JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Review Paper of Detection and Prevention of Worm hole Attack

Mrs. Annu Lakher , Mr Rajneesh Pachouri, Mr. Anurag Jain, Ms.Charu Jain

M Tech Scholar, Assistant Professor, Assistant Professor, Assistant Professor
Department of Computer Science & Engineering
Adina Institute of Science And Technology, Sagar, India

Abstract: A Wireless Sensor Network (WSN) made up of spatially dispersed independent devices using sensors is vulnerable to many different types of threats and attacks due to a number of factors, including the unattended deployment in an untrusted environment, the limited network resources, the ease of network access, and the range of radio transmission. One such vulnerability is the wormhole attack, in which a hacker sets up a low-latency link between the sensor nodes in order to misdirect those, use network resources, and gain access to private information. This essay outlines the WSN wormhole attack and provides a critical assessment of the defences. In wireless sensor networks (WSN), the efficacy of various wormhole detection techniques and defences against wormhole attacks are compared and analysed.

I. INTRODUCTION

A wireless ad hoc network called a "vehicular ad hoc network" (VANET) is used to connect automobiles and surrounding roadside equipment. Integrating the capabilities of a new generation of wireless networking to cars is a developing technology. One of the main goals of VANET is to give mobile users who are already connected to the outside world through other networks at home or at work ubiquitous connectivity while they are on the road, as well as efficient vehicle-to-vehicle communications that support Intelligent Transportation Systems (ITS). Applications of ITS include cooperative trac monitoring, trac ow control, blind crossing (a crossing without controlled lighting), collision prevention, nearby information services, and computing of real-time diversion routes. More over 17 million people live in the metropolis, yet there aren't enough ways to get them there. Being a citizen of this nation entails having a responsibility to consider and attempt to resolve its problems [6].

In this study, NS2 is used as a simulator to simulate a network layer attack (or "Worm Hole"). In a Worm Hole attack, a malicious node poses as the first hop on the shortest path to carry out a denial of service attack. Instead of transmitting the packet to the next hop when it is sent to the Worm Hole node, the packet is dropped. Because so many reliable nodes in a VANET reject packets for genuine reasons, it is difficult to identify a node as a Worm Hole. A gureless topology is the VANET. Because the node(s) aren't stationary for this reason, a malicious node could move around and pose as a trustworthy node. The MAC address must be used to block Worm Hole nodes[6].

Vehicle ad networks (VANETs) are a small subset of mobile ad networks (MANNETs) using vehicles as their nodes, including cars, trucks, buses, and motorcycles. Accordingly, the nodes' range of motion is constrained by things like the road direction, which mingles traffic with traffic regulations. Because node mobility is constrained, it is believed that VANET will be supported by a fixed infrastructure that supports certain services and might provide access to static networks. Consistent infrastructure will be given to critical locations such as icy roadways, gas stations, dangerous crossroads, or areas that are particularly sensitive to catastrophic weather.

Even though Vehicular Ad-hoc Network (VANET) is not a brand-new subject, it still presents fresh study difficulties. The fundamental goal of VANET is to assist a collection of vehicles in setting up and maintaining a communication network among themselves without the need of a controller or a central base station. One of the main uses for VANET is in life-threatening medical emergencies where there is no infrastructure but it is essential to transmit information to save lives. However, new difficulties and issues arise alongside these beneficial VANET applications. Vehicles in VANET are given new obligations because to a lack of infrastructure. Each new vehicle that joins the network manages and controls both the network's connectivity and its own communication requirements. Networks of Vehicular ad hoc are used in one situation to handle communication between moving autos. Direct communication between two cars is known as "vehicle-to-vehicle" (V2V) communication. [5,6]. Vehicle-to-Infrastructure (V2I) communication is the term for direct communication between a vehicle and an infrastructure, such as a Road Side Unit (RSU) (V2I). A example VANET setup is shown in Figure 1.

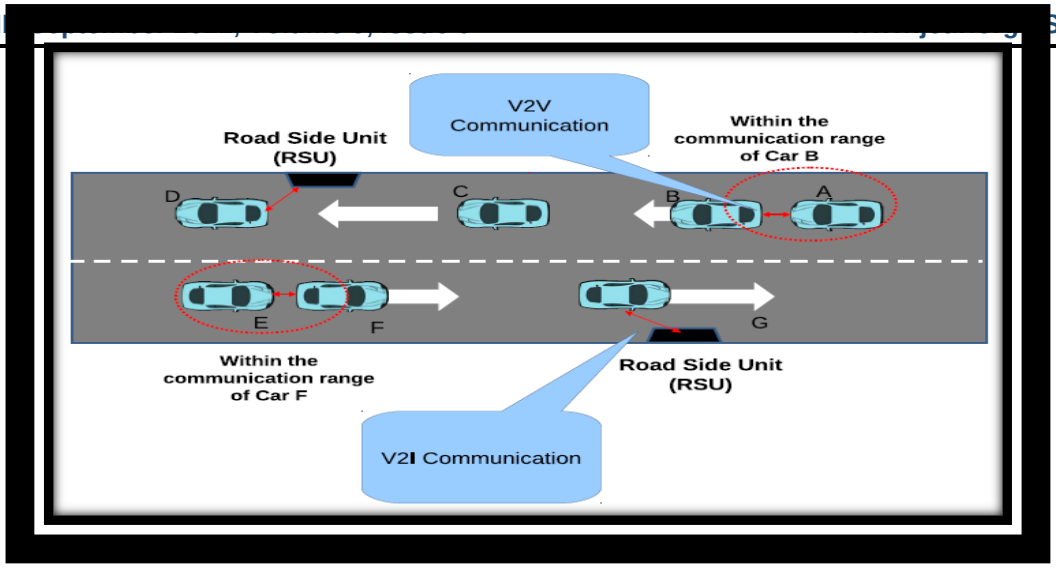

Figure 1Creating an Ad-hoc Network using Vehicles (VANETs)

The key contributions of this work are the state-of-the-art VANET technologies that are presented. This paper presents a thorough analysis of network architecture using various topologies and network modelling. Effective packet routing is a crucial design component in VANET that must be considered in order to construct a functioning communication network. The constraints of the various routing methods for VANET are discussed in the study. In order to construct reliable network architecture, the article also addresses security challenges in the VANET context. The main areas of research and difficulties in this subject are also covered in the report.

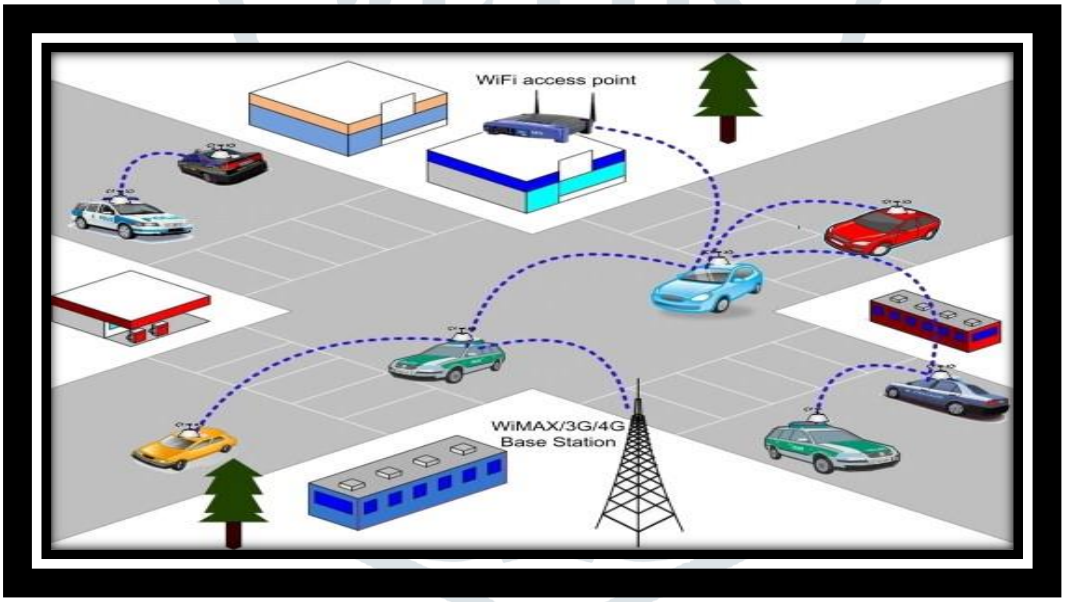

Figure 2 Vehicular Ad-hoc network

A network of moving automobiles that interact in a non-autonomous way is what the Vehicular Ad-hoc Network (VANET) is. Due to traffic congestion, which causes unanticipated changes in network architecture, the effective and efficient dissemination of information is a significant difficulty. People who live in wealthy nations may struggle daily with traffic congestion. Road traffic conditions also have an impact on public safety because it is estimated that 1.2 million people die on the world's highways each year. Because of this, governments and the auto industry are investing more money today in resources that will increase traffic efficiency and street safety while also reducing the environmental impact of transportation. This goal has opened up a wide range of opportunities by using communicative technology and information. The communication between automobiles and roadside equipment, particularly the current vehicular ad hoc network (VANET) traffic, is one of the most promising topics for research.

The creation of an effective, dependable, and secure routing protocol is a key component of VANET's design. This topic has been the subject of extensive research [6, 7, 8]. Any routing protocol's primary goal is to determine the best channel for node communication (vehicles). Ad-hoc On Demand Vector Routing (AODV), which uses a demand-driven route building technique, is one well-known VANET routing protocol. This method's drawback is that it can cause widespread flooding throughout the network. Numerous researchers have offered solutions to flooding in AODV. Dynamic Source Routing, which is also categorised as reactive in nature, presents a different routing strategy. Routes are cached, and it is anticipated that the source will be fully aware of the hop-by-hop path to the destination. Using the concept of border nodes, authors have given another routing strategy in.

1.1 Architecture VANET

Tries to establish contact amongst several nearby automobiles. According to ISO/IEC 42010 and IEEE 1471-2000 rules, the entities in a VANET can be categorised into three categories.

1. Mobile domain: The mobile domain is divided into two sections. The first is the vehicle domain, which includes all continuously moving vehicles including buses, cars, trucks, and so forth. The second section is the mobile device domain, which includes all portable hand-held gadgets including PDAs, laptops, GPS, cellphones, etc.

2. Infrastructure domain: There are also two components to the infrastructure domain. The roadside infrastructure domain consists of fixed roadside elements like poles, traffic lights, etc. In contrast, the central infrastructure domain includes the central managing centres, including the traffic management centre and vehicle management centre.

3. Generic domain: It consists of both private and public infrastructure. Examples of generic domain include various nodes, servers, and other computational resources that are used directly or indirectly by a VANET. The infrastructure domain, which processes data and performs its own modulation, receives information from the mobile domain and connects with it. The second stage is when the infrastructure domain converses with the generic domain and exchanges data with it. The efficient and effective use of the road by the users is a result of the data flow between the stationary and mobile resources.

Another sort of VANET design is communication architecture, in which the four portions are classified as follows:

1) Communication In vehicle communication: It evaluates elements like driver fatigue or drowsiness, among others, by detecting the inner system data or performance of the car. For both driver and public safety, it is critical to ascertain these elements' presence and magnitude [1].

2) Communication of Vehicle to Vehicle (V2V): transferring data between vehicles so that they can communicate warnings and other important information to one another and help the driver. V2V communication supports applications for data dissemination, safety, and security because it does not depend on established infrastructure for data transmission.

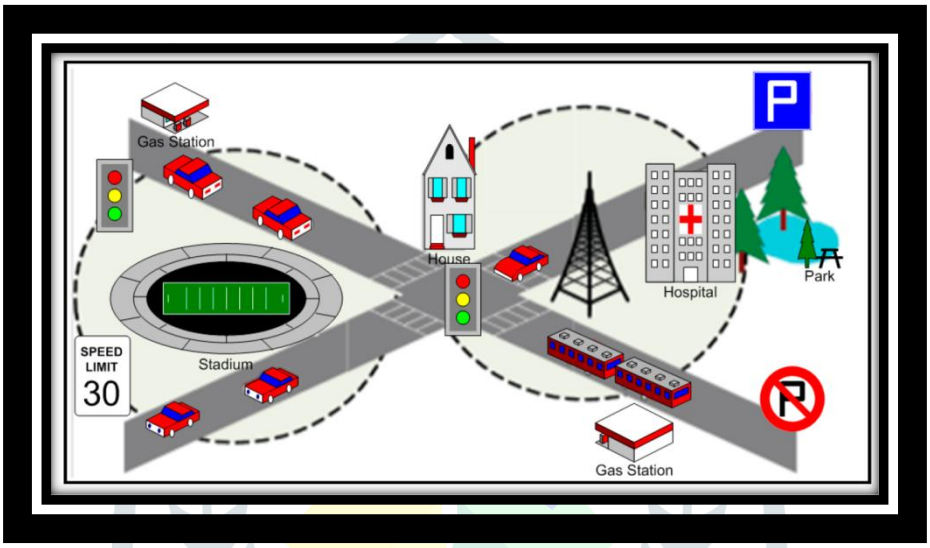

Figure 3 Vehicle-To-Vehicle Communication Architecture

3) Vehicle-to-road infrastructure (V2I) communication: This data collection occurs through communication between mobile vehicles and permanent infrastructure along the road. It offers updates on environmental sensing and monitoring, such as current weather or traffic conditions.

4) Vehicle-to-broadband cloud (V2B) communication: This enables car communication via broadband connections like 3G and 4G. As more traffic data and other data may be included in the broadband cloud, this improves driver assistance and vehicle tracking. Every form of communication mentioned above occurs within one or more VANETs. The manner of communication is irrelevant as long as the VANET's performance is unaffected. Information sharing starts as the cars move and an ad hoc network is established. In one of the modes mentioned above, information is transmitted to other cars and nodes. As long as the car is connected to that specific network, it can utilise the VANET and function. The two main application categories supported by VANET are information distribution and driver assistance. Information exchanged for driver assistance helps the driver maintain a safer and more productive driving environment. The goal of information transmission is to reach as many people as possible, including drivers, nodes, passengers, etc. Applications for information dissemination span the entertaining and life-saving safety spectrum [7] [8].

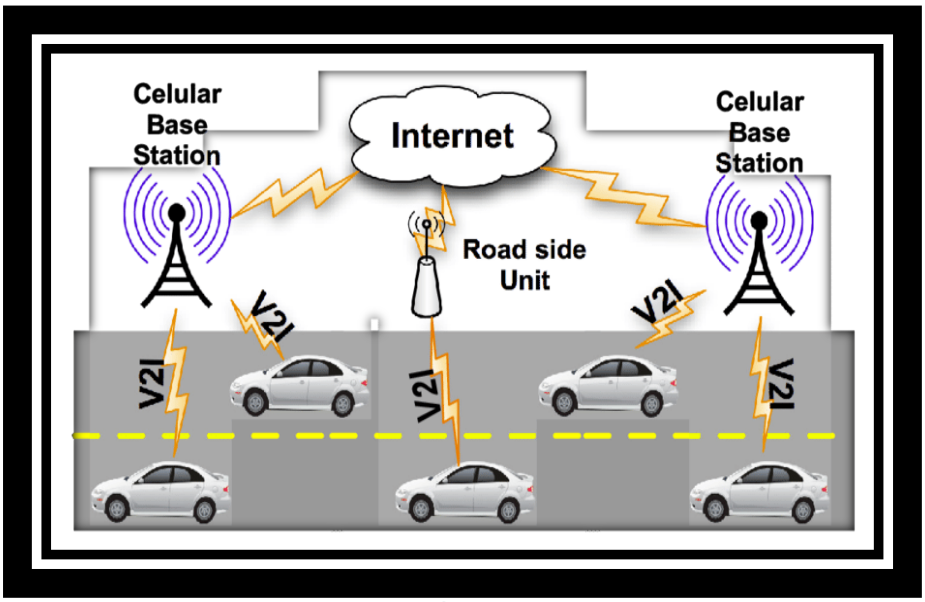

Figure 4 Vehicle-to-Infrastructure (V2I) Communication.

1.2 Applications of VANETS

The RSU can be utilised as a router, access point, or even a buffer point that can store data and provide it as needed. Vehicles upload or download all data from the RSUs. Has additionally classified applications as Car to Car Traffic applications, Car to Infrastructure applications, Car to Home apps, and Routing based applications. According to their classification, the writers of address numerous attacks. We categories VANET applications into the following types based on the type of communication, either V2I or V2V [9]:

1) Safety oriented,
2) Commercial oriented
3) Convenience oriented and
4) Productive Applications

1.3.1 Safety Applications

Monitoring the surrounding road, oncoming traffic, the road's surface, road curves, etc. are only a few examples of safety applications. The applications for road safety can be divided into:

1) Real-time traffic: The RSU can retain the real-time traffic information, making it accessible to the cars whenever and wherever they need it. This may be crucial in resolving issues like traffic bottlenecks, avoiding congestion, and emergency warnings like accidents, etc.

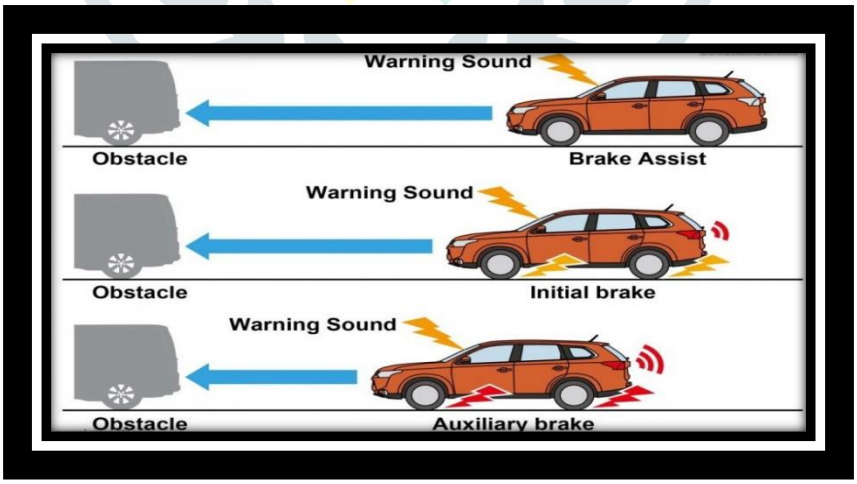

Figure 5 Warning of Cooperative Collision

2) Co-operative Message Transfer: Slow/Stopped Cars will communicate with one another and work together to assist other vehicles. Even while latency and dependability would be huge issues, it might automate safety measures like emergency braking. Similar to the last application, emergency electronic brake lights may be another.

3) Post Crash Notification: As shown in **Figure 5,** a car engaged in an accident would send warning messages about its location to following vehicles so that they may make decisions quickly and to the highway patrol for assistance with towing.

4) Road Hazard Control Notification: automobiles alerting other cars to landslides on the road or information about road features because of a road curve, a rapid drop, etc.

5) Cooperative Collision Warning: Notifies two drivers who may be in an accident path so they can change their driving habits.

6) Traffic Vigilance: The RSU can install cameras that can serve as an input and the newest instrument in a campaign to discourage driving while intoxicated or under the influence of drugs.

II. LITERATURE REVIEW

In this framework there are two major components.

• **Application Monitoring Control System** - The network management system must keep track of each application's availability in order to efficiently support various applications. On VANET, the programme can typically be distributed to several locations (RSUs and/or OBUs) or accessible locally (RSU or OBU). Servers must register the kind and availability of these apps in the control framework in order to provide these applications. Additionally, frequent updates or updates based on previously specified occurrences will be made to the discovery information. The control panel will be in charge of sending this message to the VANET nodes after receiving it.

• **Integrated Route Program with Security Requirements-** The integrated route plan will be created with the availability of application information in order to support every application outlined in the previous section. Accordingly, particular flow packets will be forwarded.

2.2. Casing

Illustrate the behavior of the framework, we use the following situations as examples.

• **Case 1** - All OBUs and RSUs are registered with the control framework for security-related applications (Key Health Security Requests, Safety Warning Requests). All neighbouring VANET nodes will receive request-related security messages for streaming. Request-related request messages do not need to be encrypted in order to comply with the requirement for message confidentiality, but they do need to meet the standards for message integrity and authenticity in order to avoid message rejection and for business verification. To avoid causing a disruption in traffic, safety precautions should be taken.

• **Case 2** For OBUs enrolled in the control framework for Electronic Toll Collections. Every ETC-related app communication acts as a one-hop wireless connection between the car and the Toll Collection Point. App messages associated to ETC must adhere to message confidentiality, message authenticity and integrity, and message non-denial and business verification requirements.

• **Case 3** - Assume that each RSU is registered with the control framework as an online access gateway. Now, suppose a common request for a significant online access effort from the OBU enters the regulatory framework. For such an application, a single unicast route plan between the OBU and the adjacent RSU can be put up. Keep in mind that in this situation, the single-route scheme cannot provide multihop mode protection for vulnerable OBUs. To avoid causing a disruption in traffic, safety precautions should be taken.

• **Case 4** - More broadcasts are used to monitor the application from among the OBUs registered for Group Communication in the regulatory framework. In that circumstance, security precautions had to be taken to guarantee the security of several streams on VANET. Secure multi-stream techniques on VANET still need to be taken into consideration, even if the security of multiple streams on MANET has been momentarily studied.

• **Case 5** - One route may be established between an OBU requesting services and the closest RSU for OBUs that have registered a Roadside Services Finder application in the regulatory framework. The same safety precautions as in Case 3 must be implemented.

Researchers are always focusing on the security of VANET communications, looking for solutions to this extremely complicated issue, and there have been several proposed methodologies.

[13] Khaoula Jeffane, and Khalil Ibrahimi, "Detection and Identification of Attacks in Vehicular Ad-Hoc Network", IEEE, 2016.

Khaoula Jeffane, and Khalil Ibrahimi et.al [13] To enhance traffic conditions, a system was proposed that would integrate traffic information with a distribution system suitable for the city region and based on the Vehicle Ad hoc Network (VANET). Using vehicle-to-vehicle communications and vehicle interactions, sidewalk units (RSUs) can gather, produce, and distribute traffic messages. Drivers can plan ahead for traffic incidents and choose the optimal route with the aid of traffic messages. Avoiding gridlock and lowering the likelihood of accidents on the road are both beneficial. However, because it is a critical matter to identify the attacker, who is the primary source of overcrowding, the author of this study does not demonstrate how the attack affects the fact that overcrowding happens.

[14] Mengjiong Qian, Yong Li, Depeng Jin, Lieguang Zeng, "Characterizing the Connectivity of Large Scale Vehicular Ad-Hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, 2013.

. Mengjiong Qian, Yong Li, Depeng Jin, Lieguang Zeng,et.al [14] Due to worries about traffic safety, the Vehicular Ad-hoc Network (VANET) focuses on the automotive sector. Network access should always be available since it is crucial when a node provides any crucial health information to other nodes. Security is another security aspect in VANET. The growth of wireless apps being created and disseminated in a well-known wireless environment, however, makes it likely that security threats will expand in the future. As a result, network access is vulnerable to several kinds of attacks. An introduction to a Distributed Denial of Service (DDOS) attack on network access is made in this study. The complexity of this attack's brutality in the VANET domain is discussed. The VANET paradigm has been used to prevent DDOS assaults developed and other possible solutions for overcoming attacks have been discussed.

[15] Sourav Kumar Bhoi, Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout, "RRP: A Robust Routing Protocol for Vehicular Ad Hoc Network against Hole Generation Attack ", International conference on Communication and Signal Processing, pp. 1175-1179 April 3-5, 2013.

Sourav Kumar Bhoi, Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout et.al [15] proposes five distinct attack stages, with each class being intended to offer a deeper understanding of VANETsecurity. The division and identification of various attacks on VANET are addressed in this paper's main contribution.

[16] M. Sivasakthi and S. Suresh, "Research on vehicular ad hoc networks (VANETs): an overview," Journal of Applied Sciences and Engineering Research, vol. 2, no. 1, pp. 23–27, 2013.

M. Sivasakthi and S. Suresh, et.al [16] accelerates data flow between vehicles and between roadside vehicles and traffic availability by integrating mobile communication devices. On VANET, messages can be sent from one automobile to another and

the wireless device can broadcast information to neighbouring vehicles. Therefore, employing VANET can improve traffic efficiency and security. There are serious issues with VANET, just like with other technologies. Security is among the things that are most significant to them. One of the most crucial topics in the vehicle industry is safety, so I try to address it in this essay.

[17] F. Li and Y. Wang, "Routing in vehicular ad hoc networks MANETs: a survey," IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12–22, 2007.

F. Li and Y. Wang, al [17] is developing a crosslayer control system with an increased focus on vehicle tracking precision rather than MAC efficiency. The authors take into account a lost shared channel where an increase in message frequency can clog the channel and inadvertently reduce the accuracy of other vehicles' placements. With the help of the suggested algorithm, full accuracy can be attained by modifying the transmission periodicity.

[18] K. Hong, J. B. Kennedy, V. Rai and K. P. Laberteaux. Evaluation of Multi-Channel Schemes for Vehicular Safety Communications. In Proc. of IEEE VTC-Spring, Taipei, pp. 1-5, 2010.

K. Hong, J. B. Kennedy, V. Rai [18] The rate of packet injection is adjusted to achieve the desired channel load in the suggested approach for managing congestion. The issue of acquisition performance and choosing a full channel capacity is not, however, explicitly taken into account.

[19] H. Moustafa and Y. Zhang, Vehicular Networks: Techniques, Standards, and Applications, CRC Press, Boca Raton, Fla, USA, 2009.

One of the most frequent security attacks on MANETs and VANETs is the Worm hole attack. When nodes decline to join a network or when a fixed node collapses, a Worm hole is produced. This kind of attack causes no data loss because all network traffic is diverted to a single point H. Moustafa et.al.[19]. There are two potential remedies for this issue in MANETs. The protocol finds several ways to get you there. It is obvious that the network could get very cluttered as a result of this method. Additionally, while this strategy might work for MANETs, adding another mobile node to a VANET with several mobile nodes would introduce needless restrictions like delays or service fees. The second solution is to use a package sequence number attached to any packet head.

[20] A. Amoroso, G. Marfia and M. Roccetti. Going Realistic and Optimal: A Distributed Multi-Hop Broadcast Algorithm for Vehicular Safety. Computer Networks, 55(10), pp. 2504-2519, 2011.

A. Amoroso, G. Marfia and M. Roccetti [20] Other methods have recommended distributing information to VANET as settings using the publishing / subscription model. These techniques have been crucial in determining how effective VANET's publishing and registration are. In these systems, a mixed set is used to discuss a collaborative approach, including moving vehicles and stationary information stations. The ultimate objective is to create automobile networks' P/S middleware that accounts for the location and time of its design objectives. By using location as context, this middleware enables app developers to quickly broadcast a notification locally. It makes use of the possibility to produce subscriptions using data that may be derived from automobile navigation systems (location, map, driver location, etc.). The navigation system determines whether the vehicle wants to receive a specific notification or not. The proposed system is a program that takes advantage of Publish / Subscribe opportunities.

[21] J. Misic, G. Badawy and V. Misic. Performance Characterization for IEEE 802.11p Network with Single Channel Devices. IEEE Transactions on Vehicular Technology, 68(4), pp. 1775-1789, 2011.

J. Misic, G. Badawy and V. Misic [21] In this study In order to analyse the placement and timing of radio transmissions, we present a novel model of congestion for urban transportation networks. We view the marked intersections and connected road segments as the fundamental elements of urban traffic systems in order to portray traffic congestion. The congestion model gives us a framework for characterising crucial radio frequency and local circuits in accordance with VANET scenarios intended for urban transportation systems, which is not possible with the same congestion models that are frequently employed in existing literature. In order to send a message of security to VANETs, it studies the channel volume associated with sporadic lighting using a remote radio model. This study also offers a common framework for analysis that can be used to look at further elements of data performance and security message transmission on VANETs. In order to reduce channel loading caused by crowded traffic circumstances, test findings utilising the suggested real-time congestion model point to the need for an adaptive strategy to modifying the transmission capacity and data level.

[22] Y. Zhang, Q. Wang, S. Leng, and H. Fu. A QoS Supported Multi-channel MAC for Vehicular Ad Hoc Networks. In Proc. of IEEE VTC-Spring, Budapest, pp. 1-5, 2011.

(Y. Zhang, Q. Wang et al.) Existing [22] technique for reducing security application traffic jams. The system's fundamental goal is to scam IEEE 802.11p MAC transmission channels in order to ensure that security signals are sent to the control station while also detecting congestion using event-based detection and monitoring. Standard-based traffic detection includes measuring channel usage and comparing it with a set limit, whereas event-driven traffic detection is launched continually once a vital security message is recognised to guarantee the QoS of security applications. However, because local context and efficient bandwidth sharing are not taken into account, the effective transmission of security signals is not assured.

[23] D. Jiang and L. Delgrossi. IEEE 1609.4 DSRC Multi-Channel Operations and Its Implications on Vehicle Safety Communications. In Proc. of IEEE VNC, Tokyio, pp. 1-8, 2009.

D. Jiang et al.[23] The hop-by-hop mode of the available bandwidth is adjusted in the suggested density control approach , which is intended to operate within car network networks. Therefore, a sizable percentage of the available bandwidth will be made available to nodes transmitting information via the VANET utility. Depending on its usage and size, the package's significance varies with its size. Then, using the result of the calculation, the data speed is established. The application layer monitors the message usage, which disregards the context in terms of the density and adaptability of the nodes. Additionally, by allowing surrounding nodes to contextually exchange information in order to split the available bandwidth among them, this method establishes more connections without considering the volume of traffic volume and density of the transmission nodes.

[24] Marc Torrent-Moreno, Daniel Jiang, Jannes Hartenstein "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks" VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networksOctober 2004 Pages 10–18https://doi.org/10.1145/1023875.1023878

Marc Torrent-Moreno et al. existing [24] as a method of sharing the suitable bandwidth of VANETs. This strategy calls for tight management between vehicles and occasionally restricts wireless message loading. The authors suggest a centralised power control method that offers the right transmission range for every node using a constant package production rate. This suggestion received

formal approval. Nevertheless, simulation has been carried out under plausible circumsstances, presuming that the distortion between node transfers adheres to the governing model. Additionally, the suggested algorithm necessitates vehicle synchronisation, increasing communication.

[25] S. Wang and C.-C. Lin. NCTUns 5.0: a network simulator for IEEE 802.11(p) and 1609 wireless vehicular network researches. In Proc. of IEEE VTC-Fall, Calgary, 11(2), pp. 3-20, 2008.

III. WORM HOLE ATTACK

Without any established infrastructure, Mobile Ad hoc Networks (MANETs) function. Each node in the network acts as a router to transfer data to the destination. MANETs are more susceptible to routing attacks than other networks because they lack a centralised point of control. Wormhole attack, one of the most dangerous routing assaults, is simple to use yet difficult to spot. The process typically takes place in two stages: first, the wormhole nodes draw increasing amounts of traffic to themselves via the wormhole channel, and then, second, they start disrupting the network by changing or discarding the traffic. Different defences against wormhole assaults have been put forth by various writers for MANETs. In this research, we do a thorough analysis of various existing approaches based on their shortcomings and key features for wormhole attack detection in MANETs.

Mobile Ad hoc Networks (MANETs) have developed in a number of ways during the past few years as a result of the exceptional advancement in wireless communication technology. Lack of infrastructure, a shared broadcast channel, a risky wireless environment, the absence of a centralised point of control, changeable topology, and resource constraints are among the main characteristics of MANETs. MANETs can be used for a variety of purposes, such as gathering helpful information in disaster zones, facilitating soldier communication on the battlefield, and gathering and transmitting vital information in the ocean, among others. Each node in a MANET serves as both a host and a router, communicating directly with other nodes nearby that are within its transmission range. A node creates an indirect link with non-neighbors in a hop-by-hop fashion with the aid of other nodes in its neighbourhood. In order to locate, maintain, and repair routes in the network, routing protocols are crucial. Over the past few years, a variety of routing protocols for MANETs have been suggested by researchers.

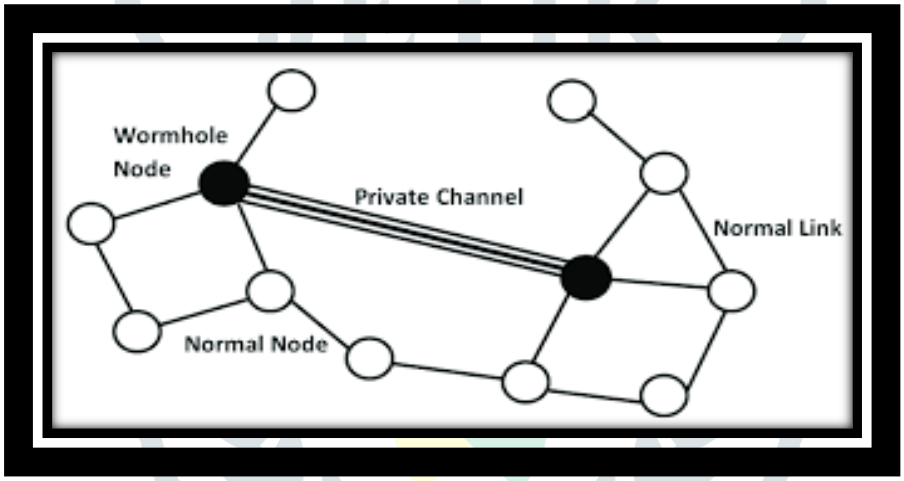

Figure 6 Wormhole Attack Working in MANETs.

Wormhole attacks are among the most serious security risks to MANETs and are widely acknowledged. It can impair a number of MANET routing protocols, including Topology Dissemination Based on Reverse-Path Forwarding (TBRPF), Ad hoc On-Demand Distance Vector (AODV), Optimized Link State Routing (OLSR), Destination Sequenced Distance Vector (DSDV), and Dynamic Source Routing (DSR). Typically, a wormhole attack is carried out by two or more malicious nodes utilising a tunnel, a private channel that connects them. Figure illustrates how a wormhole attack operates. A malicious node at one end of the tunnel intercepts a control packet and delivers it across a private channel to a cooperating node at the other end, which rebroadcasts the packet locallyThe private channel is chosen as the route for communication between the source and the destination because it has better metrics, such as fewer hops or less time, when compared to packets transmitted over other conventional channels. Typically, the attack involves two stages. The wormhole nodes engage in a number of routes in the initial stage. These malicious nodes begin utilising the packets they receive in the second phase. These nodes have a variety of ways that they can impair the operation of the network. These nodes may mislead protocols that rely on node position or geographic proximity, for instance, or they may work together to overload other intermediary nodes' batteries by repeatedly sending data packets back and forth over a virtual tunnel. Data can be dropped, altered, or sent to a third party through wormhole nodes in order to harm another person.

3.1 Features of Detection

In this part, we go through many MANET characteristics that can be useful in wormhole attack detection. One or more of these characteristics are also utilised by the approaches outlined in section 2 for wormhole discovery. Here, we go into great detail on each feature.

Location

Location is a crucial component in a wormhole assault. It would be relatively simple to construct a network graph if we knew the precise location of mobile nodes. Including a Global Positioning System (GPS) device in every network node is one approach to put this system into practise. To cut costs, specialised nodes with GPS receivers can be placed at certain points in the network to determine the locations of nearby nodes. Additionally, the direction from which the data is received can be determined by utilising

specialised antennas, which are able to gather the relative location data. Using a GPS device or a specialised antenna will raise the cost of nodes and increase the cost of the network. Additionally, the battery timing of mobile nodes will be reduced. Since nodes in MANETs constantly change positions, utilising exact or relative location as a detection feature might also raise the False Positive Rate (FPR).

Time

Detecting wormhole attacks can also be aided by the time feature. In comparison to the regular route, the wormhole assault route will have a longer average time per hop. All nodes in the network should have closely synchronised clocks in order to calculate the precise time difference between the source and destination. Without a closely synced clock, the time difference can alternatively be computed by the source node sending a specific, light-weight Hello message to the destination and noting the packet's transmission time. The destination node responds with a Hello-Reply message after receiving the Hello message. After subtracting the processing time at the source, destination, and intermediate nodes, the difference between sending and receiving time is determined and divided by two. Then the typical duration of each hop is calculated. In MANETs, synchronising a clock is a challenging and expensive process. Techniques that use time difference as a detecting characteristic may run into the issue of rising FPR because of network congestion. Additionally, it is challenging to locate and recognise rogue nodes using straightforward time difference techniques.

Hop Count

The shorter paths (i.e., fewer hops) taken by wormhole nodes tend to draw network traffic, hence the hop count characteristic can also be employed as a detection metric. Because the hop count does not grow while the message travels across the secret channel between malicious nodes, a path through wormhole nodes has less hops than a normal path. Some methods use hop count data in conjunction with time or location to detect the presence of wormholes. By dividing the total number of hops by the total amount of time or distance, the average hop time is computed. The path contains malicious nodes if the average hop time or distance is longer than the standard preset hop time. Techniques based on distance or average time may need a GPS device or synchronised clock, respectively. The valid path with the shortest route to the goal may go unnoticed by the intrusion detection system (IDS), which focuses on avoiding the shortest route.

Neighborhood

Wormhole attacks' fundamental characteristic is their representation of two non-neighboring nodes as neighbours. So, gathering information about nearby nodes can also be used to identify the wormhole. These methods gather and retain track of information about a node's close (one hop) neighbours, whereas other methods attempt to detect wormhole attacks by keeping and examining information about two-hop neighbours gathered via the Hello message. In dense networks with many neighbours at each node, these strategies have difficulties. Therefore, greater memory, storage, and computing power are needed to maintain and evaluate data up to two-hop neighbours. Additionally, the overall network traffic will increase as a result of the Hello messages. These methods won't function well in networks with high rates of mobility since FPR will rise and neighbour lists will also change often.

Data Packets

Some intrusion detection methods use the ratio of data packets transmitted and received to identify wormhole nodes. All nodes are configured in promiscuous mode for these strategies, allowing them to listen for data packets in their immediate vicinity. In order to determine whether their neighbours drop, modify, or forward data packets to nodes other than the target node, the nodes keep track of the number of packets received and forwarded by their adjacent nodes in a table. They determine the trust value of each surrounding node using this data. Although this is a straightforward method, it can be used successfully in sizable networks with considerable mobility. Setting nodes in promiscuous mode, however, is ineffective since each node would then have to process each data packet broadcast in its neighbourhood in addition to handling control messages.

Route Reply

In order to identify wormhole assaults, Route Reply (RREP) is also employed as a detection tool. When a node receives a request for a new route, if the source node is the destination node or has a new route to the destination node, it sends an RREP message to the source node. This rule is typically broken by the wormhole nodes to start the attack. Because RREPs can only be unicasted once, nodes that want to keep track of RREPs must be configured in the promiscuous mode, which might reduce the effectiveness of the network.

Route Request

The most crucial component for on-demand routing in MANETs is Route Request (RREQ). Similar to RREP, it is used in conjunction with a few other properties to identify wormhole assaults. IDSs based on RREQ often have simple computations and consume fewer resources in comparison to other approaches because each RREQ emitted by a source node typically reaches every node in the network.

IV. CONCLUSION

In this paper modified the AODV routing protocol for the detection of wormhole attack. The modified protocol is called improved efficient routing protocol (IMAODV). The IMAODV protocol basically based on two functions one is RTT function and other is clustering process. The function of RTT estimates the hop of routing load during the process of communication. The estimated value of RTT proceeds for the generation of cluster. The cluster estimated the value of normal node and abnormal node. The modified and improved AODV protocol is better than AODV protocol. The RTT and clustering technique is good technique for wormhole detection technique. in future this algorithm is used for real time scenario of wormhole detection.

A promising technique for an intelligent transportation system, vehicular ad hoc networking delivers a state-of-the-art overview of networking difficulties (ITS). Despite the fact that many issues are yet unresolved, the general Autonomous wireless technology is thought to be advantageous for automobiles. VANETs (Vehicular Ad Hoc Networks) will be used for vehicular a fact) (Ad-Hoc Networks). This is how we categorised the difficulties into various facets and briefly examined each one.

REFERENCES

1. Liang, W., Li, Z., Zhang, H., Wang, S., & Bie, R. (2015). Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. International Journal of Distributed Sensor Networks, 2015, 17.
2. Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J-L. bin Ab Manan. "Classes of Attacks in VANET." IEEE Saudi International Electronics, Communications and Photonics Conference (SIECPC), 2011, pp. 1-5, 2011.

3. Sarah Madi, Hend Al-Qamzi, "A Survey on Realistic Mobility Models for Vehicular Ad Hoc Networks (VANETs)", IEEE 10th IEEE International Conference On Networking, Sensing And Control (ICNSC), 2013.
4. Vishal Kumar, Shailendra Mishra, Narottam Chand "Applications of VANETs: Present & Future", Communications and Network, 2013, 5, 12-15 doi:10.4236/cn.2013.51B004 Published Online February 2013.
5. Mengjiong Qian, Yong Li, Depeng Jin, Lieguang Zeng", Characterizing the Connectivity of Large Scale Vehicular Ad-Hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC): Networks, 2013.
6. Sabih ur Rehman*, M. Arif Khan, Tanveer A. Zia, Lihong Zheng "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications 2013, 3(3): 29-38
7. Willke, T. L., Tientrakool, P., & Maxemchuk, N. F. (2009). A survey of inter-vehicle communication protocols and their applications. Communications Surveys & Tutorials, IEEE, 11(2), 3-20.
8. Vishal Kumar, Shailendra Mishra, Narottam Chand "Applications of VANETs: Present & Future", Communications and Network, 2013, 5, 12-15 doi:10.4236/cn.2013.51B004 Published Online February 2013.
9. Jair Jose Ferronato, Marco Antonio, Sandini Trentin, "Analysis of Routing Protocols OLSR, AODV and ZRP in Real Urban Vehicular Scenario with Density Variation", IEEE Latin America Transactions Volume: 15 , Issue: 9, pp.1727 - 1734, 2017.
10. A.P. Jadhao, Dr.D.N.Chaudhari, "Security Aware Routing Scheme In Vehicular Adhoc Network", IEEE Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), 2018.
11. Kumud Dixit Priya Pathak Sandeep Gupta, "A New Technique for Trust Computation and Routing in VANET", IEEE, 2016.
12. Trupil Limbasiya, Debasis Das, "Secure Message Transmission Algorithm for Vehicle to Vehicle (V2V) Communication", IEEE, 2016.
13. Khaoula Jeffane, and Khalil Ibrahimi, "Detection and Identification of Attacks in Vehicular Ad-Hoc Network", IEEE, 2016.
14. Mengjiong Qian, Yong Li, Depeng Jin, Lieguang Zeng, "Characterizing the Connectivity of Large Scale Vehicular Ad-Hoc Networks", IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, 2013.
15. Sourav Kumar Bhoi, Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout, "RRP: A Robust Routing Protocol for Vehicular Ad Hoc Network against Hole Generation Attack ", International conference on Communication and Signal Processing, pp. 1175-1179 April 3-5, 2013
16. M. Sivasakthi and S. Suresh, "Research on vehicular ad hoc networks (VANETs): an overview," Journal of Applied Sciences and Engineering Research, vol. 2, no. 1, pp. 23–27, 2013.
17. F. Li and Y. Wang, "Routing in vehicular ad hoc networks MANETs: a survey," IEEE Vehicular Technology Magazine, vol. 2, no. 2, pp. 12–22, 2007.
18. K. Hong, J. B. Kennedy, V. Rai and K. P. Laberteaux. Evaluation of Multi-Channel Schemes for Vehicular Safety Communications. In Proc. of IEEE VTC-Spring, Taipei, pp. 1-5, 2010
19. H. Moustafa and Y. Zhang, Vehicular Networks: Techniques, Standards, and Applications, CRC Press, Boca Raton, Fla, USA, 2009.
20. A. Amoroso, G. Marfia and M. Roccetti. Going Realistic and Optimal: A Distributed Multi-Hop Broadcast Algorithm for Vehicular Safety. Computer Networks, 55(10), pp. 2504-2519, 2011.
21. J. Misic, G. Badawy and V. Misic. Performance Characterization for IEEE 802.11p Network with Single Channel Devices. IEEE Transactions on Vehicular Technology, 68(4), pp. 1775-1789, 2011.
22. Y. Zhang, Q. Wang, S. Leng, and H. Fu. A QoS Supported Multi-channel MAC for Vehicular Ad Hoc Networks. In Proc. of IEEE VTC-Spring, Budapest, pp. 1-5, 2011.
23. D. Jiang and L. Delgrossi. IEEE 1609.4 DSRC Multi-Channel Operations and Its Implications on Vehicle Safety Communications. In Proc. of IEEE VNC, Tokyio, pp. 1-8, 2009.
24. Marc Torrent-Moreno, Daniel Jiang, Jannes Hartenstein "Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks" VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networksOctober 2004 Pages 10–18https://doi.org/10.1145/1023875.1023878
25. S. Wang and C.-C. Lin. NCTUns 5.0: a network simulator for IEEE 802.11(p) and 1609 wireless vehicular network researches. In Proc. of IEEE VTC-Fall, Calgary, 11(2), pp. 3-20, 2008.
26. T. L. Willke, P. Tientrakool and N. F. Maxemchuk. A Survey of Inter-Vehicle Communication Protocols and Their Applications. IEEE Communications on Surveys and Tutorials, 11(2), pp. 3-20, 2009
27. Lingyun Zhu; Chen Chen; Xin Wang; Azman Osman Lim "SMSS: Symmetric-Masquerade Security Scheme for VANETs" Published in: 2011 Tenth International Symposium on Autonomous Decentralized Systems, 3-27 March 2011 Accession Number: 11929122, IEEE Xplore: 05 April 2011, DOI: 0.1109/ISADS.2011.88, ISBN:978-1-61284-213-4.