Volume 9, Issue 6, June – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN210

A Careful Examination of the Security and Traffic Effects Associated with the Vehicle Ad-hoc Network (VANET)

Joseph Wheeder
PG Scholar, Department of CSE, School of CSE, Sandip University, Nashik, Maharashtra, India.

Sivaram Ponnusamy
Professor, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India.

Mohammad Muqeem
Professor, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India.

Pawan R Bhaladhare
Professor, School of Computer Science and Engineering, Sandip University, Nashik, Maharashtra, India.

Abstract:- During recent years, vehicular ad hoc networks, or VANETs, have emerged as one of the most exciting and difficult study fields. VANET is regarded as a subset of MANET, or mobile ad hoc network, which is primarily used on automobiles. With the use of traffic data, VANET hopes to supply an advanced Intelligent Transportation System (ITS) with a wealth of information. Mention how daily traffic data collection helps with transportation planning, particularly with regard to intra-city communication. Two of the main issues with the existing traffic system are jams in traffic and accidents. Around the world, numerous people lose their lives or suffer severe injuries in traffic accidents each year. Human lives on the road are directly impacted by these issues. VANET can help to avert these mishaps and facilitate the efficient operation of daily traffic. Furthermore, VANET offers a plethora of intriguing applications, including real-time traffic condition monitoring, dynamic route scheduling, blind crossing prevention, safety, and more. In addition, there are certain drawbacks in terms of traffic and security. The absence of a centralised infrastructure in VANET is one of the main security issues. One of the most difficult jobs in the resultant decentralised and self-organizing VANETs is the administration of the wireless channel to make an efficient use of its capacity because there is no centralised infrastructure in charge of synchronisation and coordination of transmissions. VANET is primarily used to lower the risk of accidents in urban areas with a high volume and complexity of vehicles. We introduce the VANET Security R&D Ecosystem and examine traffic in this article. The four main components of the R&D ecosystem are end customers, government agencies, automakers, and university research. Every facet of VANET is covered in detail. Our study primarily focuses on the security and traffic within VANETs, including how data is safeguarded from vehicle-to-vehicle (V2V), vehicle-to-roadside infrastructure communications devices (V2I), access points, and other sources.

I. INTRODUCTION

Vehicular Ad-hoc Networks, a prominent area of research in recent years, date back to 2001. First mentioned in the category of vehicular communication systems, VANET stands for vehicle-to-vehicle ad hoc mobile networking and communication. Since the 1970s, there have been systems for sharing and distributing information among automobiles, computer networks, and roadside equipment as a means of preventing accidents and traffic jams. These systems are known as vehicular communication systems. Furthermore, these nodes are devices for dedicated short-range communications (DSRC). With a frequency of 75 MHZ and a range of roughly 300 metres (980 feet), DSRC is intended for one-way or two-way short- to medium-range wireless communication channels, particularly for the automotive industry. It operates in the 5.9 GHZ band. Because there are more cars on the road, there are more accidents and traffic jam every day, which negatively impacts our quality of life. As a component of the intelligent transportation system (ITS), VANET has grown in importance and popularity throughout numerous nations. The Global Positioning System (GPS) is used in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications over the VANET in order to share and exchange messages.

Providing safe and secure vehicular communication is one of the biggest security-related implementation problems of VANET. Since a VANET connection is wireless, there are numerous threats and attacks that could undermine the network and communication inside it. Data threats and VANET system threats are the two categories of potential assaults that VANET is most vulnerable to. One of the most common types of assaults that can prevent radio channels from broadcasting

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN210

and prevent On-board units (OBU) or Road Side Units (RSU) from connecting to the network is denial of service. There are numerous routing protocols for data transmission. The Dynamic Source Routing protocol (DSR) is a straightforward and effective routing protocol created especially for use in multi-hop wireless ad hoc networks of mobile nodes because VANETs lack centralised infrastructure. DSR removes the requirement for any current network administration or infrastructure and enables the network to be fully self-organizing and self-configuring.

II. OVERVIEW OF VANETS

Vehicle Ad-hoc Networks, or VANETs for short, are a subset of Mobile Ad-hoc Networks, or MANETs. With the use of traffic data, VANET hopes to supply an advanced Intelligent Transportation System (ITS) with a wealth of information. Mention how daily traffic data collection helps with transportation planning, particularly with regard to intra-city communication [14]. Road accidents and traffic jams are two of the main issues with the present traffic system. Around the world, numerous people lose their lives or suffer severe injuries in traffic accidents each year. Human lives on the road are directly impacted by these issues. VANET can help to avert these mishaps and facilitate the efficient operation of daily traffic. Furthermore, VANET offers several intriguing applications in the areas of safety, collision avoidance, blind crossing, dynamic route scheduling, real-time traffic state monitoring, etc [8].

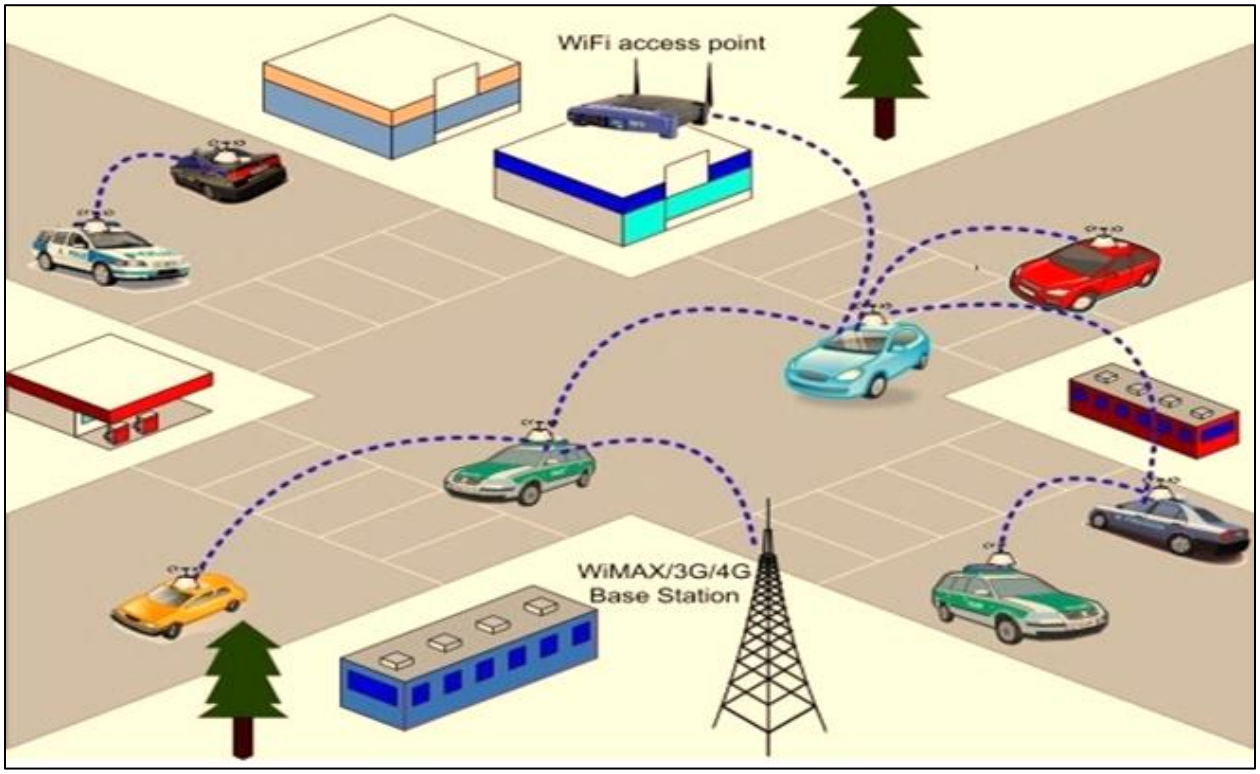

Fig 1. How Nodes within VANET Communicate with each other , RSUs and others [15].

A. Some Characteristics of VANET

A VANET is a type of network where the nodes are mobile vehicles or Road Side Units (RSUs) and there is no static network infrastructure. Because VANET has a static network architecture, node position determines the topology, which can alter at any time. VANET's characteristics are as follows:

- *High Mobility*

Because VANET nodes move quickly, it is challenging to pinpoint each node's precise location within the network and hence offer security [3].

- *Rapidly Shifting Network Topology*

The topology of a VANET is determined by its nodes, which are constantly moving at a fast pace. The VANET's dynamic topology and unexpected nature result from this [3,11].

- *Frequent Information Exchange*

Because VANETs are ad hoc in design, nodes can repeatedly gather information from other roadside units and surrounding automobiles.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN210

➢ *Restricted Bandwidth*

The conventional DSRC band in VANET should be measured as limited; its width was 27 MHZ. The throughput, which is a theoretical figure, was 27 Mbps [3,12].

➢ *Attenuations*

Doppler Effect, losses, reflection, diffraction, and dispersion, as well as various fading modes, are among the transmission issues that digital transmission claims DSRCband faces with those frequencies. Multipath reflections are the cause of the propagation delays.

➢ *Time-Sensitive*

The VANET information must reach the correct node within the allotted time frame in order for it to make a judgement and take the appropriate action [8].

➢ *Processing and Energy Storage*

There is no problem with energy, processing power, or storage failure on the VANET nodes. This permits the use of complex techniques like RSA and ECDSA implementation on VANETs and offers limitless transmission power.

➢ *Improved Physical Protection*

The vehicle in the VANET needs to be well-protected physically. Thus, it will be challenging to physically compromise the VANET node, and it will be challenging to lessen the impact of an infrastructure attack. restricted gearbox power The transmission power of the WAVE should be sufficient to reach the data. One may say that the data reachability distance is 1000 metres. It is permissible to broadcast at a high strength during times of crisis and for public safety issues like accidents or traffic congestion [1,2].

B. Safety Related Application

The following application, which falls under this category, can improve road safety:

➢ *Collision Avoidance*

Reduces the number of accidents by sending out an alert 0.5 seconds before a collision. A collision can be prevented if the driver is informed of the location of a vehicle or a nearby node.

➢ *Cooperative Driving*

When there are any traffic-related alerts, such as a lane-change warning or a curve-speed warning, drivers will receive signals. The signal can work together to enable the driver to drive safely and without interruption.

➢ *Traffic Optimisation*

Vehicles can be alerted to events such as accidents, traffic jams, etc. to help improve traffic flow. in order for them to choose a different route and determine when to seek help.

III. SECURITY ATTACKS IN VANETS

- Services for VANET Security. To guarantee the security of the connection and the data, the security services in VANET offer the following.
- Availability: Because of its connection to all safe-ty applications, availability is one of the most important aspects of security services. It guarantees that information should always be accessible to the authorised user [10].
- Confidentiality: It ensures that information is only disclosed to authorised users or network nodes.
- Authentication: VANET relies heavily on it. It aids in defending the Vehicle ad hoc network against alleged network entities. It gives each network node a unique identity and sender address [9].
- Data Integrity: It guarantees that the message's content is appropriate for the context of its transmission. By utilising cryptograph encryption and public key infrastructure, the VANET is able to accomplish this.
- Non-Repudiation: this service makes sure that, in the event that the sender of the dispute is discovered, the recipient of the message does not decline to participate in transmission and reception [1].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN210

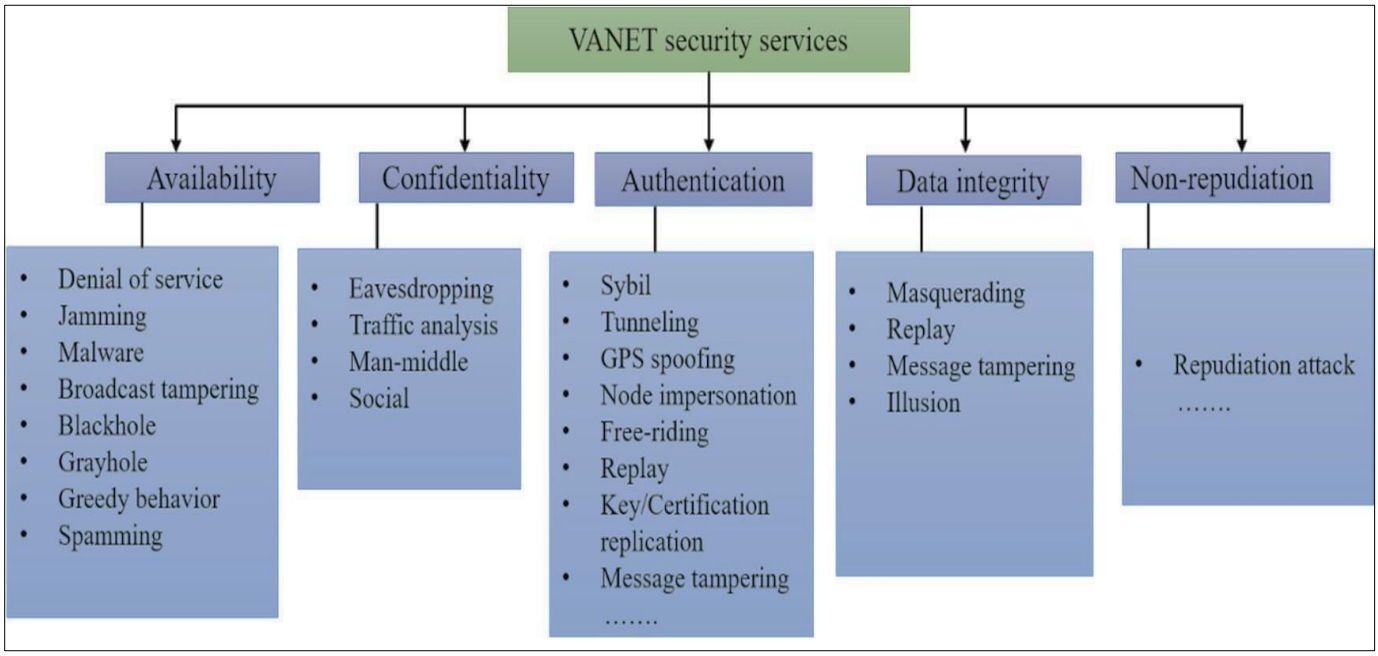

Figure 2. The Security Risks Available within VANET Breakdown [1].

A. Attacks and Security Risks in VANETs

A VANET broadcasts messages in an open access environment, making it more susceptible to attacks. Additionally, because of the network's nodes' high speed, it can be challenging to identify suspicious cars [4].

VANET attacks fall into one of the following categories.

➢ *Insider vs. Outsider Attackers*

Insider attackers are those who are physically present within a node or network and possess significant knowledge about how the system functions. Outside attackers, on the other hand, are unauthenticated users who have less ability to compromise the network than insider attackers [11].

➢ *Active vs. Passive Attackers*

Active attackers don't participate in the conversation, while passive attackers either create phoney messages or don't relay communications they have already received.

➢ *Malevolent vs. Rational Attackers*

while attackers assaulted the network in order to gain personal gains, the primary goal of malevolent attackers is to harm other nodes on the network without receiving any personal benefits. additionally [13].

➢ *Local vs. Extended Attackers*

While extended attackers use all available resources to take control of several networks, local attackers only employed restricted resources on a single vehicle [1,2].

IV. ROUTER PROTOCOLS FOR NETWORKS

Due to its highly dynamic architecture, VANET routing protocols are more difficult to design. Numerous routing protocols have been designed for VANETs, which can be divided into two types. Both position-based and topology-based routing protocols are available.

Topology-based routing techniques transfer data packets between nodes across the VANET by using link information. This mechanism is divided into two subcategories: the proactive approach, which relies on table-driven methodology-related routing techniques, and the reactive approach, which relies on on-demand methodology-related routing techniques [4, 13].

Geographically based routing protocols rely on algorithms linked to the positioning system using location-based apps (like GPS). These apps offer this kind of path-selection data. Furthermore, no tables containing routing information or details about the state of joins with neighbouring nodes are serviced by these protocols [6, 7].

DSR The DSR protocol keeps functional pathways open and makes use of source routing. Route servicing and route detection are its components [5]. To participate in the DSR, a node needs four fundamental data structures, which are regarded as conceptual: a Retransmission Buffer, a Send Buffer, a Route Cache, and a Route Request Table [5].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24JUN210

➢ *Route Request Table*

The target home address of the route discovery divides the table of route requests. The Route Request Table is thought of as a repository for information regarding recent packets that this node has originated or forwarded [5].

➢ *Route Cache*

Every node in the VANET network maintains its own tables, which store the route cache. When a new participant node joins a VANET network utilising the DSR routing protocol, the Route Cache is in charge of keeping track of all the information they request for routing [5].

➢ *Retransmission Buffer*

A node's Retransmission Buffer is the queue of packets that it sends out in anticipation of receiving an acknowledgment from the source path's subsequent hop [14].

➢ *Send Buffer*

Each packet that has been registered in the buffer shall be removed from it and disposed of within the send buffer timeout seconds; this timeout is also linked to the packet's registration time [5].

V. CONCLUSION

Since different new kinds of attacks are being developed, security is the most important feature to include in VANETs. The primary focus of our analysis in this study was on VANET applications, security concerns, assaults, and security vulnerabilities. Excellent routing performance is offered by the Dynamic Source Routing protocol (DSR) in multi-hop wireless ad hoc networks. As demonstrated by our thorough simulation research and our application of the protocol in an actual autonomous vehicle network that drives and routes amongst itself, DSR has a very low routing overhead and can deliver nearly all of the data packets that are sent correctly, even when every node in the network is moving quickly and continuously.

REFERENCES

[1]. Sheikh, Liang, Wang, 2019, ‘A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)’, MDPI, PP 10-14.
[2]. Rajkumar, Nithya, P. Hemalatha. ‘Overview Of Vanet with Its Features and Security Attacks’, International Research Journal of Engineering and Technology (IRJET), Vol. 03, no. 01.
[3]. Mostofa Kamal Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali, ‘Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network’, International journal of scientific & technology research volume 2, issue 4, april 2013.
[4]. Ahmed Yasser, M. Zorkany & Neamat Abdel Kader | (2017) ‘VANET routing protocol for V2V implementation: A suitable solution for developing countries, Cogent Engineering,’ 4:1, 1362802, DOI: 10.1080/23311916.2017.1362802
[5]. Johnson, D.B. and Maltz, D.A. (1996) Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing, 353, 153-181.
[6]. Chakraborty, 2022 ‘Performance Analysis of VANET Based Routing Protocol’, ResearchGate, vol. 13.
[7]. Chaubey, 2016 ‘Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study’ ResearchGate.
[8]. Mahmood, Duan, Yang, Wang, Nebhen, Bhutta, 2021, ‘Security in Vehicular Ad Hoc network: Challenges and Countermeasures’ Hindawi, PP- 3-6.
[9]. Johnson B., Maltz A., Broch, ‘DSR: The Dynamic Source Routing protocol for Multi-Hop Wireless Ad Hoc Networks’ Carnegie Mellon University, PP 3-6;
[10]. J. Pan, S. Paul and R. Jain, "A survey of the research on future internet architectures," in IEEE Communications Magazine, vol. 49, no. 7, pp. 26-36, July 2011, doi: 10.1109/MCOM.2011.5936152.
[11]. R. Mishra, A. Singh and R. Kumar, "VANET security: Issues, challenges and solutions," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016, pp. 1050-1055, doi: 10.1109/ICEEOT.2016.7754846.
[12]. P. G. Shinde and M. M. Dongre, "Traffic congestion detection with complex event processing in VANET," 2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN), 2017, pp. 1-5, doi: 10.1109/WOCN.2017.8065852.
[13]. Y. Xia, X. Qin, B. Liu and P. Zhang, "A greedy traffic light and queue aware routing protocol for urban VANETs," in China Communications, vol. 15, no. 7, pp. 77-87, July 2018, doi: 10.1109/CC.2018.8424605.
[14]. S. S. Sepasgozar and S. Pierre, "Network Traffic Prediction Model Considering Road Traffic Parameters Using Artificial Intelligence Methods in VANET," in IEEE Access, vol. 10, pp. 8227-8242, 2022, doi: 10.1109/ACCESS.2022.3144112.
[15]. V. Hemakumar and H. Nazini, "Optimized traffic signal control system at traffic intersections using VANET," IET Chennai Fourth International Conference on Sustainable Energy and Intelligent Systems (SEISCON 2013), 2013, pp. 305-312, doi: 10.1049/ic.2013.0330.