International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 07, July-2019

Analysis and Detection of DoS Attack in Designed System using Time Stamp Protocol

Ankush Hans
M.Tech Research Scholar
Department of Computer Science
CTITR, Jalandhar

Dr. Anurag Sharma
Assistant Professor
Department of Electronics and Communication
CTITR, Jalandhar

***Abstract*:- Network security has a pivotal role in vehicular ad hoc networks mainly due to the size and complexity of the network. There are a number of generic tools which are commonly being used by organizations as well as individual users for security like Anti-Spam, Anti-Virus etcetera. In this paper different aspects of security in vehicular ad hoc (e.g. multi-layer intrusion detection technique in multi hop network of vehicular ad hoc network, security problems relates between multi-hop network and Vehicular nodes in vehicular ad hoc etc) are being discussed. The simulation has been done in java using socket programming and multi-programming principles and techniques. The aim of this implementation is to provide inter communication between the clients (Vehicular Ad hoc Network Nodes) and server (Wireless sensor network) using socket programming so that the main objectives such as Inter vehicle communication, Neighbor updates, Collision detection, Collision prevention, Malicious node detection can be achieved successfully**

INTRODUCTION

Vehicle Ad Hoc Network is a form of Mobile ad-hoc network, it provides communications between the different vehicles and the fixed equipment, usually described as roadside equipment. Vehicular Ad-hoc Networks are emerging in an advanced version of the mobile ad hoc network or MANET [1]. It is a distributed type of network, which means that the networks built up by moving vehicles itself, and it works on the characteristics of very high node mobility and limited degrees of freedom in the mobility patterns. The main purpose of the VANET is to provide road safety and comfort to the passengers. It has the outstanding properties of self maintenance and self-configuring. Also, it can make and break the connection in a network. In VANET security is considered as one of the primary concerns in order to provide secure communication between different nodes in a VANET environment [2]. VANET has its own characteristics and due to its characteristics only vehicular ad hoc network security come in advanced or the popular research topic [5]. In today’s scenario vehicular ad hoc network becomes one of the main topics in research.

Wireless sensor network is also a form of adhoc network. A sensor network is a collection of a large number of sensor nodes that are deployed in a particular region. Sensors are wirelessly connected and they, at appropriate times, relay information back to some selected nodes [6]. These selected nodes then perform some computation based on the collected data to derive an ultimate statistic to allow critical decisions to be made. There are a variety of sensors, including acoustic (sound related), seismic (subject to an earthquake or earth vibration), image, heat, direction, smoke, and temperature sensors [7].

VANET has many challenges associated with it like open network architecture, shared wireless medium, stringent resource constraint, highly dynamic network topology. Also the wired network solution do not work with VANET domain. Due to different-different properties of vehicular ad hoc networks like infrastructure less and self-organizing, there are more chances for trusted node to be compromised and launch attacks on networks. In other words, the need is to cover up the VANET from both insider and outsider attacks, in which it is more difficult to deal with insider attack [8]. Moreover, it is difficult to distinguish between stale routing and faked routing information because mobility of node mechanism. There are more chances of attack in node mobility mechanism it is because it enforces frequent networking reconfiguration.

RELATED WORK

Zhang.X.et al proposed that CTB protocol includes two parts, broadcast in a street and broadcast at intersections. even if some selected forwarders fail to receive the message, other forwarders having received the message can still rebroadcast which reduces the broadcast delay and increases the broadcast reliability[1]. Siti.S.et al. analysed the parameters of VANET and their consequences .VANET handover based on long term evolution advanced (LTE-A) using decision techniques able to be a solution model approach to quality of service[2]. Navjot.K.et al. analysed that various requirements, characteristics, challenging issues & techniques of security in VANETs. Theoretical analyses of different security techniques of vehicular Ad hoc Network has been done which compare different schemes at different levels like hardware, authentication, privacy and certification techniques[3].Patel A.et al. reviewed the paper for defending against worm hole attacks in wireless sensor networks. This type of attack majorly affects the network layer of network. This paper deals with detection of worm hole attack and an approach for prevention is proposed. The proposed approach is based on Hash based compression function (HCF) which is actually using any secure hash function to compute a value of hash field for RREQ packet[4]. Lyamin N.et al. analysed a Denial-of Service (DoS) attacks in IEEE 802.11p vehicular ad-hoc networks (VANETs) is proposed. The study is focused on the ”jamming” of periodic position messages (beacons) exchanged by vehicles in a platoon. Probabilities of attack detection and false alarm are estimated for two different attacker models[5]. Campolo C.et al. reviewed the main open issues related to the use of multiple channels in vehicular networks. The analysis starts from the consideration that several design challenges unique to the vehicular environment need to be addressed in order to make decisions on the adoption, adaptation, and improvement of the multichannel architecture proposed by standardization bodies. Standardization efforts and related literature have been surveyed that provide countermeasures for some of the identified issues, which are under discussion in relevant bodies or still uninvestigated[6]. Bergenhem C.et al. analysed the project vision is to develop and integrate solutions that allow vehicles to drive in platoons with a reduction in fuel consumption, improvement in safety and increased driver convenience. A platoon according to SARTRE is a manually controlled lead vehicle with a number of automatically controlled (both longitudinally and laterally) following vehicles[7]. Gambhir S.et al. proposed Prime product number based malicious node detection scheme for MANETs. One of the principal routing protocol AODV used in MANETs. The security of AODV protocol is influence by malicious node attack. In this attack, a malicious node injects a faked route reply claiming to have the shortest and fresh route to the destination. However, when the data packets arrive the malicious node discards them[8]. Pelechrinis K.et al. implemented Jamming techniques vary from simple ones based on the continual transmission of interference signals, to more sophisticated attacks that aim at exploiting vulnerabilities of the particular protocol used. In this survey, we present a detailed up-to-date discussion on the jamming attacks recorded in the literature [9]. Mustafa.B.et al. reviewed in this study different ad hoc routing protocols for VANET. The main aim of our study was to identify which ad hoc routing method has better performance in highly mobile environment of VANET. To measure the performance of routing protocols in VANET, we considered two different scenarios i.e. city and highway. Routing protocols were selected carefully after carrying out a literature review. The selected protocols were then evaluated through simulation in terms of performance metrics i.e. throughput and packet drop [10].

SIMULATION SET UP

A virtual ad hoc network is designed and simulated using NetBeans with the following parameters and their respective conditions. At server side, three main sensors server sensor, collision sensor and fuel sensors which are connected to the vehicles and collects the information which is further stored in the database of the system. At client side, nodes are activated which are basically vehicles that are to be connected to the server or the wireless access vehicular network (WAVE). After activation of nodes, vehicles are activated which is equal to the number of nodes that are being activated by the client side. At the activated sensor, the information of vehicles regarding quantity of fuel left, collision prevention distance left, neighbor vehicles etcetera.

Sr .no.	**Parameters**	**Conditions**
1	Protocol	802.11p
2	Nodes	3
3	Total Distance	10000 m
4	Speed limit	30-50 km/h
5	Collision sensor activate	<100 m b/w vehicles

Table 1: Conventional system parameters

Sr .No.	**Parameters**	**Conditions**
1	Protocol	802.11p
2	Nodes	3
3	Distance	1000 m
4	Speed limit	30-50 km/h
5	Collision sensor activate	<100 m
6	Malicious node	By using TSP

Table 2: Designed system parameters

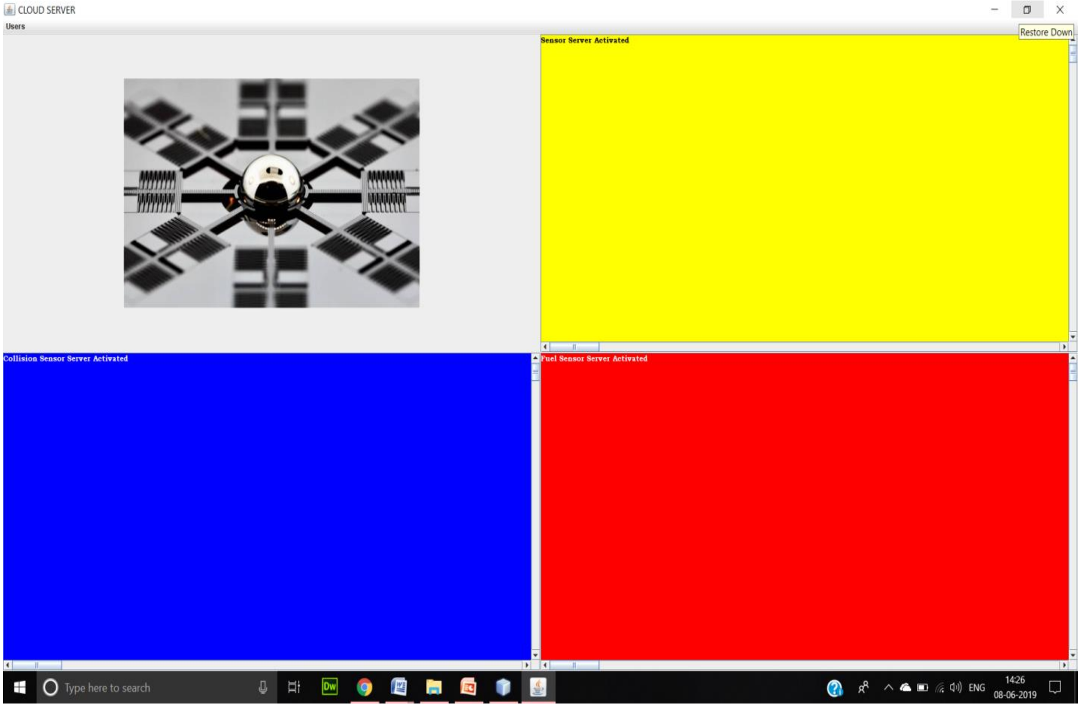
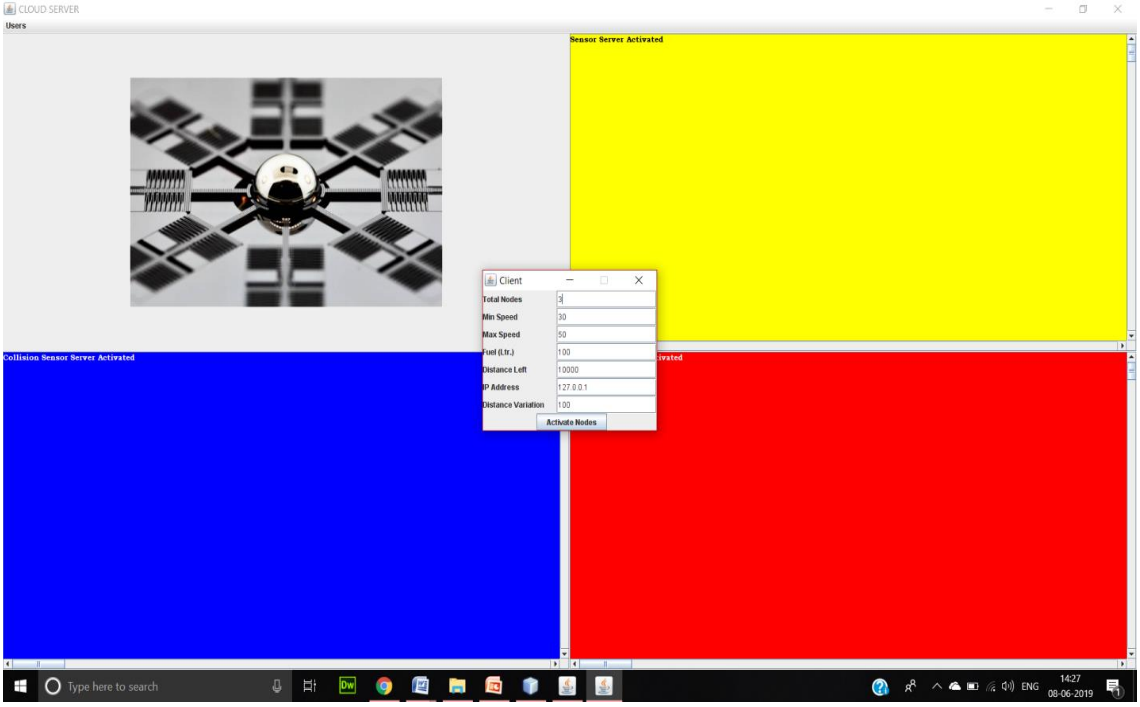


Figure 1: Server side of designed system

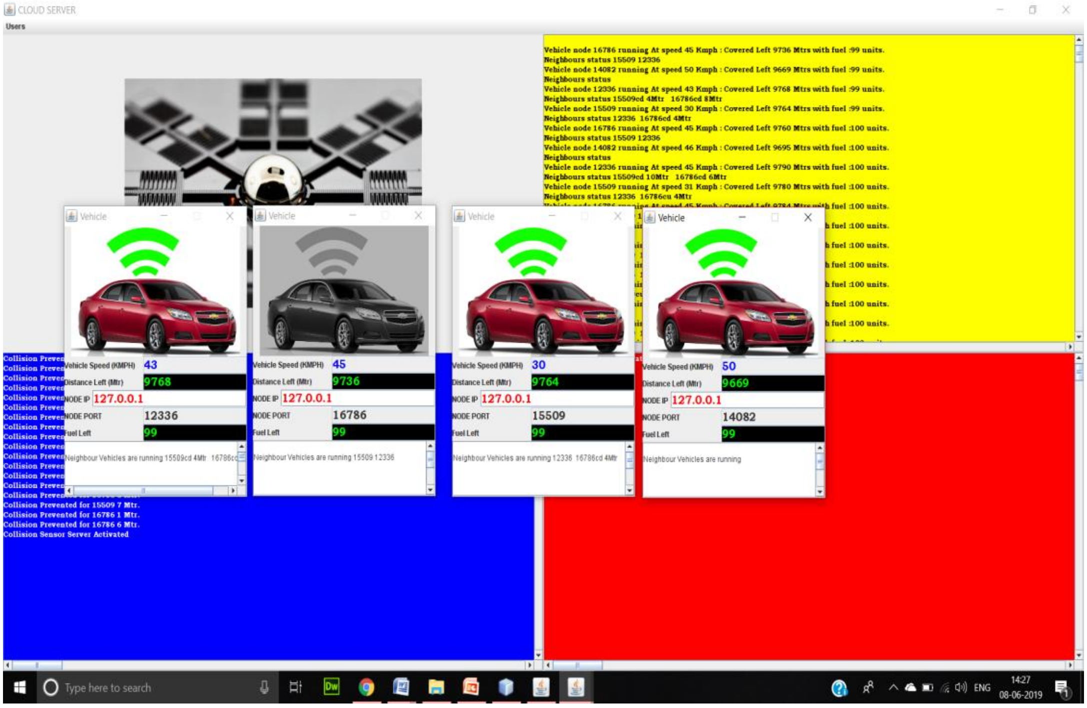


Total Nodes 3
Min Speed 30
Max Speed 50
Fuel (Ltr.) 100
Distance Left 10000
IP Address 127.0.0.1
Distance Variation 100

Figure 2: Client side of designed system

RESULTS AND DISCUSSION

A malicious node is detected by using time stamp protocol in which the distance from source destination to the next RSU is calculated. If the distance is covered with in the time or exact time, it is termed as an authorized node or vehicle. If the time taken to cover the distance is more than the exact time, it is termed as a malicious node or unauthorized vehicle. Using the designed system the detection of malicious nodes becomes easy and it further prevents any false alarming. Hence, the designed system is much better in performance as compared to the previous systems in use.



```
Vehicle node 16786 running At speed 45 Kmph : Covered Left 9736 Mtrs with fuel :99 units.
Neighbours status 15509 12336
Vehicle node 14082 running At speed 50 Kmph : Covered Left 9669 Mtrs with fuel :99 units.
Neighbours status
Vehicle node 12336 running At speed 43 Kmph : Covered Left 9768 Mtrs with fuel :99 units.
Neighbours status 15509cd 4Mtr   16786cd 8Mtr
Vehicle node 15509 running At speed 30 Kmph : Covered Left 9764 Mtrs with fuel :99 units.
Neighbours status 12336  16786cd 4Mtr
Vehicle node 16786 running At speed 45 Kmph : Covered Left 9760 Mtrs with fuel :100 units.
Neighbours status 15509 12336
Vehicle node 14082 running At speed 46 Kmph : Covered Left 9695 Mtrs with fuel :100 units.
Neighbours status
Vehicle node 12336 running At speed 45 Kmph : Covered Left 9790 Mtrs with fuel :100 units.
Neighbours status 15509cd 10Mtr   16786cd 6Mtr
Vehicle node 15509 running At speed 31 Kmph : Covered Left 9780 Mtrs with fuel :100 units.
Neighbours status 12336  16786cu 4Mtr
```

```
Collision Prevented for 15509 7 Mtr.
Collision Prevented for 16786 1 Mtr.
Collision Prevented for 16786 6 Mtr.
Collision Sensor Server Activated
```

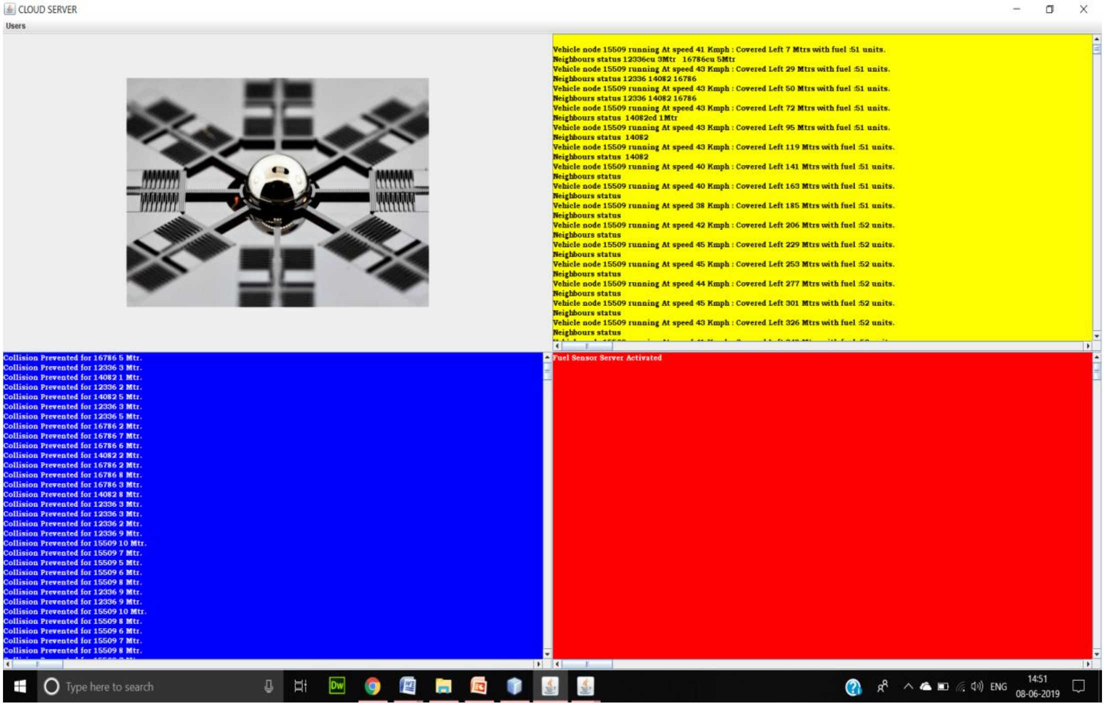
Vehicle Speed (KMPH) 43
Distance Left (Mtr) 9768
NODE IP 127.0.0.1
NODE PORT 12336
Fuel Left 99
Neighbour Vehicles are running 15509cd 4Mtr 16786cd

Vehicle Speed (KMPH) 45
Distance Left (Mtr) 9736
NODE IP 127.0.0.1
NODE PORT 16786
Fuel Left 99
Neighbour Vehicles are running 15509 12336

Vehicle Speed (KMPH) 30
Distance Left (Mtr) 9764
NODE IP 127.0.0.1
NODE PORT 15509
Fuel Left 99
Neighbour Vehicles are running 12336 16786cd 4Mtr

Vehicle Speed (KMPH) 50
Distance Left (Mtr) 9669
NODE IP 127.0.0.1
NODE PORT 14082
Fuel Left 99
Neighbour Vehicles are running

Figure 3: Malicious node detection



```
Vehicle node 15509 running At speed 41 Kmph : Covered Left 7 Mtrs with fuel :51 units.
Neighbours status 12336cu 3Mtr   16786cu 5Mtr
Vehicle node 15509 running At speed 43 Kmph : Covered Left 29 Mtrs with fuel :51 units.
Neighbours status 12336 14082 16786
Vehicle node 15509 running At speed 43 Kmph : Covered Left 50 Mtrs with fuel :51 units.
Neighbours status 12336 14082 16786
Vehicle node 15509 running At speed 43 Kmph : Covered Left 72 Mtrs with fuel :51 units.
Neighbours status  14082cd 1Mtr
Vehicle node 15509 running At speed 43 Kmph : Covered Left 95 Mtrs with fuel :51 units.
Neighbours status  14082
Vehicle node 15509 running At speed 43 Kmph : Covered Left 119 Mtrs with fuel :51 units.
Neighbours status  14082
Vehicle node 15509 running At speed 40 Kmph : Covered Left 141 Mtrs with fuel :51 units.
Neighbours status
Vehicle node 15509 running At speed 40 Kmph : Covered Left 163 Mtrs with fuel :51 units.
Neighbours status
Vehicle node 15509 running At speed 38 Kmph : Covered Left 185 Mtrs with fuel :51 units.
Neighbours status
Vehicle node 15509 running At speed 42 Kmph : Covered Left 206 Mtrs with fuel :52 units.
Neighbours status
Vehicle node 15509 running At speed 45 Kmph : Covered Left 229 Mtrs with fuel :52 units.
Neighbours status
Vehicle node 15509 running At speed 45 Kmph : Covered Left 253 Mtrs with fuel :52 units.
Neighbours status
Vehicle node 15509 running At speed 44 Kmph : Covered Left 277 Mtrs with fuel :52 units.
Neighbours status
Vehicle node 15509 running At speed 45 Kmph : Covered Left 301 Mtrs with fuel :52 units.
Neighbours status
Vehicle node 15509 running At speed 43 Kmph : Covered Left 326 Mtrs with fuel :52 units.
Neighbours status
```

```
Collision Prevented for 16786 5 Mtr.
Collision Prevented for 12336 3 Mtr.
Collision Prevented for 14082 1 Mtr.
Collision Prevented for 12336 2 Mtr.
Collision Prevented for 14082 5 Mtr.
Collision Prevented for 12336 3 Mtr.
Collision Prevented for 12336 5 Mtr.
Collision Prevented for 16786 2 Mtr.
Collision Prevented for 16786 7 Mtr.
Collision Prevented for 16786 6 Mtr.
Collision Prevented for 14082 2 Mtr.
Collision Prevented for 16786 2 Mtr.
Collision Prevented for 16786 8 Mtr.
Collision Prevented for 16786 3 Mtr.
Collision Prevented for 14082 8 Mtr.
Collision Prevented for 12336 3 Mtr.
Collision Prevented for 12336 3 Mtr.
Collision Prevented for 12336 2 Mtr.
Collision Prevented for 12336 9 Mtr.
Collision Prevented for 15509 10 Mtr.
Collision Prevented for 15509 7 Mtr.
Collision Prevented for 15509 5 Mtr.
Collision Prevented for 15509 6 Mtr.
Collision Prevented for 15509 8 Mtr.
Collision Prevented for 12336 9 Mtr.
Collision Prevented for 12336 9 Mtr.
Collision Prevented for 15509 10 Mtr.
Collision Prevented for 15509 8 Mtr.
Collision Prevented for 15509 6 Mtr.
Collision Prevented for 15509 7 Mtr.
Collision Prevented for 15509 8 Mtr.
```

```
Fuel Sensor Server Activated
```

Figure4:Designed system runs successfully without false alarming.

CONCLUSION

In this paper, the main focus is to improve the functioning of the VANET by designing a system which can easily detect the false alarms. Also, it has been observed that after detection of malicious nodes there is not any issue of false alarming which was the prevalent issue in the previous literature, so it has been derived from the results that the designed system is able to detect malicious nodes without generating false alarming**.** Hence, it is far better in performance then the previous networks.

REFERENCES

[1] Lyamin, Nikita. "Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks." IEEE Communications letters 18.1 (2014): 110-113.

[2] Bergenhem, Carl, Erik Hedin, and Daniel Skarin. "Vehicle-to-vehicle communication for a platooning system." Procedia-Social and Behavioral Sciences 48 (2012): 1222-1233.

[3] C. Campolo, A. Molinaro, Multichannel communications in vehicular ad hoc networks: a survey // IEEE Communications Magazine, vol. 51, no. 5, pp. 158–169, 2013.

[4] S.K. Pelechrinis, M. Iliofotou, S.V. Krishnamurthy, Denial of service attacks in wireless networks: the case of jammers // IEEE Communications Surveys and Tutorials, vol. 13, no. 2, pp. 245–257, 2011.

[5] Mustafa, Bilal. Issues of Routing in VANET. Diss. Blekinge Institute of Technology, 2010.

[6] Papadimitratos, Panagiotis. "Secure vehicular communication systems: design and architecture." IEEE Communications Magazine 46.11 (2008): 100-109.

[7] Patel, Anal, Nimisha Patel, and Rajan Patel. "Defending against wormhole attack in MANET." 2015 Fifth International Conference on Communication Systems and Network Technologies. IEEE, 2015

[8] Kaur, Navjot, and Sandeep Kad. "A review on security related aspects in vehicular adhoc networks." Procedia computer science 78 (2016): 387-394.

[9] Nebbou, Tawfiq, Mohamed Lehsaini, and Hacène Fouchal. "Partial backwards routing protocol for VANETs." Vehicular Communications (2019): 100162..

[10] Siti Sabariah Salihin, Rafidah Md Noor, Liyth Ahmed Nissirat and Ismail Ahmedy. “Vehicular Ad Hoc Network (VANET) Handover Based on Long Term Evolution Advanced (LTE-A) Using Decision Technique”. FCSIT 2017: pp 9-17