International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# IDS System against Gray Hole Attack in VANET

**Gurtej Kaur[1], Amandeep Kaur[2]**

[1]Punjab Technical University, Sri Sukhmani Institute of Engineering and Technology, Derabassi, Punjab

[2]Sri Sukhmani Institute of Engineering and Technology, Derabassi, Punjab, Punjab Technical University

**Abstract:** ***In this paper various approaches used for gray hole attack in VANET. Gray hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network VANETs must have a secure way for transmission and communication which is quite challenging and vital issue.***

**Keywords:** malicious nodes, VANET, gray hole node, IDS, attacks in VANET.

## 1. Introduction

### 1.1 VANET

VANET uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns turn participating car into a wireless router or node which allowing cars 100 to 300 meters of ea ch other to connect and create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile network is created. It is estimated that the first systems that will be this technology are police and fire vehicles to communicate with each other for the purpose of security.[1]

Vehicular Ad-hoc Network (VANET) is not a new topic; it continues to provide new research challenges and problems. The main objective of VANET is to help a group of vehicles to set up and maintain a communication network among them without using any central base station or any controller. One of the major applications of VANET is in the critical medical emergency situations where there is no infrastructure while it is critical to pass on the information for saving human lives. However, along with these useful applications of VANET, emerge new challenges and problems. Lack of infrastructure in VANET puts additional responsibilities on vehicles. Every vehicle becomes part of the network and also manages and controls the communication on this network along with its own communication requirements Vehicular ad-hoc networks are responsible for the communication between moving vehicles in a certain environment. A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V) communication, or a vehicle can communicate to an infrastructure such as a Road Side Unit (RSU), known as Vehicle-to-Infrastructure (V2I). The main contributions of this research are to present state – of – the - art in VANET technology. A detailed study of network architecture with different topologies and network modeling is presented in this paper. A key design area in VANET in order to properly form a communication network is routing the packets in effective manner. The paper discusses different routing algorithms for VANET and presents limitations of those algorithms. Security issues in VANET environment are also addressed in the paper so that trustworthy network architecture can be modeled.

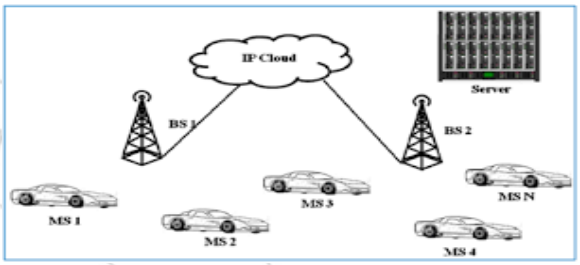


**Figure 1.1:** VANET

### 1.2 Security Requirements of VANET'S

#### 1.2.1 Authentication

Authentication is a major requirement in VANET as it ensures that the messages are sent by the actual nodes and hence attacks done by the greedy drivers or the other adversaries can be reduced to a greater extent.

#### 1.2.2 Message Integrity

This is very much requires as this ensures the message is not changes in transit that the messages the driver receives are not false.

#### 1.2.3 Message Non-Repudiation

In this security based system a sender cannot deny the fact having sent the message. But that doesn't mean that everyone can identify the sender only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends.

#### 1.2.4 Entity authentication

It ensures that the sender who has generated the message is still inside the network and that the driver can be assured that the sender has send the message within a very short period. Access control it is required to ensure that all nodes function according to the roles and privileges authorized to them in the network.

#### 1.2.5 Message confidentiality

It is a system which is required when certain nodes wants to communicate in private. But anybody cannot do that. This can only be done by the law enforcement authority vehicles to communicate with each other to convey private information. An example would be, to find the location of a criminal or a terrorist.

**1.2.6 Privacy**
This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information Third parties should also not be able to track vehicle movements as it is a violation of personal privacy.

**1.2.7 Real time guarantees**
It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety related applications such as collision avoidance is met.

**1.3 Possible Attacks in VANET**

VANET is facing many attacks and these attacks are discussed in the following subsections:

**1.3.1 Denial of Service Attacks**
DOS attacks can be done by the [9] network insiders and outsiders and give the network not available to real users by flooding the control channel with high sound of naturally generated messages and stops the network connection. As a result OBU and RSU are unable to process the capacity sufficiently.

**1.3.2 Broadcast Tampering**
An inside assault may inject [9] false safety messages into the network to cause damage such as causing an accident by suppressing traffic rules or manipulating the flow of traffic around a chosen route.

**1.3.3 Sybil Attack**
This attack, [6] forges the identity of multiple vehicles. Those identities can be used to cast any type of attack on the system. These false identities also create an illusion that there are additional vehicles on the road and spoof the positions of other nodes in the network.

**1.3.4message Suppression Attacks**
An attacker selectively drops packets from the network, and these packets may hold critical [8] information for the receiver. The attacker suppresses these packets and may use them again when required [8]. The goal of this attack is to prevent registration and insurance authorities from learning about collisions about the vehicle and/or to avoid delivering collision reports to RSU.

**1.3.5 Alteration Attack**
This attack happens when an attacker alters an [8] existing data. An alteration attack includes delaying the transmission of the information, replaying earlier transmission, and also altering the actual entry of the data transmitted.

**1.4 Gray Hole Attack**

In gray hole attack, a node that is a member of the network, gets RREQ packets and creates a route to destination. After creating route, it drops some of data packets. This kind of dropping against Gray hole, does not drop all data packets. Attacker drops occasionally packets. It means attacker sometimes acts like a normal node and other times as a malicious node. [4]The Gray Hole attack has two phases. Initially, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. Next, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the Gray Hole attack where the malicious node drops the received data packets with certainty. A Gray Hole may exhibit its malicious behavior in various techniques. It simply drops packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of Gray Hole attack is a node behaves maliciously for some particular time duration by dropping packets but may switch to normal behavior later. A Gray Hole may also exhibit a behavior which is a combination of the above two, thereby making its detection even more difficult.

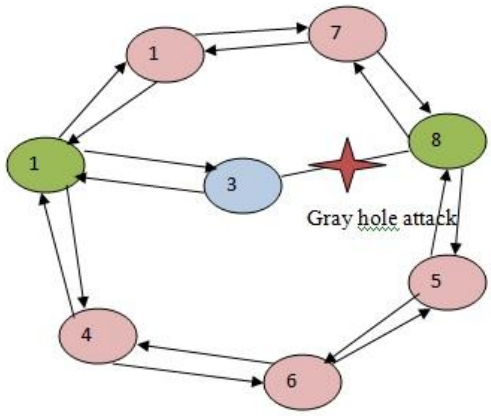


**Figure 1.3:** Gray Hole Attack

## 2. Literature Review

**Swati Verma et.al[1]** "Impact of Gray Hole Attack in V ANET" Vehicular Ad Hoc Network(VANET) is a technology which accommodate the vehicle to interconnect with each other through a wireless network. So that it can track and locate other vehicles to provide road safety. Any fixed infrastructure is missing so effective route for transporting data communication is established. Security is a major issue in VANET as it can be life threatening. V ANET is a subclass of ad hoc network and it is almost same as Mobile Ad Hoc Networks (MANET) but in V ANET nodes are vehicles. It is a challenging topic because of frequent link disruptions caused by vehicle mobility. We have used AODV routing protocol in VA NET for proper communication between nodes by forwarding data packets. We have implemented the gray hole attack on routing protocol AODV and shown its impact on implementation of VA NET. We have analyzed variable parameters like a packet delivery ratio (PDR), normalized routing load (NRL), delay and throughput.

**Faisal Khan et. al[2]** "Recovering VANET Safety Messages in Transmission Holes" in this paper The core concern in vehicular ad hoc networks (VANETs) is the reliable transfer of safety-related messages to all endangered vehicles on the road. The recent discovery of the presence of

transmission holes in the VANET communication range poses a serious challenge in the reliable safety-message dissemination. In this work, a technique for recovering the safety message for vehicles located in transmission holes is proposed. Each vehicle that successfully receives the safety message actively estimates propagation loss for its immediate neighbors. When the receiving vehicle determines a neighbor located in a coverage hole, the safety message is rebroadcast by the receiving vehicle. The propagation-loss estimation makes use of the topology information appended in the periodic beaconing messages. Contention among multiple rebroadcasters is resolved by using the relay schedule mechanism. The proposed technique is evaluated using a detailed implementation in the ns-3 network simulator. The simulation results suggest that the proposed technique guarantees the safety-message dissemination with a minimal overhead delay of five milliseconds even in the dense-urban traffic scenario.

**Ambuj Kumar et.al[3]** "An Efficient Group-Based Safety Message Transmission Protocol for VANET" Vehicular Ad-hoc Network (VANET) is a type of mobile communication in which topology changes dynamically due to high mobility of vehicles. Vehicles transmit two types of messages to update their status and to communicate with other vehicles. First is Periodic Safety Message (PSM) which gives us information about position, speed etc. and second is Event Driven Safety Message (ESM) which occurs when emergency situation like hard breaking, sudden lane change, etc. When vehicle movement is abnormal either due to change in speed or direction, vehicles generates event-driven safety alert messages. Safety alert messages are needed to be very fast and reliable for VANET applications. In this paper, we proposed a novel type approach to improve safety alert message communication in VANET using grouping of vehicles. Firstly, vehicles form a group and select their Group Leader to communicate with other Group Leaders. Secondly, we send the safety alert message by using priority in the messages and context-based communication. The priority is set according to various types of accidents and by using context-based communication the ESM messages are send to those groups which are endangered by the accidents. Simulation of proposed scheme is performed on multi-lane roads by considering vehicles movement in a single direction. Performance is evaluated in terms of packet delivery ratio and back-off counter for multi-hop broadcast communication.

**Ikechukwu K. Azogu et.al[4]** "A New Anti-Jamming Strategy for VANET Metrics-Directed Security Defense" As Vehicular Ad-hoc Network (VANET) becomes a critical infrastructure for road safety and traffic efficiency, its standardization and deployment faces many serious security challenges. The nature of VANET hinders useless many existing defense schemes that is used for wireless/mobile networks. This paper studies where the impact of jamming on 802.11p, the standard of vehicle-to-vehicle (V2V) communications. Jamming, a category in Denial-of-Service (DoS) attack, which is a legacy in wireless communications. Although some detections and countermeasures of jamming-style DoS attacks have been proposed for generic 802.11 wireless local area networks, where few is tested for 802.11p. Particularly, retreat strategies fail to lessen jammers in VANET as geography may prohibit it from escaping a jammed area, and there is only one control channel for safety critical messages in 802.11p which excludes channel hopping. Likewise, competition strategies such as tuning the carrier sense threshold does not respond fast enough to high-speed mobility. This work proposed a hideaway strategy, suitable for antijamming in VANET. The new strategy is supposed with a novel security metrics to measure the effectiveness of jammers, directing the design of defense mechanisms. The strategy utilizes Roadside Equipments to shoulder off computation and communication tasks from Onboard Equipments. A simulation study measures VANET efficiency which is protected by the new strategy compared to traditional schemes such as channel surfing. The study validates that the VANET security metrics and the metrics directed approach of design for security schemes.

**Claudia Campolo et.al[5]** "Modeling Broadcasting in IEEE 802.11p/WAVE Vehicular Networks" IEEE 802.11p/WAVE (Wireless Access in Vehicular Environments) is an rising family of standards which are used to support wireless access in Vehicular Ad Hoc Networks (VANETs).Broadcasting of data and control packets is expected to be crucial in this environment. Both safety-related and non-safety applications emphasize on broadcasting for the exchange of data or status and advertisement messages. Most of the broadcasting traffic is designed to be delivered on a given frequency during the control channel (CCH) interval set by the WAVE draft standard. The rest of the time, vehicles switch over to one of available service channels (SCHs) for non-safety related data exchange. Although broadcasting in VANETs has been analytically studied, related works neither consider the WAVE channel switching nor its effects on the VANET performance. In this letter, a new analytical model is designed to evaluate the broadcasting performance on CCH in IEEE 802.11p/WAVE vehicular networks. This model explicitly accounts for the WAVE channel switching and computes packet delivery probability as a function of contention window size and number of vehicles.

## 3. Approaches Used

**In-Vehicle Domain:** This domain consists of one or more applications units (AUs) and a single On-Board Unit (OBU) that resides inside a vehicle [19]. Applications Units (AUs) is an in- vehicle entity, where multiple AUs can be plugged within single OBU and share the OBU processing and wireless resources. An On-Board Unit (OBU) is used for providing the vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) communication. An OBU is equipped with a single network device based on IEEE 802.11p radio technology; where network device is used for sending, receiving and forwarding the safety and non safety messages in the ad hoc domain.

**Ad hoc Domain:** This VANET domain composed of vehicles or nodes that equipped with On-Board Unit (OBUs) and road-side units (RSUs), that forming the VANET. A

road side unit is a physical device located at fixed positions and used in hospitals, shopping complexes, colleges, road highways etc. An RSU is equipped with at least a network device based on IEEE 802.11p standard. The main function of RSU is to provide the internet connectivity to the OBUs. On-Board Units (OBUs) form a Vehicular ad hoc network that allows communications among vehicles without the need of a centarlized coordination instance. Two vehicles directly communicate via On-Board Units (OBUs) if there is any wireless connectivity exists between them; else multi-hop communications are used to forward data [30]. Infrastructure Domain: The infrastructure domain consists of Road-Side Units (RSUs) and wireless Hot-Spots (HS) that are accessed by the vehicles for safety and comfort based applications. These two types of infrastructure access, road-side units (RSU) and Hot-Spots (HS).In case that neither road-side units (RSUs) nor Hot-Spots (HT) provide internet access, then OBUs can make use of communication abilities with several radio networks or technologies such as GPRS, GSM, WiMax, if they are included on the On-Board Unit (OBU), particular for non-safety applications.

**Application Units (AUs):** An Applications Units (AUs) is an in-vehicle entity, where multiple AUs can be plugged within a single OBU and shares the OBU processing and wireless resources. Examples of Application Units (AUs) are I) safety applications devices like hazard-warning, or ii) a navigation system with communication capabilities. Multiple Application Units can be plugged in with a single On-Board Unit (OBU) simultaneously and share the On-Board Units (OBUs) processing and wireless resources. An Application Unit (AU) communicates solely via the On-Board Unit (OBU), which handles all mobility and networking functions on the International Journal of Advanced Research in Computer Engineering & Technology Application Unit (AU) behalf. The distinction between an Application Unit (AU) and an On-Board Unit (OBU) is just about logical and an Application Unit (AU) which can be physically co-located with an OBU. On-Board **Units (OBUs):** The On-Board Unit (OBU) used for vehicle to vehicle (V2V) communications and vehicle to infrastructure or road side unit (V2I) communications [29]. It also provides communication services to the application units and also forwards data on behalf of other On-Board Units (OBUs) in the ad hoc domain. An On-Board Unit (OBU) is operated with at least a single network device f IEEE 802.11p standard. That is responsible for sending, receiving and forwarding safety and non safety messages in the ad-hoc domain. The main functions and procedures of On-Board Unit (OBU) includes wireless radio access, geographical ad hoc routing, network congestion control, reliable message transfer, data security, IP mobility support, and others.

**Road-Side Units (RSUs):** A Road-Side Unit (RSU) is a physical device situated at fixed positions along roads and highways, or at dedicated locations such as colleges, petrol pumps, parking places, hospitals, shopping complexes, restaurants etc [19, 29]. A Road-Side Unit (RSU) is equipped with at least a network device based on IEEE 802.11p. The main function of RSU is to provide the internet connectivity to the OBUs. An overview of the main functions performed by RSU is given below.

1) Extending the communication range of an ad hoc network by means of re-distribution of information to other OBUs and cooperating with other RSUs in forwarding or in distributing safety information.
2) Running safety applications, such as for vehicle-to-infrastructure warning (e.g. low bridge warning, work-zone warning), and act as information source.
3) Providing internet connectivity to all OBUs for accessing safety and non safety applications.

## 4. Conclusion

VANET is used for communication b/w various vehicles that move on the road. In the VANET, Nodes will communicate with each other without any internal device. The Antenna has been enabled to different nodes for communication with each other. In VANET V2V& V2R they are two types of communication that is completed. All vehicles available in communication network, used to communicate with each other by sharing information. Roadside unit is available to transmit information to all the nodes in the range of RSU. Vehicles communicate with RSU to provide information about their location, Lane & Destination. RSU is responsible to transmit safety messages for avoidance of collision b/w different vehicles. The main problem in VANET is malicious nodes due to availability of various malicious nodes in the network. where Gray hole attack in the VANET is new energy problem because it is difficult to detect. Because here node that is attacked by different attackers where it usually behaves like normal node & sometime behaves like malicious node. So it is not so easy to distinguish.

To overcome this issue various approaches had been used but these approaches does not provide desired results.

## References

[1] Swati Verma "Impact of Gray Hole Attack in VANET"IEEE International Conference on Next Generation Computing Technologies, 2015, pp-127-130.
[2] Faisal Khan "Recovering VANET Safety Messages in Transmission Holes" IEEE International Conference on Information and Communication Technology, 978-1-4799-2969-6/13/$31.00 ©2013.
[3] Ambuj Kumar "An Efficient Group-Based Safety Message Transmission Protocol for VANET" IEEE International Conference on Communication and Signal Processing, 2013, pp- 270- 274.
[4] Ikechukwu K. Azogu "A New Anti-Jamming Strategy for VANET Metrics-Directed Security Defense" IEEE International Conference on vehicular network evolutlon,2013,pp-1344-1349.
[5] Claudia Campolo "Modeling Broadcasting in IEEE 802.11p/WAVE Vehicular Networks" IEEE International Conference on COMMUNICATIONS LETTERS, 2011, pp- 1089-7798.
[6] Bertrand Ducourthial. "Conditional Transmissions: Performance Study of a New Communication Strategy in VANET" IEEE International Conference on

TRANSACTIONS ON VEHICULAR TECHNOLOGY, 2007, pp-3348- 3357.
[7] Y. Bevish Jinila "A PRIVACY PRESERVING AUTHENTICATION FRAMEWORK FOR SAFETY MESSAGES IN VANET" IEEE International Conference on Sustainable Energy and Intelligent Systems, 2013, pp-446-461.
[8] Alwakeel, S "A virtual P-Persistent bandwidth partitioning manager for VANET's broadcast channel", International conf. on Multimedia Computing and Systems (ICMCS), 2014, PP 1212 – 1215,.
[9] Varshney "Security protocol for VANET by using digital certification to provide security with low bandwidth", International Conf. on Communications and Signal Processing (ICCSP), 2014, PP 768 – 772

## Author Profile

**Gurtej kaur** received the B.Tech. degree in Computer Science and Engineering from Sri Sukhmani Institute of Engineering & Technology, Dera Bassi in 2013 and pursuing M.Tech degree in Computer Science and Engineering from Sri Sukhmani Institute of Engineering & Technology, Dera Bassi.