Middle East Journal for Scientific Publishing

Vol. 4, Issue No. 1, 95-114 (2021)

E-ISSN: 2707-188X

Security Threats in Vehicular Ad Hoc Networks: survey

Noura Alotaibi, & Sabah M. Alzahrani [1]

E-mail: K_moon_n_m@hotmail.com

Received: 17 Oct. 2020, Revised: 20 . 2020, Accepted: 22 Nov. 2020

Published online: 6 Feb. 2021

Abstract

This survey deals with the Vehicle Ad Network (VANET), an updated type of MANET that allows the transportation system to produce road safety and security as well as reduce traffic congestion. This is caused by cars to roadside communications. Moreover, the main concern of VANET is the point of safety. VANET is a hybrid architecture design and dynamic topology, which makes VANET different from other Ad hoc networks. Therefore, it is important to form and design security projects to document broadcast messages and remove bad messages. This review presents different security problems for VANET and also discusses different protection techniques to reduce menaces and categorize the various VANET Security Protection issues.

Keywords: VANETs, Security attacks, Road Side Unit, Authentication, Eavesdropper, Security threats, Information security

[1] College of Computers and Information Technology, Taif University, Saudi Arabia.

1.0 Introduction

In the 1980s, researchers began developing the notion of wireless communication vehicles (van Brummelen, 2018). After this, to solve the problems related to the safety of roads, road user convenience, improve transportation quality, and ecological effects, the development of IVC has enhanced (shan, 2020). VANETs are a part of the Mobile Ad hoc Network that uses Short Range Communications engineering adjusted to a frequency of 5.9 GHz (li). Visual Optical Communication is popular alternate engineering suggested to be utilized in VANETs that provides some advantages and disadvantages once applied to communicates vehicle (Guney, 2020). Visual Optical Communication is a powerful alternative for these applications as the connected capacity extends from 400 to 790 THz which remotely from the frequency of radio and brings to soluting the issue of the radio frequency congestion (kelarestaghik.b, 2019). Unlike DSRC and VLC, VANET's possible access applications consider satellite radio, Bluetooth, and 5G. VANET nodes are vehicles and roadside infrastructures and can allow transportation between vehicles and infrastructures (Raut, 2017). VANET shows some benefits to park, reduced accidents of road, relaxation and comfortable drive. Moreover, it able to provide drivers and travelers with a lot of knowledge such as weather information, entertainment information (Hussain, 2018). VANETs deliver robust solutions to the road and vehicle security and enhance traffic flow as well as efficiency (kelarestaghik.b, 2019). This research surveys the vulnerabilities and countermeasures in securing the VANET in general ad hoc networks then examines the security problems and restrictions that differ found on the incoming applications utilized by VANETs.

In today's digital world, intelligent transportation systems play a much important purpose in each aspect of a recent lifetime (Heijden, 2018). To dominate the previous critical things in the coming, intelligent transportation systems provide comprehensive and advance services that modify traffic administration in the coming

(Lana, 2018). It is presented by the rapidly increasing advances in wireless communicating applications (Qiu t. , 2017) (Jameel, 2018)to apply a smart vehicle. Now carmakers and telecoms manufactures have accepted to equip every product with wireless equipment to empower the cars to make communication with other vehicles as well as the infrastructure on the roadside. VANET is a kind of dedicated mobile phone network and it is considered as a mobile network that utilizes technology for moving each other as nodes in the network to make a connection between vehicles and the nearly constant infrastructure (Garg, 2019). ITS is a key part of revolutionizing the old automobile digital automated vehicle, which can control unwanted events that occur due to traffic accidents, jams and serious accidents. ITS program organizes and communicates the technology with a vehicle network to enhance the safety of transportation and scheme administration. It gives safety for traffic and comfortableness for the passenger and improves passage traveling to minimize bottleneck (Qiu x. , 2020). Each VANET vehicle is shown with node communication devices that are allowed to spread safety messages over radio communication channels. Message types can be periodic (signals) or event-driven (Hasrouny H. , 2019). Previous messages (beacons) are sent periodically by vehicles to notify neighboring vehicles of their condition, such as location, direction and speed. These communications are specifically utilized by nearing vehicles to alert their situation and prevent potential hazards. Last messages are created while an anomalous status or apparent risk is identified and deployed in a specific location as a high-level primacy. It should report event-driven safety communications to the adjacent node with more accuracy and lower time. One late or missing communication may cause loss of lives (Ullah, 2018).

The major contributions of this survey are presented as follows:-

1- Studying VANET's recent attacks and remedies.

2- Study the attacks and remedies that went with applying VANETs accession applications.

3- A comparison of VANETs accession applications from security indicators.

2.0 VANET Architecture

RSU and vehicles communicate via technical wireless titled WAVE or Wireless Access in Vehicle Environment (Roy, 2020). WAVE Connect guarantees occupant safety by changing vehicle info and traffic flow rate continues to strengthen the safety of pedestrians and drivers. It enhances the traffic flow rate and the skillfulness of the traffic control systems (Ehujuo, 2017).VANETs comprise different units such as TA, RSU and OBU. Especially, RSU usually hosts a model that is utilized to connect with other network platforms, and an OBU has been installed in every vehicle to gather useful information about the vehicle such as fuel, fastness and speeding (masood, 2020).After that, the data is transmitted to near vehicles over network wireless. Each interconnected Road Side Unit is also connected to TA through a network wired. TA is the chief through all elements accountable for VANETs servicing (TA, 2016).Road Side Units are computers installed beside the way or in a specific point such as a car parking or at a crossway (wang w.c.v).It is utilized to give local property to pass vehicles. Road Side Units consist of Short Range Communication network devices. Especially, Road Side Units can be utilized to connect with different network hardware within other base networks (lelding B., 2016) .An on-board unit is an OBU found on Global Positioning System (GPS) tracking, while it is normally equipped in each vehicle to take part in vehicle info with RSU or OBU units. OBUs depend on several physical parts such as Resource Command Processor, sensors, user interfaces, and update storage to retrieve the stored data. The primary purpose of the OBU is to communicate with the RSU or OBU units through the wireless link, and it

communicates with other OBU or RSU units as messages. The OBU pick the signal energy from the battery vehicle's and depend on a GPS sensor, an event information recorder, and both back and front word sensors that are utilized to give information to the OBU (Elliot D., 2019) .

3.0 VANETs Characteristics and Disadvantage

Table 1. A summary of characteristic criteria of VANETs.

Characteristic	VANET	Description
Node Density	HIGH	VANET has higher mobility than MANET in reducing the mesh network [20, 21].
Node Speed	Med-to-high	Medium to high (~ 20 to 100 Km/h).
Cost	Expensive	High cost.
Support	Anonymity	The anonymization support structure may allow adversaries to act maliciously

		within a similar frequency band [8].
Topology Change	Quick and dynamic	The network topology changes rapidly, communications durations are short and node densities vary widely [22].
Localization	wide	GPS, AGPS and DGPS.
Power	High	There are no energy restrictions. However, the real time environment is challenging.
Reliability	High	High trustworthy.

VANETs area wireless networks where stabled and mobile nodes connect with each other. This method has features such as redundant disconnects, dynamical topology, and top node movement. Because of the high mobility of the node, the

VANETs topology is dynamical and not able to be predicted. Because of this and another factors like different weather status, VANETs may suffer from different disconnects through the model. It shows other properties of VANETs in Table 1. Each of these features could cause a system vulnerability. Comparison between VANET, MANET has a comparatively greater ability to move. In VANETs, a vehicle's movement is random inside the system and their moving is restricted through the system topology. It structures VANET into structure and Ad hoc situation (Ellot d., 2019) .In the structure situation, it is able to interconnect distinct entities. These entities consider industrialist, Trusted Third Parties, authorization and service providers. industrialist is accountable for vehicle unparalleled identification, while police authorizations handle vehicle enrollment and offence reports. Trusted Third Partie and service provider are presenting multiple service in VANETs environments like location-based services and documented management. The environment of ad hoc is where connection happens between V2I or V2V. This communicating happens with OBU, Trusted Platform Module and sensors are set up for security (Ellot d., 2019).Rely on the access application being utilized, the communication between the industrialist and the ad hoc surrounding changes. For illustration, this communication occurs by RSU when the technical access is DSRC, or 5G BTS of technical access is 5G (Mueck, 2018).

4.0 VANETs challenges and security impacts

VANET features pose some challenges that can affect the implementation of the security approach to establishing secure communications in vehicle to vehicle or vehicle to road. In the next section, we will mention some challenges facing VANET. Liability versus privacy: Access to vehicle info, that able to be utilized in examinations, must be accessible to each vehicle within a case or that could help extract any info. Besides, it must find privacy to ensure that this specific information is kept by allowed structure. Delaying-sensitivity systems: Some VANET systems,

concerned with security and passenger comfortableness, are time-sensitivity so they must have delay believes with some toleration (Hussein, 2017) .Therefore, there should route technologies that implement their purposes with a communication that carries little expenses and lower process times lag. It can create secure functions to conduct monitoring of misconduct activities that can reduce the Quality of Service of VANET, then taking into account the restrictions imposed on these systems.

Network Scales: VANET may include many compounds, and this may impact its functionality whether there is no strong secret scheme that can administer encryption keys for this enormous amount. As a result, a thoughtful scheme must be implemented prior to deployment of VANET to ensure scalability for any changes in the number of connected vehicles. Low Infrastructure: Some potential subjects for VANET rely only on vehicle for communication. Thus, no key servers or routers are utilized, hence a property relation must be based between vehicles utilizing repute administration schemes. Use of wireless connection: VANET networks rely on wireless transmissions to communicate either in V2R or V2V as ad hoc network, and this needs strong safety performances to get covert transmissions and network unity. Multi-hop communication: VANET in communications occasionally rely on multiple vehicles to transmit data that every vehicle has to be passed standard contents to potential nearer in its area.

It must note vehicle behaviors such any misleading or misbehaving vehicles could be separated and punished. Network fluctuations: Communicating between each vehicle is transient so that the communication can be based for a period, then terminate because of speeding between them. Therefore, the potential for long-term situation VANET is little, it is difficult to implement a security approach based on identity verification.

5.0 Applications

VANET applications settings can be categorized into next major subdivisions: spread V2V warn, V2V set communications, V2V shift, and relation between the infrastructure and vehicle warning (I2V or V2I) (Hoque, 2020).The systems of greatest interest may suit those related to safety and comfort. In the most recent information sheet supplied by the United States management of transportation (Renne J, 2020),security applications are presented for the V2I and V2V environment; Pedestrian warn and pre-collision measures are through these systems. On the one hand, safety-related application purpose to give convenience to road individuals and change traffic skillfulness (for example, environmental traveler information's and environmental lane administration). It can be found in the full list of applications in (Cho, 2017).

Some requirements must be found for success of VANET applications in order to have a reliable interaction between compounds. There must be communication vehicles moving with different acceleration and well established successful communication channels between vehicles. The proportion of vehicles equipped with VANET tools is about to rise to those that do not. Moreover, some technical issues such as required message size, latency restrictions, frequency, security levels, and communication ranges are needed (Huan, 2020).Moreover, the introduction of RMS is a critical factor in achieving beneficial VANETs applications. Each vehicle displays in VANET equipped with node communication devices; This allows safety messages to be spread over wireless communication channels. Message types can be either periodic (signals) or event driven (Gupta N, 2016).Previous messages (signals) are sent periodically by vehicles to notify nearby vehicles of their condition such as location, direction and speed. These sheets are utilized specifically by nearby nodes or vehicles to alert their situation and prevent potential hazards. Final messages are created once an unusual status or apparent risk is identified and deployed in a specific

high preference area. Event-driven safety device contents could be communicated to the near or adjacent node with more reliability and shorter time. One late or missing message may result in loss of life (Gyeongcheol, 2020).

VANETs are a sub-class of MANETs, which have many applications that direct different aspects of transportation systems, for example public security, driving assistance, roadside facility locator, road traffic control, highway internet connectivity, in addition to expanding the range of security and effectiveness of highway systems.

There are two kinds of communication technologies in VANETs are implemented:-

1- A vehicles to A vehicles (V2V)

2- A vehicles to Infrastructures (V2I).

Every vehicle based on Global Positioning System (GPS), sensors, antennas, and processors called On Board Units (OBUs) to match with another vehicle. This vehicle is also connected to the roadside infrastructure with fixed space from each other called Roadside Units (RSUs) (lin, 22017).RSUs can be mobile as well as internet. VANETs are required to implement security, reliability, confidentiality and consent measures to provide protection against invaders or malicious people connected to the Internet via V2I because RSUs are linked to Internet nodes. The vehicles are also connected to roadside infrastructures, in a fixed space from each other called Roadside Units. Roadside Units can be motion and can utilize a wireless or wired medium to transmit between them and the Internet. Vehicle can also be communicated with the internet via V2I. Generally speaking, Vanette has two types of applications, one related to safety and the other related to the application of comfort (A- Safety B- Comfort).

Safety application: There are many VANET apps that aim to save people on the streets, which feature safety-related data to the real receiver at the right time.

Messages are helper messages, informational messages, and warning messages. As shown in Figure 1.

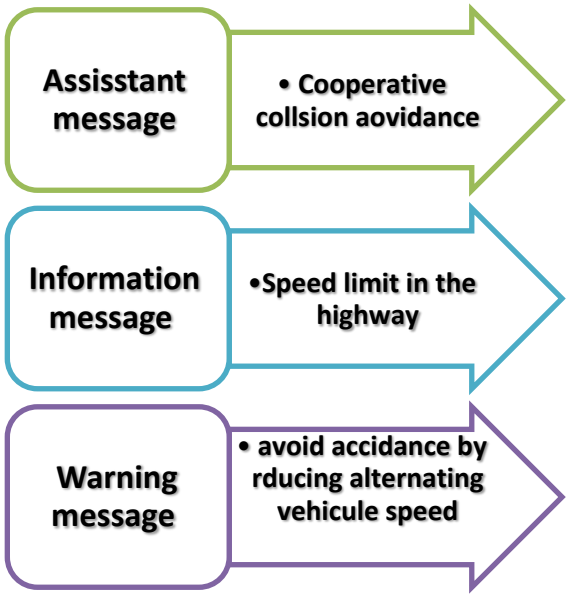

Figure 1. Sample of Safety application technique.

Comfort application: The main goal of the comfort app is to enhance people's satisfaction as well as traffic effectiveness. Some applications (VAS) may include value-added services, such as automatic charging, location-based applications, internet connection, and entertainment applications. The mechanism of this application as shown in Figure 2.

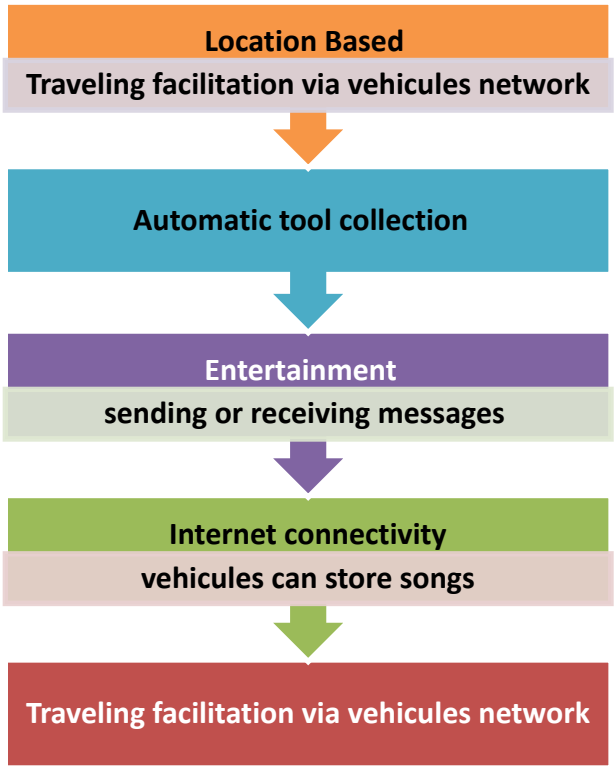

Figure 2. The mechanism of comfort application technique.

6.0 VANETs Attacks

Gaining a strong knowing of the cause and capabilities of a possible opponent is essential to providing an unafraid communications network of whatever kind. Depending on relationship, motive, style, and range, attackers can fall into four classes (.wang, 2019) (Erskine, 2020) in VANETs:

(A) the member (a legal member) and the intruder (the intruder with many restrictions).

(B) A bad attacker has no special gain (like scammers) and a logical attacker follower a rewarding just may be more expected than a bad attacker (such as an avid driver). (C) live attacker for creating packages and inactive attacker for eavesdrop. Relying on how advanced the opponent, their attacks may lead to desperate bad effects. Although another type of attacker exists, insiders (or industry insiders) may

pose the largest risks to VANETs, even the probability is very weak and able to be blocked.

(D) The Localized attackers have constricted powerfulness through the structures, while the extended attackers can power the different structures around VANETs to a greater level.

Relying on how advanced the opponent is, their attacks could lead to critical bad results. Different from other types of attacker, insider (or industry workers) may pose the largest risks to VANETs, even the probability is too low and can be blocked. Various attacks can affect the performance of VANET devices. Some attacks are internal, which are means from inside or from authorized, malicious, or penetrating indoor vehicles. While the others are outside the vehicles, where the attacks occurred from the vehicle's outermost point, or in other words it does not belong to a particular VANET. Moreover, attacks can be discussed according to availability, confidentiality, authentication, and non-repudiation attacks (Hasrouny, 2017) .

7.0 Attack of Authentications

It must authorize every node inside VANETs to be safe from attackers able to penetrate the framework by a false identification. Fail to keep an adequate authorization system can lead to a violent regression of the communicating networks (s, 2018).An authentication is a tool used by VANET, for protection against attacks as shown in Table 2.

Table 2. A types of authentications VANET attacks.

Type of attack	Definition
Message tempering	Exchange message V2Vor V2I
Sybil	Fake identities

	Most dangerous
Message spoofing	Irrelevant message
Free riding	Malicious user take advantage of other authentication
Impersonation	Assertion legitimate vehicles
Message reply	Reshows previous messages
Masquerading	False ID acts as another vehicle

8.0 Attacks on Confidentially

Confidentiality: it is another requirement that only guarantees legitimate user access to data (H, 2018).Failure to address confidentiality jeopardizes the security of exchanged data and affects users' privacy. It is a part of VANET security takes place by confidentiality among the known vehicles. Confidentiality types see table 3.

Table 3. A types of Confidentiality VANET attacks.

Type of attack	**Definition**
Eavesdropping	Secrets information used

	by a non-authorized user
Traffic analysis	Analysis of the frequency by the attacker
Man-in Middle	Attackers control V2V messages
Social attack	Deviation of driver attention

9.0 Attack of Availability

It is an essential demand for VANETs that ensures scheme practicality at every time. Even if the attack on accessibility has been selected as the maximum significant attack, the authors believe that information safety and privacy have a higher primary than accessibility. Because of the hazards related to critical information's being detected by liabilities. A security message won't contain any sensitivity data; authorization will give safety for security message (it requires no encoding). Availability in VANET as efficacy depends on it largely there are many types of attacks as shown in the table 4. Availability confirms VANET is working. It can direct availability threats at both the network and the taking part nodes. There are different attacks be launched to reduce the availability of VANETs. Previous studies have suggested various security mechanisms to thwart threats to availability. Among the attacks that threaten VANET availability, DoS is the most well-known that can affect both RSU and OBU to disrupt and endanger the network. In a DoS attack, enemies either intent to overload the communicating channels or make intrusions to block the usage of the communicating channels. The authentication system based on

signatures proposed in (R, 2020) , founded on the pre-authorization procedure, decrease the effect of DoS attack. This system avoids attacker from powering getting structures to operate duplicate signatures checks.

Table 4. A types of Availability VANET attacks.

Type of attack	**Definition**
Denial of Service	Lack performance external or internal VANET
Jamming	Use of powerful signals to disturb communication
Malware	Penetration of software of RSU & OBU
Black hole	Disturbance of the routing table prevent receive important message
Gray hole	Type of Black hole select part of packet
Greedy behavior	On (MAC) message authentication code lead to traffic jump
Spamming	Large spam messages lead to collisions

10.0 Conclusion

VANETs are expected to increase integrity, rest and transportation efficients and defeat the environmental effects of transportation, but with a safety foothold, all benefits could be diminished. With any vulnerabilities present, attacker can take advantage of VANET availableness, authorization, recognition, privacy, comfort, data confidence, and non-rejection safety targets. An effective security rule must be in line with VANETs safety demands with a comprehensive process. There are much challenges that want to be resolved before it implements VANETs on a high-scale. Present, VANET is going to be the trusted networking platform, which would defend the future of the vehicular application. This paper had a concise survey about the applications, attacks and some solutions. Future works should carry more work to detect different attacks and recognize them in solving and being more precise and accurate to protect the safety message.

References

wang, A. (2019). "A survey on security attacks in VANETs: Communication, applications and challenges." Vehicular Communications 19 .

Cho, y. (2017). "Technology acceptance modeling based on user experience for autonomous vehicles." 대한인간공학회지36.2 .

Ehujuo. (2017). application computer in rood traffic .

Elliot D. (2019). "Recent advances in connected and automated vehicles." Journal of Traffic and Transportation Engineering (English Edition) 6.2.

Ellot d. (2019).

Erskine. (2020). Secure Intelligent Vehicular Network Including Real-Time Detection of DoS Attacks in IEEE 802.11 P Using Fog Computing. Diss.

Garg, s. (2019). Edge computing-based security framework for big data analytics in VANETs." IEEE Network 33.2.

Guney, f. (2020). Vehicular Ad Hoc Network (VANET) Localization Techniques: A Survey." Archives of Computational Methods in Engineering.

Gupta N. (2016).

Gyeongcheol. (2020). "Clustering based cognitive MAC protocol for channel allocation to prioritize safety message dissemination in vehicular ad-hoc network." Vehicular Communications 5.

H, K. (2018). Security and privacy issues in vehicular named data networks: An overview." Mobile Information Systems 2018 .

Hasrouny. (2017). "VANet security challenges and solutions: A survey." Vehicular Communications 7 .

Hasrouny, H. (2019). "VANet security challenges and solutions: A survey." Vehicular Communications 7 .

Heijden, V. d. (2018). "Survey on misbehavior detection in cooperative intelligent transportation systems." IEEE Communications Surveys & Tutorials 21.1 .

Hoque. (2020). *"The extent of reliability for vehicle-to-vehicle communication in safety critical applications: an experimental study." Journal of Intelligent Transportation Systems.*

Huan. (2020). Research on term extraction technology in computer field based on wireless network technology. Microprocessors and Microsystems,.

Hussain, R. (2018). Autonomous cars: Research results, issues, and future challenges." IEEE Communications Surveys & Tutorials 21.2 .

Hussein, A. (2017). *). SDN VANETs in 5G: An architecture for resilient security services. In 2017 Fourth International Conference on Software Defined Systems* .

Jameel, f. (2018). Wireless social networks: A survey of recent advances, applications and challenges." IEEE Access 6.

kelarestaghik.b. (2019). "Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures." arXiv preprint arXiv:1903.01541.

Lana, I. (2018). "Road traffic forecasting: Recent advances and new challenges." IEEE Intelligent Transportation Systems Magazine 10.2 .

lelding B. (2016). vehicular ad-hoc networks." Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct.

li, f. (n.d.). Connectivity probability analysis of VANETs at different traffic densities using measured data at 5.9 GHz." Physical Communication 35 . 2019.

lin, c. (22017). Resource allocation in vehicular cloud computing systems with heterogeneous vehicles and roadside units." IEEE Internet of Things Journal 5.5 .

masood, A. (2020). "Security and Privacy Challenges in Connected Vehicular Cloud Computing." IEEE Communications Surveys & Tutorials .

Mueck, M. (2018). . Networking Vehicles to Everything: Evolving Automotive Solutions. Walter de Gruyter GmbH & Co KG, .

Qiu, t. (2017). "Heterogeneous ad hoc networks: Architectures, advances and challenges." Ad Hoc Networks 55 .

Qiu, X. (n.d.). "Heterogeneous ad hoc networks: Architectures, advances and challenges." Ad Hoc Networks 55 . 2020.

Qiu, x. (2020). . China 40 Years Infrastructure Construction. Springer Singapore.

R, P. (2020). Cyber Security: The Lifeline of Information and Communication Technology. Springer, .

Raut, c. (2017). "Intelligent transportation system for smartcity using VANET." 2017 International Conference on Communication and Signal Processing (ICCSP). IEEE.

Renne J. (2020). *Emergence of resilience as a framework for state Departments of Transportation (DOTs) in the United States." Transportation Research Part D: Transport and Environment 82* .

Roy, s. (2020). Application of Computer Technology in Road Traffic Control in Enugu State. Diss. 2017..

s, A. (2018). security algorithm in terms of trust computation error and normalized routing overhead." Journal of Sensors .

shan, m. .. (2020).). Demonstrations of Cooperative Perception: Safety and Robustness in Connected and Automated Vehicle Operations.

TA, V. (2016). Automated road traffic congestion detection and alarm systems: Incorporating V2I communications into atcss.

Ullah. (2018). "Emergency message dissemination schemes based on congestion avoidance in VANET and vehicular FoG computing." IEEE Access 7 .

van Brummelen. (2018). . *"Autonomous vehicle perception: The technology of today and tomorrow." Transportation research part C: emerging technologies 89.*

wang w.c.v, 2. (n.d.). Fusion of Environmental Sensing on PM2. 5 and Deep Learning on Vehicle Detecting for Acquiring Roadside PM2. 5 Concentration Increments." Sensors20.17.