American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-12, Issue-12, pp-33-46
www.ajer.org
Research Paper Open Access

Advancing security in IoT-Driven critical infrastructure: A focus on smart transportation system

H.O Jimoh[1], C J Abolle-Okoyeagu[2], M.O Ahmed[3], N.O Lawal[1]
[1]*The Federal Polytechnic, Offa*
Kwara State, Nigeria
[2]*Robert Gordon University*
Garthdee House, Garthdee, Aberdeen AB10 7AQ, UK
[3]*Cisco Systems, Nigeria*
Lagos, Nigeria

Abstract
As new technological platforms such as the Internet of Things (IoT), blockchain, Artificial Intelligence (AI) andMachine Learning (ML) are gradually emerging and being integrated into critical infrastructures which are subjected to digital attacks. i.e., the critical systems are vulnerable to new cybersecurity threatsand thus requires corresponding security approach to challenge the threats.It is therefore imperative to identify the various types of possible cyber-attacks on the systems and develop a security framework to manage the associated security risks. IoT-based critical infrastructure systemslike smart healthcare, smart transportation and smart manufacturing are prone to attacks such as Denial of Service (DoS) attacks, brute-force attacks, Man-in-the-Middle attacks (MiTM), Stuxnet computer virus etc.
This paper focuses on a detailed study of the smart transportation system and its security issues; various threat vectors used by the attackers are examinedalongsidecorresponding countermeasures. Additionally,an in-depth analysis on how an identified malicious attack on smart transportationcould be achieved was carried out by using an open-source vehicular network tool called Vehicle in Network Simulation (Veins).A detailed evaluation of the impact of MiTM attack was then carried out based on the evaluation metrics.
Results from the simulation results indicate that attacks on the built STSthesis vehicular network have a higher influence on the network. Also, although the STSthesis was a basic network that was run with considerable node, limited time and injected malicious node, the impact of the MiTM attack was still visible. Furthermore, implementing the elliptic-curve Diffie-Hellman (ECDH) with the Advanced Encryption Standard (AES) in the early stage of design and implementation will prevent the MiTM attacks from intercepting messages between legitimate nodes.

Date of Submission: 06-12-2023 Date of acceptance: 19-12-2023

I. INTRODUCTION

There has been a phenomenal growth in Internet of Things (IoT) over the last decade due to the smart city revolution. The main concept behind IoT is connecting devices to the internet without human intervention. As a result of digital transformation, the number of cyber assets has increased rapidly within the last decade. Similarly, its usage in the critical infrastructure systems such as smart health, smart transportation, smart manufacturing, smart energy etc., has also increased. Each of these critical infrastructure systems has its peculiar security challenges, however, in this work,our focus will be on Smart Transportation Systems.

Smart transportation system has become an indispensable component of every smart city due to its ability to achieve traffic efficiency by reducing traffic problems, accidents and its propensity to enrich users with prior information about traffic,thus enhancing their safety. Recently, the smart transportation system has been subjected to various tests i.e., efficiency and ssafety tests [1]. Thesetests are carried out to ascertain if the features such as energy saving, environmental friendliness, reliability, and most importantly, safety adhere to standards and expectations of the system. All these features contribute to making the transportation system "smart". Essentially, the evaluation of success and failure is used to improve on the efficiency and safety of the

system. However, one of the major concerns about the smart transportation system is its vulnerability to cyber-attack. If a vehicle is connected to a wireless network and open to receive information, it can be hacked or hijacked by a giant botnet. An attacker could release the brake of the vehicle without the knowledge of the driver, open windows or tamper with the global positioning system (GPS) to re-route the vehicle and/or explore any vulnerable means to breach the system. So, it is imperative for cybersecurity experts to develop techniquesfor the vehicle toidentify and validate sources of communication before granting access to the system.

Smart Transportation Systems can be categorized into public infrastructure and the automotive industry. Generally, these two systems use an embedded sensor and GPS to provide the system with remote management control and for geolocation and real-time information. The system also uses the roadsideunit (RSU) which is a transceiver mounted on a road/pedestrian walkway and / or vehicle to provide connectivity and information support to passing vehicles, including safety warnings and traffic information.

A classic example of an RSU is a traffic light which is used to regulate and control the flow of traffic. In a conventional transport system, the traffic lights are triggered either through timers or by the pedestrian pressing the button on the control box. But in a smart city, a vehicle may use Bluetooth or light detection and ranging (LIDAR) or both to detect pedestrians and can automatically begin braking to avoid an accident. The traffic lights can also pick up pedestrian presence and signals sent from the vehicles to determine the number of cars waiting and from which direction the car is coming. Vehicles and traffic lights can also communicate; when the green indicator traffic light turns on, a signal is sent to the vehicle's computer and automatically the car begins to move without any human intervention. Also, when the red indicator is activated, a signal is sent to the vehicle and the moving or up-coming vehicles automatically slows down and stops. This is all possible with the growing rate of use of the IoT in the transport system.

Unfortunately, every smart device is prone to attack, within the scenario outlined above, a cyber-attacker can disrupt vehicle traffic, hijack or manipulate the RSU or use a DoS or MiTM attack to disrupt the vehicular network in a smart transportation system.

As mentioned above, there are several vulnerabilities and cyber-attacks that exist within the smart transport system and in this paper, we will critically examine how a specific attack (MiTM) is carried out by using a simulation modelling framework (Veins) and extensively examining the procedure of safeguarding the IoT devices in accordance with the global cybersecurity framework.

Cyber-Attacks on IoT-based Critical Infrastructure Systems.

Cybersecurity entails the safeguarding of computer networks and IoT; which is about connecting and networking devices. Essentially, IoT comprises of technologies such as smart device and data from the physical world in a global network to provide secured services to end-users. In the cyber world, the most important threat focuses on critical infrastructure such as connected vehicles, connected IoT medical devices, smart homes etc. [2]. These connected devices create a new entry point to the connected network which pose an increasing level of security threat and privacy risk. In a physical attack, since majority of governmental, business and industrial activities rely heavily on either computer network, sensor equipment and/or control systems, its advantages have helped in effective operational activities and its disadvantages have led to an increase in numerous types of cybersecurity threats.

Cyber-Attack on Smart Transportation System

Transportation is a key sector for every developed country to drive economic growth and social inclusion. With the rise of interconnected technologies such as IoT, smart transport system has revolutionized how cites approach mobility and emergency response while minimizing the environmental pollution. This is achieved by the provision of innovative services which are related to various modes of transportation and traffic control and management to allow different users to be well informed and make a safer, more coordinated and better use of transportation network.

As more connected smart transportation systemsare coming online, attacks such as ransomware attacks, Malware, DoS attack, distributed denial of service (DDoS) attacks,MiTM attack, phishing/spear phishing etc. are increasing. Studies have shown that ransomware attacks aretheleading threat against the transport sector [3]. If an attacker observes any vulnerability in the cryptographic mechanism of the system during reconnaissance, an attack can be launched to disable the brakes or disrupt the infotainment services to malfunction. In considering individual attacks, adversaries could attack vehicle management services (e.g., tyre monitoring) by spoofing the sensed data with false data to disrupt driving. Moreover, in a large-scale cyber-attack, a massive number of vehicles will be negatively affected. Also, attacks on operations can directly result in inefficient vehicle operation and failure. For example, failure on route management leads to higher trip costs and can further result in congestion. In this case, adversaries can delay the delivery of traffic condition messages to disrupt efficient route management systems on vehicles. Considering a single small-scale attack, an adversary

could launch a jamming attack to disrupt the delivery of congestion warning messages. Thus, the route optimizations fail to compute an efficient route to avoid congested areas.
Therefore, to improve the cybersecurity of smart transport system, it is crucial to understand the distribution of the cyber threats, it's trends and patterns as well as their potential impact.

Security threats and vulnerabilities in Smart Transportation System
Like any other wireless network, smart transportation systemsare vulnerable to various security attacks despite the significant technological improvement. From a cybersecurity perspective, threat to this system occurs in series of ways, and some are based on the network location of the attacker, motive of the attacker and attack mode as noted below.
Location and Motive of the attacker: This is an important factor as an attacker could be an insider or outsider. An insider attack can directly communicate with other vehicles, but difficult for an outsider.As the smart transport system is considered a trusted node and they are connected via the internet or virtual private network (VPN), an attacker can easily exploit the system to gain unauthorized access into the network to launch malicious attack that can completely destroy the network infrastructure of the system. Some of the reasons that motivate threat actors to launch attack on smart transportation system includes ransom, data theft, information warfare, revenge and terrorism [4].
Attack modes: The mode of attackers can be either active or passive, active attackers actively send packets to invade vehicles or steal cloud services platforms while passive attackers monitor the network only to possibly intercept data to steal.
The major security threat/attack in the Smart TransportationSystem can further be classified into four (4) categories viz: Attacks on Availability, Attacks on Authenticity, Attacks on Confidentiality and Attacks on Integrity [5]. When this happens, it can cause serious damage due to the real time nature of several applications on a smart transport system. A typical example of attack on availability is (DoS) attack. The countermeasure for this kind of attack is by using digital signature: The strategy adopted by digital signature is to create an encrypted message which can only be decrypted through a signer's public key. Signers are supplied with PINs, passwords, codes which will certify and verify their identity before approving their signature. The recipient with the signer's key can access and open available message. This will validate the sender and the integrity of the message's content [6].
Attack on Authenticity: Authenticity is an important attribute that requires to be considered in the early stages of design and implementation of smart vehicles. Generally, authenticity refers to how an application verifies who you are, i.e., who are the authorized users that can access data/information. Therefore, attacks on authenticity are aimed at gaining access to resources without correct credentials to steal vital information about the vehicle or the user with the intent to perpetrate an unlawful act. A typical example of an attack on authenticity is the sybil attack. This attack is the hardest to detect in vehicular network because of its mode of operation. [7].

A few additional security attacks on smart transportation system under authenticity are wormhole attacks, global navigation satellite system (GNSS) spoofing attacks, node-impersonation attacks etc. Wormhole attack occurs mainly in the wireless ad hoc network. It appears in such a way that two attackers strategically locate themselves in the network, thereby listening and recording the wireless information. It is by far one of the hardest attacks to detect on any network [8]. Spoofing has been a growing threat for global navigation satellite system (GNSS)-enabled infrastructure. The attack is common in transportation, power and communication networks. Its method of attack can be compared to jamming which happens when weak GNSS signals are overpowered by stronger radio signals on the same frequency. In node-impersonation attacks, attackers impersonate the RSU in a vehicular network in an attempt to deceive users into giving out their authentication details in order to use it to access sensitive information or impersonate other vehicles [9].
The countermeasure for these kinds of attack is by using digital signature and encryption: All data and information stored on smart transport system needs authentication before it can be assessed. Authentication must be granted when storing and retrieving within the system. To validate an information, a digital signature can be adopted by using a digital certificate. A digital certificate provides a secure environment for the system to operate. The certificate reduces data leakage and hacking risks with point-to-point encryption and flawless authentication [10].

Attack on Confidentiality: Confidentiality is key in the design of smart transportation system where devices within the system should be able to communicate with one another in a secure and private way without exposing information to a third party and to any potential threat actors. Basically, majority of the security threats that target confidentiality in smart transportation system occurs at the network /communication layer [11]. Attackers gather confidential information about the network by quietly observing the traffic or the current position and

activities of a particular vehicle node. Typical example of an attack in this regard is eavesdropping. Eavesdropping attack is "easier and can be passive, i.e., a piece of software can simply be sitting somewhere in the network path and capturing all the relevant network traffic for later analysis. The attacker does not need to have any ongoing connection to the software at all. An attacker can insert the software onto a compromised device by direct insertion or by a virus or other malware, and then come back some time later to retrieve any data that is found or trigger the software to send the data at some determined time. The countermeasure for this kind of attack is by encryption: To prevent attackers from gaining access to confidential data and information, it must be encrypted. The most common encryption method is data encryption standard (DES); a symmetric-key algorithm for encrypting digital data and advanced encryption standard (AES) [12].

Attack on Integrity: Data integrity is impacted by attacks such as masquerading in which a vehicle uses a valid network identifier to broadcast itself as an emergency vehicle and thus affect movement of other vehicles. Among other attacks in this category are replay, and timing attacks. Replay attack which is also known as repeat or playback attack are variant of MiTM and are type of security attack that occurs when the hacker or anyone with an unauthorized access, intercepts and eavesdrops on secured network communication and then act as the original sender. In vehicular networks, replay attacks often target communications between the vehicle and the RSU. If an attacker intercepts a message between an RSU and a vehicle containing the encryption key or password, it would be able to authenticate itself later[13]. Timing attack is a type of an attack called side-channel attacks which occurs by causing a communication delay, thereby disrupting the operation of application that have real-time requirements. Rapid movement of vehicles within the network, introduces the need for real-time updates and exchange of information between both RSUs and vehicles. The real-time updates are needed as any delay of messages can result to compromise of the system. Timing attacks are similar in many ways to black and grey hole attacks. However, instead of dropping all or part of the packets, a malicious node adds a time slot to introduce an intentional delay. This causes major problems, especially in autonomous vehicles, where a delay in time-sensitive information can lead to a major accident. The countermeasure for this kind of attack is by encryption: The integrity of data can be put to test if not secured. With encryption, information on smart transport system will be more protected [14].

The attack on IoT-based critical infrastructure such as smart transportation system are still prone to numerous security attacks despite invention of different security frameworks, as attackers are getting trained and updated always to identify vulnerabilities in the systems.

Currently, there are lots of research work focusing on investigating cyber-attack incidents on critical infrastructure and researcher are developing ways of mitigating such cybersecurity related issues [15]. None has managed to successfully identify and analyse the security threats and vulnerabilities in a smart transport system. The proposed work will enable the integration of artificial intelligence (AI) and machine learning into the development of IoT-based critical infrastructure. This will enhance the detection of any cyber threat on the device in real time.

A typical structure of any smart transport system contains at least one trusted authority (TA), one or multiple fixed roadsideunits (RSU) and massive numbers of mobility on-board units (OBUs) which is also equipped for each nodes/vehicle. Apparently, communications between V2V and V2I are done through a dedicated short-range communication (DSRC), where nodes/vehicles can easily exchange messages or information about their status as shown in figure 1. Due to this nature, nodes in V2V and V2I are vulnerable to attacks such as MiTM, which can alter, replay or impersonate the legitimate message during broadcast. Our problem definition for this paper will focus on one of the examples of Attack on Integrity, which is an MiTM attack.

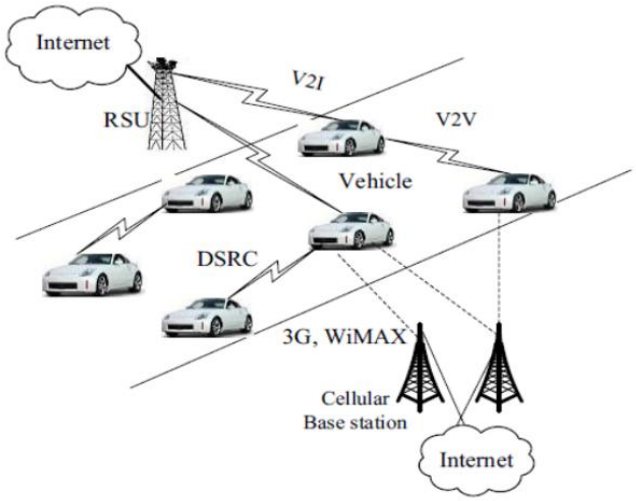

Figure 1: Communication between V2V and V2I through DSRC[16]

MiTM Attacks

MiTM is one of the susceptible attacks that occurs at the network layer when data is transferred using various protocols such as TCP/IP. This attack poses severe risks to smart vehicle because malicious node during the attack could either alter or drop the messages of legitimate nodes/vehicles or eavesdrop during exchange of sensitive information. This could result in violation of security requirement i.e., confidentiality Integrity and Availability (CIA). MiTM attacks usually take two forms:passive or active. A passive attack on smart transportation system is when there is an instance of eavesdropping; where the attacker silently monitors a conversation or reads the contents of message between any legitimate nodes/vehicles. e.g., police vehicles, ambulance, automated teller machine (ATM) among others. For instance, if an attacker successfully initiates MiTM attack on an ATM van, this will enable them to intercept the communication network of the van and share communication with an interested organization for their own benefits. On the other hand, active attack is when an attacker alters, delays or drops the content of the information received in the network or modifies the communication. e.g., infecting the victim with malware. This occurs whenan attacker intercepts information about a traffic accident, he can either alter, delay or drop the message which could lead to legitimate nodes/vehicles receiving compromised messages and these could cause huge road accidents, traffic density and pollution of environment.

Figure 2 shows the holistic view of how MiTM attack occurs within the structure of a smart transportation system. The RSU, which is one of the main elements of V2I for communication is strategically positioned and monitored at the traffic management center. While monitoring is on-going, MiTM attackers are actively listening to the network, by delaying, altering and dropping messages and also eavesdropping communication between legitimate vehicle and the V2I.

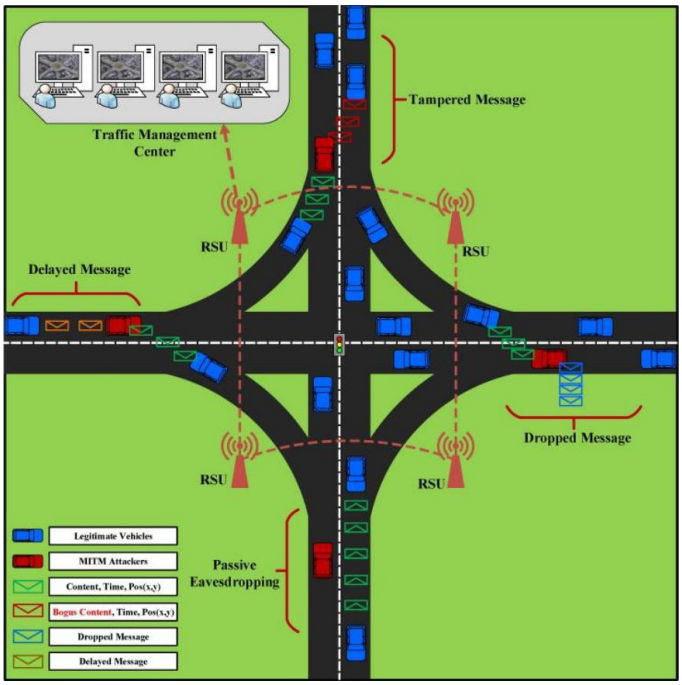

Figure 2: MiTM Attack in Vehicular Adhoc Network [17]

II. Methodology

The main aim of this work is to understudy the performance of vehicular networks in the presence of malicious nodes performing MiTM attacks. To achieve this, the simulation set up shown in figure 3 is used. In this setup, a widely used open-source framework for the simulation of vehicle network, Veins is used.Veins utilizes both OMNET++ (object modular network) and SUMO (simulation of urban mobility) to capture interactions of vehicular networks and traffic. For ease of simulation, it is assumed that the threat actors successfully launch MiTM attack on smart transportation device such as OBU and RSU (smart traffic light), which directly manipulates transmission of message and the frequencies of traffic light.

All these three tools i.e., Veins, OMNET++ and SUMO, work together when evaluating emerging technology of vehicular network (VANET). In most cases, the accident and traffic considerations are collected from SUMO, while the network part i.e., connectivity between vehicles and RSUs are handle by OMNET++. A small patch "TraCI" (traffic control interface) is a technique for interlinking road traffic and network simulators. Whenever an event such as accident information is triggered in OMNET++, TraCI allows other vehicles in SUMO to find an alternative route by sending out respective commands. The communication protocol media access control (MAC) implemented for this simulation is the IEEE 802.11p.

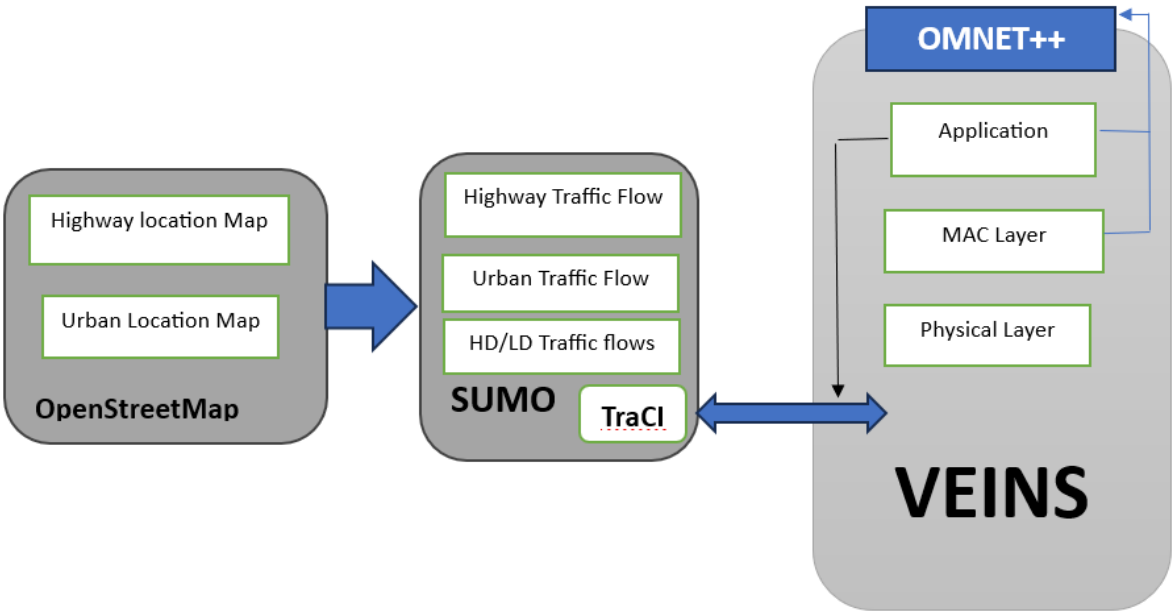

Figure 3: Architecture of Vehicle in Networks (Veins)

To evaluate the MiMT Attack in Veins, a simple network called "STSthesis" (smart transportation system thesis)is built using SUMO GUI, the SUMO GUI interface was specifically chosen for this work due to its ability to create a personalized traffic simulator, which allowed for specification of the number of nodes/vehicles for the proposed attack. Since the OMNET++ provides various modules such as the application layer, physical layer and MAC layer, otherwise known as the DSRC, built layer (STSthesis) was imported into the Vein network.

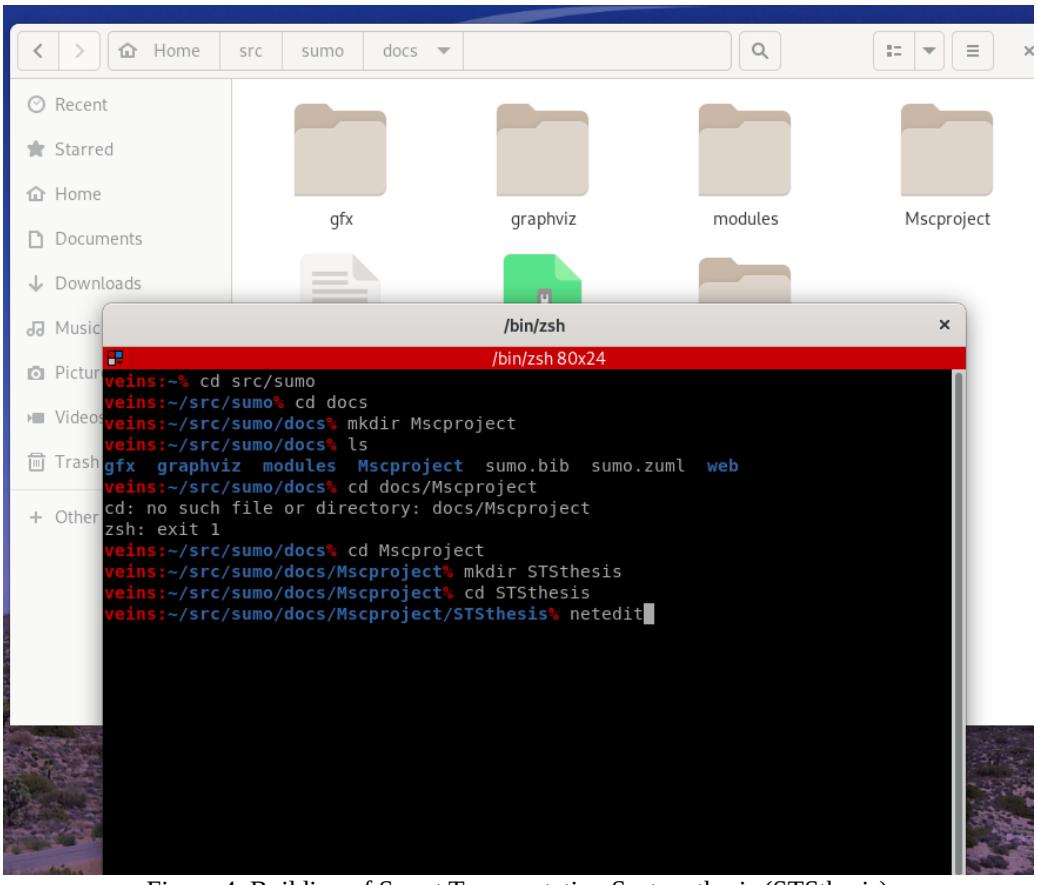

Figure 4: Building of Smart Transportation System thesis (STSthesis)

The Smart Transportation System interface is shown in figure 4, where a new directory for the project called **"STSthesis"** was successfully created. It's pertinent to be in this directory to create the network used in the simulation aspect of this work. In the creation of this network, a network editor **"Netedit"** will be used for the simulation due to the ease in altering nodal positions. Also, for better graphical interface, route and configuration files were created before moving to SUMO for a new project creation in OMNET++ (figure 5) via the instant veins from virtual box. The SUMO files (configuration, route files) are then copied into the newly created project in OMNET++. This is followed by the configuration files from the Veins folder into the STSthesis folder. A network description file (NED) is then created, and the initialization file (ini) was set up.

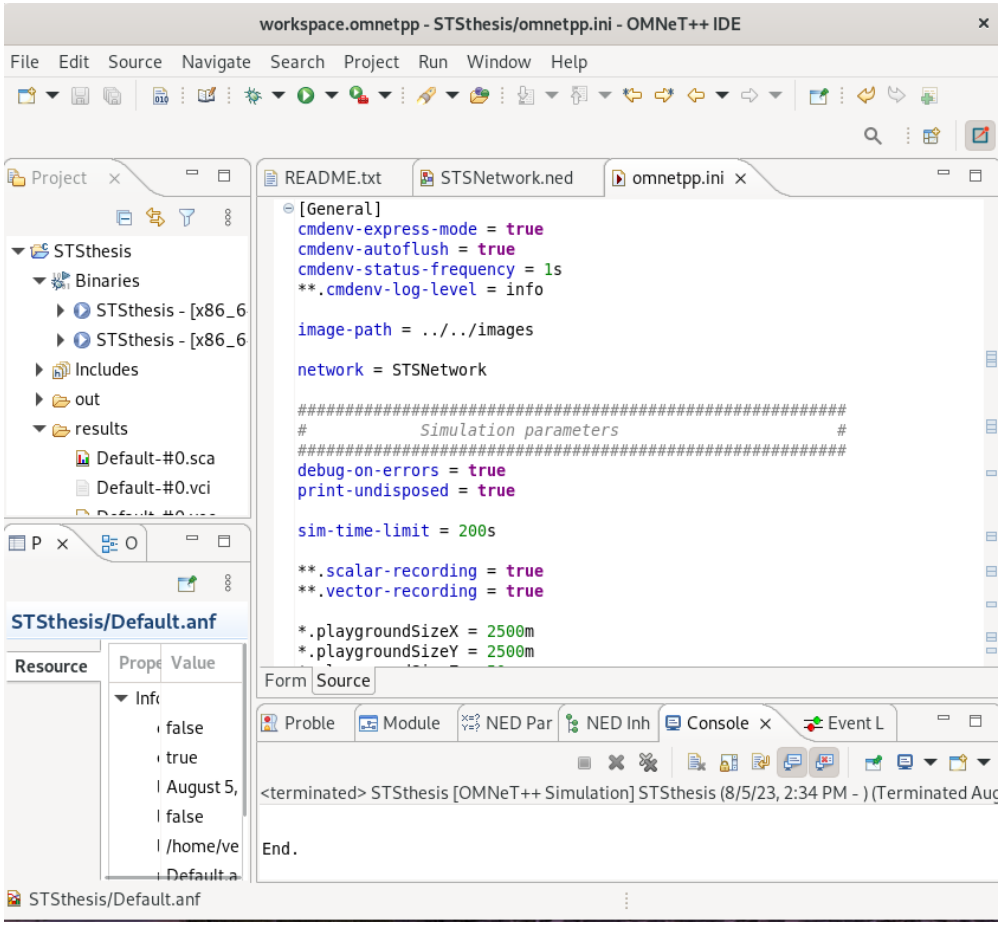

Figure 5: Project Workspace for STSthesis

Launching of MITM Attack

Once the simulation environmentwas successfully set up, theMiMT attackwas launched. For the attack used in this work, the instant vein 5.2i1 was designed with an urban location map and the default map in Veins was used. While on the OMNET++ environment, the SUMO scripting was launched as shown in figure 6. 70 nodes/vehicles were then injected in the network, the time limit was set to 300s, and the simulation was setto run.

Figure 6: Launching of SUMO on VirtualBox

The simulation for STSthesis was run 20 times on the average time of 300s, which was set as our time limit for the simulation. This was done to have sufficient data about the criteria discussed in the evaluation metric and also have an insight about the knowledge of the attack.

To accurately evaluate the performance of the STSthesis vehicular network in the presence of attackers, the highlighted evaluation criteria to access the performance of the network during the MiTM attack was used. These criteria are stated below:

One-Way Delay (OWD): This metric is similar to network quality of service (QoS), i.e., the time taken for a packet to be transmitted across a network from source to destination. The one-way delay in this attack (MiTM), indicates the delay induced by legitimate node packets and then shared with the neighboring nodes. The differences between the Packet generated time and packet receipt time is measured as follows:

$$\mathbf{OWD = PKT_R - PKT_G}$$

Data Delivery Ratio (DDR): The data delivery ratio displays the number of data messages which was successfully received by the legitimate vehicle over the network. This can be achieved by dividing the number of successfully received message M_R by the number of expected messages M_E, which is the number of messages predicted to be received within the network. DDR can be calculated as shown below [18]:

$$\mathbf{DDR = M_R \,/\, M_E}$$

Assuming N vehicles is the total number of vehicles sending messages **(M_S)**, $\mathbf{M_E}$is computed as:

$$\mathbf{M_E = N \times M_S}$$

Packet Loss Ratio (PLR): Packet loss ration indicates the number of packets that got missing due to MiTM nodes. To calculate the packet that are missing during the attack, the total number of lost packets was divided by the number of the received packets from legitimate node. Essentially, each packet sent as a broadcast can potentially be received by lots of other node/vehicle which results to the fact that in a situation where a simulation sent just a single packet, it might record different reception and packet loss ratio. To accurately calculate PLR, let $\mathbf{M_{Tt}}$be the total num of messages and $M_{L,}$ be the number of lost messages:

$$\mathbf{PLR = M_L \,/\, M_T}$$

If the total number of messages (M_T), contains all the messages received at both the legitimate and malicious node, and $\mathbf{M_R}$as the number of received messages at legitimate nodes and$\mathbf{M_L}$ is the number of messages lost at the MiTM nodes, then $\mathbf{M_T}$ is given as:

$$\mathbf{M_T = M_R + M_L}$$

Number of Delayed Messages: This metric generated here will display detailed number of messages emanated from the malicious node, which was compromised.

Number of Dropped Messages: During MITM attack on the vehicular network, the attacker intentionally drops the authentic messages obtained from the legitimate nodes. This metrics will show the number of messages lost by the attackers in the network.

III. Simulation Results

The delay attacks based on the evaluation metrics discussed above. During simulation, once an event such as accident occurs, an airframe which is turn like a broadcasted message is sent to other nodes. During this period, the threat actor launches an attack. The one-way delay (OWD) in the presence of the MiTM causes message delays by 4 seconds as shown in figure 7. Addition of more malicious nodes within the network which could delay legitimate communication or message will eventually cause the one-way delay to increase. Moreso, since the attacker perpetrating the MiTM attack has the capability of delaying broadcasted message or communication within the network, these prevent the legitimate nodes from receiving message on time. Under normal circumstance, the legitimate nodes are received such legitimate messages with minimum delay. In addition, the one-way delay (OWD) significantly increased as the attacker are dispersed around the network.

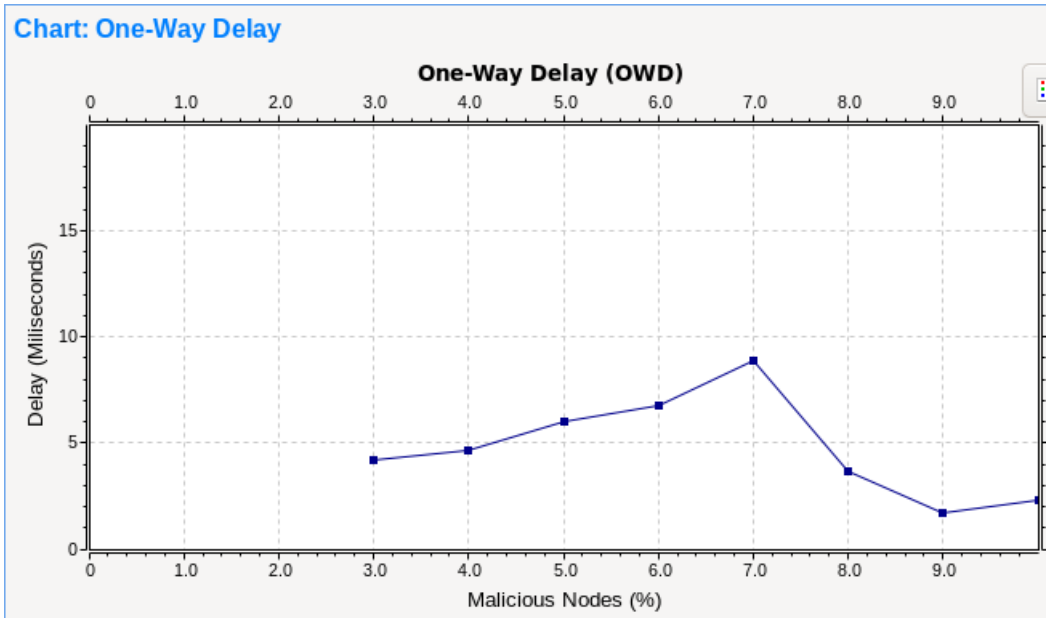

Figure 7: One-Way Delay in Message Delay Attack

Data Delivery Ratio

Figure 8 shows the number of data that can be delivered to the legitimate nodes with potential delays by the attackers via the malicious nodes. When malicious nodes rapidly increase in the network, the number of delays rises and as a result, legitimate nodes receive data but get delayed.

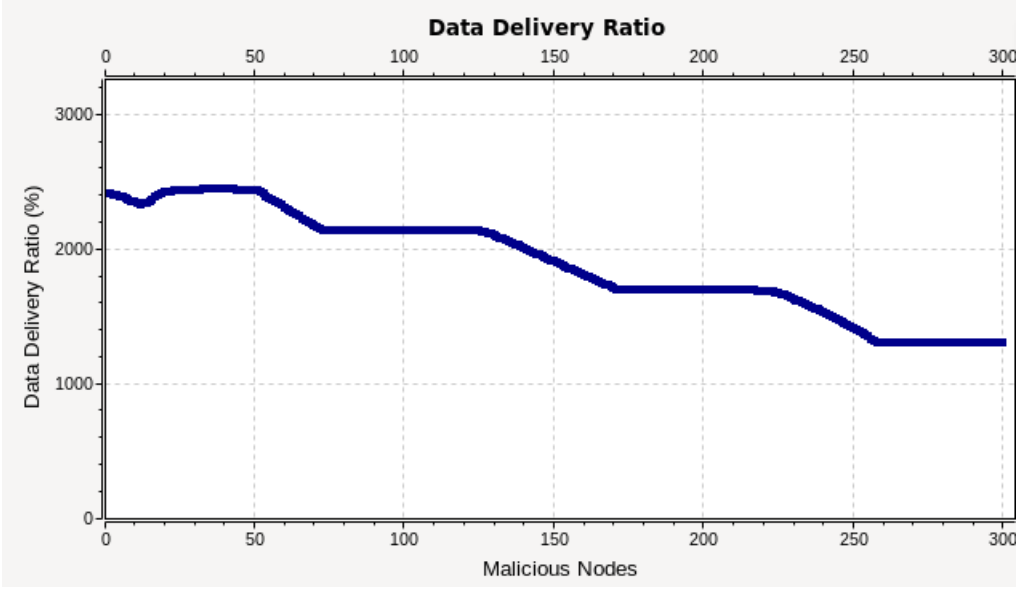

Figure 8: Data Delivery in Message Delay Attack

Packet Loss Ratio

It is demonstrated from the figure9 below that as the packet lossratio (PRL) increases based on the total number of messages sent at random, the number of malicious nodes in the network subsequently increases. For instance, when the vehicular network is flooded with 30% of malicious nodes as shown in figure9, about 15.5% more packets were lost in the presence of attackers. This basically happens because the destination where the packet is been discarded was engaged with excessive delay due to the presence of the malicious nodes.

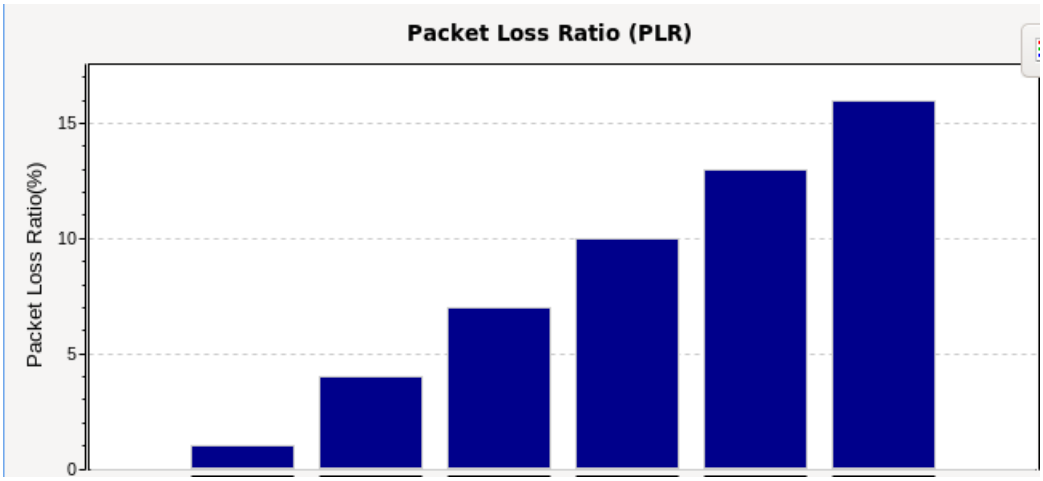

Figure 9: Packet Loss Ratio in Message Delay Attack

Message Dropped Attacks

The OWD in case of message dropped attacks as shown in the figure 10, depicts that the presence of harmful nodes, causes a message drop of about 4 seconds. The reason for the increase in OWD is the addition of harmful nodes which seemingly drops legitimate messages within the network. Under normal circumstances, legitimate nodes should receive messages without dropping, but with the attackers prevent such circumstances to manifest due to their message-dropping capabilities.

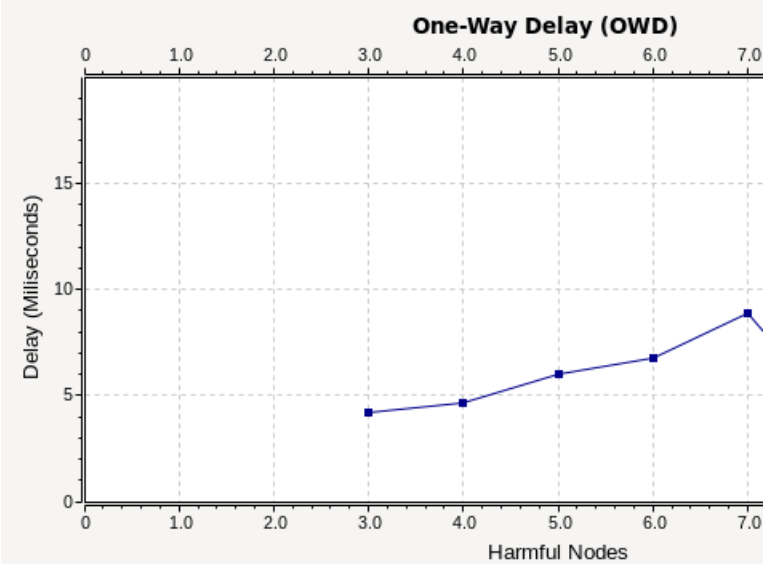

Figure 10: One-Way Delay on Message Dropped Attacks

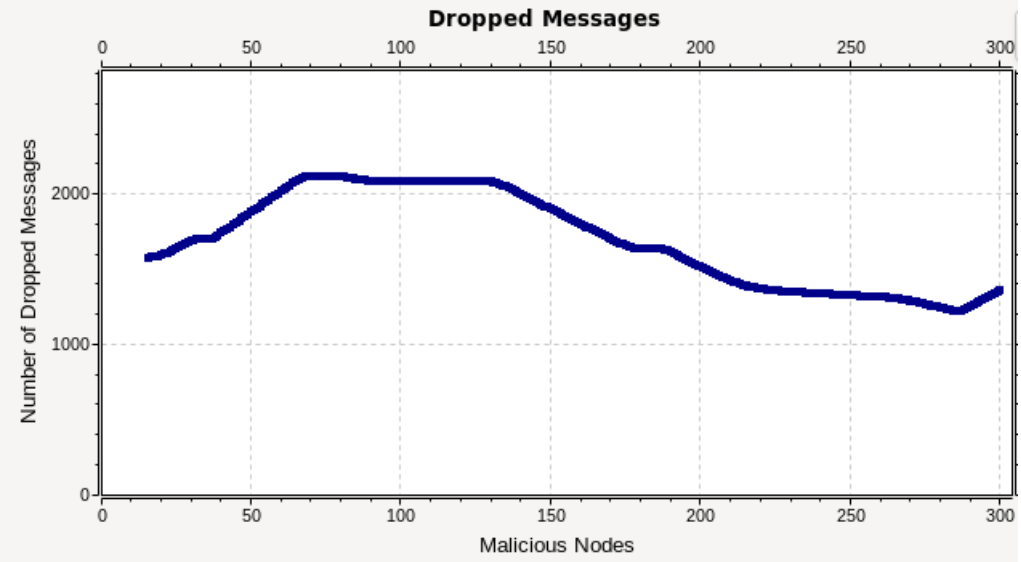

Figure 11: Dropped Messages on Message Dropped Attack

IV. Discussion of Results

In this work, the result was analyzed based on the evaluation metrics and the increase in OWD was observed based on the malicious node injected. It is clearly noted from the simulation results analyzed above that the attack on the built STSthesis vehicular network has a higher influence on the network. Although, the STSthesis was a basic network that was run with considerable node, limited time and injected malicious node, the impact of the MiTM attack was still visible. Additionally, the low data delivery ratio was observed as well as the increase in packet loss ratio and the propagation of delayed and dropped messages. Thus, to achieve a secured approach in managing the vehicular network, it is imperative to put these metrics into consideration prior to implementation on a real network. To address the MiTM attack on the network, the Encryption framework is used because the MiTM attack is a cryptographic attack and when a smart transportation is in operation, the data traffic controlling the IoT device for the system must be properly encrypted by using a very secured channel or method to avoid vulnerability.

Furthermore, as MiTM attackers eavesdrops on data transits to alter, drop or delay a message, the elliptic-curve Diffie-Hellman (ECDH) with advanced encryption standard (AES) was adopted as they are method of encrypting data in transit and can provide both authentication and confidentiality required by the vehicular network. The workflow for ECDH is that when A and B agree on the elliptic curve group E of order n and a primitive element P in E, which then also has the order n. E, n and P are assumed to be known to the adversary. The elliptic-curve discrete logarithm problem (ECDLP), which the ECDH is based on, is defined as the computation of the integer k given P and Q such that Q = [k]P. The ECDH let A and B compute a shared secret key S, using the property of the ECDLP as described below. A selects an integer a in the range [2, n − 1], computes Q = [a]P and sends Q to B. B on the other hand selects an integer b in the range [2, n − 1], computes R = [b]P and sends R to A. A and B receives R and Q respectively, and computes the shared secret key S; S = [a]R =[b]Q = [a][b]P = [$a * bmod(n)$]P. Both A and B get the same value for S, and the shared key is established[19].

To use ECDH in addressing the problem of MiTM attack, a process of authentication will be required, whereby the public keys created in the key exchange algorithm have to be either static or ephemeral. Static key is mostly used in the instance of any cryptographic key establishment scheme. To initiate an authentication in this process, either of the party key has to be static, once this is successfully authenticated, MiTM attack is thwarted. However, to avoid MiTM attack using the ephemeral algorithm, the keys are not necessarily needed to be authenticated as authenticity assurance will be obtained using alternative method.

Using the ECDH with AES algorithm on a vehicular network will provide V2V encryption on a broadcasted request sent to other nodes on the network or the service provider from the V2I, and because of the hardness of AES security, it is impossible for the MiTM attacker to decrypt the V2V encrypted request without obtaining the key messages of each session. Although, MiTM attacker might want to obtain the key messages of each session from the key agreement phase, but due to the hardness of solving elliptic curve computational Diffie Hellman problem (ECCDHP), the MiTM wouldn't succeed in obtaining the key messages. As a result, if this proposal of using ECDH with AES algorithm is considered and implemented in the early stage of design and implementation, this will prevent the MiTM attacks from intercepting messages between legitimate nodes.

V. Conclusion

The integration of the Internet of Thing (IoT) to critical infrastructure especially smart transportation system has provided ease of connectivity between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Therefore, it is imperative for the developer to ensure that during the design phase of any IoT-based critical infrastructure, a design review, threat modelling and penetration testing techniques are implemented. Insecure devices on the network may impact security and privacy if appropriate measures to control it aren't taken. So, to protect the network, it must be ensured that implementation of some international standards such as **ISO/IEC 27400** which provides detailed information about the risk and controls for IoT security and privacy and **ISO/IEC 27001**; which is a security standard that assist in managing and protecting information asset and comply with regulatory and legal requirements related to information security. Moreso, the information security management of an IoT-based critical infrastructure system, who are saddle with the responsibility of protecting the CIA triad of assets from threats and vulnerabilities, must implement certifications such as certified information system auditor (CISA), certified information security manager (CISM) and certified information system security professional (CISSP) or any other certifications related to information security.

However, for the case study of interest, smart transportation system; observation during the search for relevant tool to run vehicular simulation, that the vehicular network is an open network environment which is prone to several cyber-attacks like Man-in-the-Middle (MiTM), Denial-of-Service (DoS) attack etc., but a seamless vehicular network environment is the future of smart transportation system where a safe and secured environment is required to achieve the desired traffic efficiency.

References

[1]. Muhammad, K., Ullah, A., Lloret, J., Del Ser, J. and de Albuquerque, V.H.C., 2020. Deep learning for safe autonomous driving: Current challenges and future directions. IEEE Transactions on Intelligent Transportation Systems, 22(7), pp.4316-4336.

[2]. Liu, X., Qian, C., Hatcher, W.G., Xu, H., Liao, W. and Yu, W., 2019. Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities. IEEE Access, 7, pp.79523-79544.

[3]. Yuryna Connolly, L., Wall, D.S., Lang, M. and Oddson, B., 2020. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. Journal of Cybersecurity, 6(1), p.tyaa023.

[4]. Stoddart, K., 2022. Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In Cyberwarfare: Threats to Critical Infrastructure (pp. 351-399). Cham: Springer International Publishing.

[5]. Lamssaggad, A., Benamar, N., Hafid, A.S. and Msahli, M., 2021. A survey on the current security landscape of intelligent transportation systems. IEEE Access, 9, pp.9180-9208.

[6]. Hahn, D., Munir, A. and Behzadan, V., 2019. Security and privacy issues in intelligent transportation systems: Classification and challenges. IEEE Intelligent Transportation Systems Magazine, 13(1), pp.181-196.

[7]. Chen, S., Pang, Z., Wen, H., Yu, K., Zhang, T. and Lu, Y., 2020. Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks. IEEE Transactions on Industrial Informatics, 17(3), pp.2041-2051.

[8]. Dasgupta, S., Rahman, M., Islam, M. and Chowdhury, M., 2020. Prediction-based GNSS spoofing attack detection for autonomous vehicles. arXiv preprint arXiv:2010.11722.

[9]. Dewanta, F. and Mambo, M., 2019. A mutual authentication scheme for secure fog computing service handover in vehicular network environment. IEEE Access, 7, pp.103095-103114.

[10]. Ahmad, M., Farid, M.A., Ahmed, S., Saeed, K., Asharf, M. and Akhtar, U., 2019, January. Impact and detection of GPS spoofing and countermeasures against spoofing. In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-8). IEEE.

[11]. Arif, M., Wang, G., Bhuiyan, M.Z.A., Wang, T. and Chen, J., 2019. A survey on security attacks in VANETs: Communication, applications and challenges. Vehicular Communications, 19, p.100179.

[12]. Hamza, A. and Kumar, B., 2020, December. A review paper on DES, AES, RSA encryption standards. In 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) (pp. 333-338). IEEE.

[13]. Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y. and Yu, S., 2020. Attacks and defences on intelligent connected vehicles: A survey. Digital Communications and Networks, 6(4), pp.399-421.

[14]. Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., Zhang, Y., Deng, Y., Wen, S., Zhang, J. and Xiang, Y., 2019. An overview of attacks and defences on intelligent connected vehicles. arXiv preprint arXiv:1907.07455.

[15]. Plėta, T., Tvaronavičienė, M., Della Casa, S. and Agafonov, K., 2020. Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases. Insights into regional development. Vilnius: Entrepreneurship and Sustainability Center, 2020, vol. 2, no. 3.

[16]. Dey, K.C., Rayamajhi, A., Chowdhury, M., Bhavsar, P. and Martin, J., 2016. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation. Transportation Research Part C: Emerging Technologies, 68, pp.168-184.

[17]. Ahmad, F., Adnane, A., Franqueira, V.N., Kurugollu, F. and Liu, L., 2018. Man-in-the-middle attacks in vehicular ad-hoc networks: Evaluating the impact of attackers' strategies. Sensors, 18(11), p.4040.

[18]. Chaqfeh, M. and Lakas, A., 2016. A novel approach for scalable multi-hop data dissemination in vehicular ad hoc networks. Ad Hoc Networks, 37, pp.228-239.

[19]. Haakegaard, R. and Lang, J., 2015. The elliptic curve diffie-hellman (ecdh). Online at https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/Haakegaard+ Lang. pdf.

Compliance with Ethical Standards

Competing Interests: The authors declare that they have no competing interests, there are no financial and personal relationships with other people or organizations that could inappropriately influence this work.
Ethical Standards: The authors declare that this study does not contain any studies with human participants or animals.
Data Availability: This study adheres to the principles of data sharing and transparency. We affirm that all relevant the datasets generated and analysed during the current study supporting the findings of this research are provided within the paper and its supplementary materials are also available through the corresponding Author (j.abolle-okoyeagu@rgu.ac.uk).