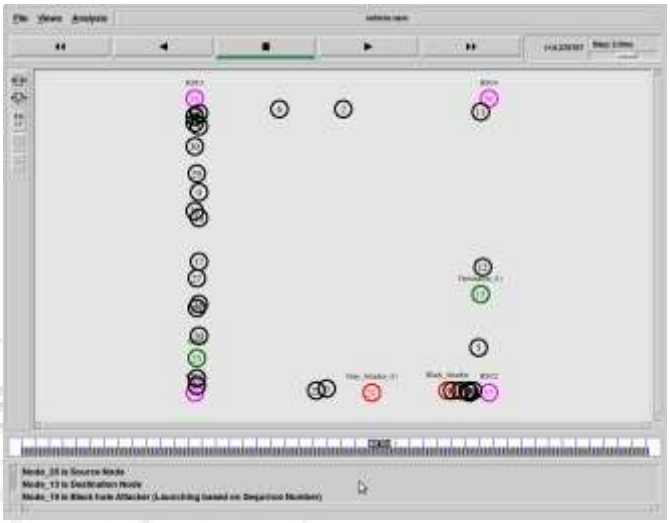
When the number of attackers are varied delay is similar performance for with and without detection schemes

- **Scenario:**

With detection of attacker and without detection of attacker schemes are compared for the scenarios of varying number of attackers. Scenario is kept same for both schemes with same topology, source, destination and number of nodes. Totally 3 simulation runs are made by varying number of attackers as 2, 4, and 6. Parameters such as packet delivery ratio, throughput and delay are computed and plotted as Xgraph.

5. Implementation Result

Without Detection of Attacker in AODV

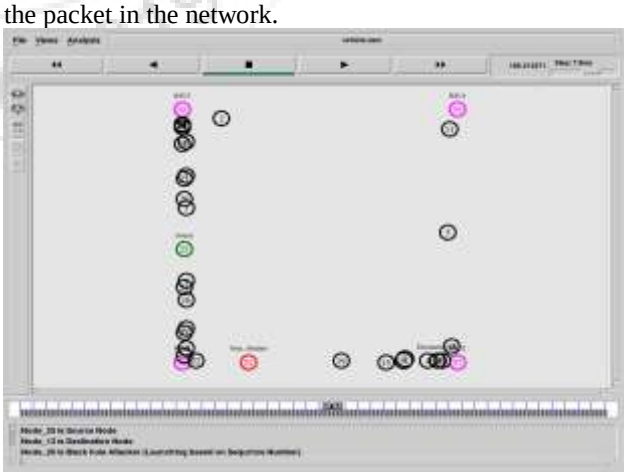


Attacker node send false route reply that it contains a highest destination sequence number. But originally it does not contain shortest route. Now source node receives multiple RREP, it accepts greater sequence number RREP and ignores lesser in normal AODV routing process.

In AODV Routing protocol higher sequence number denotes the fresh information of the network. Hence source node sends the data packets to attacker node. The attacker node drops the all the data packets. So performance is degraded.

- **Gray hole Attacker Creation:**

Node 21 is an attacker node, which node selectively drops the packet in the network.



Result:

	With Detection of Attacker			Without Detection of Attacker		
Varying number	2	4	6	2	4	6
Delay	0.8244s	0.1179s	3.3152s	1.4755s	0.1690s	1.6457s
Throughput	0.00103s	0.00234s	0.00384s	0.00057s	0.00185s	0.0032s
Packet delivery ratio	72.5s	79.761s	92.063s	38.095s	63.095s	74.603s

6. Conclusion

It analyzed possible VANET security threats and mainly focuses on black hole attack and gray hole attack both . Comparison of reactive routing protocol AODV of with or without detection of attacker is carried out. After all experiments in Base Paper, they conclude AODV performance is better than other routing protocols with and without black hole attack and gray hole attack. AODV is more scalable than other routing protocols. AODV is better routing protocol to be deployed in VANET.

In the future work we will focus on detection of Black hole and Gray hole Attacks using other reactive routing protocols such as DSR and AMODV in VANET.

References

[1] Irshad Ahmed Sumra, Iftikhar Ahmad, Halabi Hasubullah, Jamalul-lial bin Ab Manan , “Classes of attacks in VANET”, IEEE- 2011.
[2] Swati Verma,Bhawna Mallick, Poonam Verma , Impact of Gray Hole Attack in V ANET ,IEEE, 2015
[3] Dilendra Shukla ,AkashVaibhav, Sanjoy Das, Prashant Johri, Security and attack analysis for Vehicular Ad hoc Network- A Survey ,International Conference on Computing, Communication and Automation,2016
[4] Ms Annu , Ms Sarul, “Comparative Study of Black Hole Attack on VANET” ,Volume 5, Issue:5, Sep-Oct 2015.
[5] Mohammed Saeed Al-kahtani, “Survey on Security Attacks in Vehicular Ad hoc Networks(VANETs)” ,IEEE-2012.
[6] Manjyot Saini , Harijit Singh, “VANET, its Characteristics , Attacks and Routing Techniques: A Survey”, International Journal of Science and Research, Volume 5, Issue:5, May 2016.
[7] Ujwal Parmar , Sharanjit Singh, ”Overview of Various Attacks in VANET ”, International Journal of Engineering Research and General Science , Volume 3, Issue 3 , May-June 2015.
[8] M.Newlin Rajkumar, M.Nithya ,P.HemaLatha, “ OVERVIEW OF VANET WITH ITS FEATURES AND SECURITY ATTACKS”, International Research Journal for Engineering Technology, Volume: 03 Issue: 01 | Jan-2016
[9] Sikha Sharma , Er. Shivani Sharma ,”A Review: Analysis of Various Attacks in VANET” ,International Journal of Advance Research in Computer Science, Volume 7 ,No.3 ,May-June 2016.
[10] Vinh Hoa LA, Ana CAVALLI ,” SECURITY ATTACKS AND SOLUTIONS IN VEHICULAR AD HOC NETWORKS: A SURVEY”, International journal on Adhoc Networking Systems, Volume:4, No.2, April 2014.
[11] Bharti, D.P.Dwivedi , “Performance Analysis of Black Hole Attack with AODV using Different no. of Nodes in VANET ”, Volume 5, Issue:7 , July 2016.
[12] A. Malathi, N. Shreenath ,”Black Hole Attack Prevention and Detection in VANET USING Modified DSR protocol”, Volume 168, No.7, June 2017.
[13] Hanin Almutairi, Samia Chelloug, Hanan Alqarni, Raghda Aljaber, Alyah Alshehri ,” A New Black Hole Detection Scheme for Vanets ” ,ACM 2014