A Secure DSR Routing against Blackhole Attack to Improve Traffic in VANET

Rakhee Singhai
Dept. of Computer Science and Engineering
Adina Institute of Science and Technology, Sagar (MP)
India

Rajneesh Pachouri
Dept. of Computer Science and Engineering
Adina Institute of Science and Technology, Sagar (MP)
India

Anurag Jain
Dept. of Computer Science and Engineering
Adina Institute of Science and Technology, Sagar (MP)
India

ABSTRACT

The requirement of secure communication is very crucial part in network due to presence of unwanted attackers. The SDSR is identified the packet dropping but only due to presence of attacker. If an intrusion is detected quickly enough, the intruder can be identified and turned out from the network before any harmful action is done or any data are compromised. Moreover, proposed SDSR have served as prevention, acting to prevent intrusions. Proposed scheme enables the collection of information about intrusion techniques that can be used to reinforce the intrusion prevention facility. The performance of previous scheme is better and secure network from calculating the trust value of values and the trust value calculation is dependent on the packets forwarding of nodes in network. The performance of normal routing, with presence of Balckhole attack (BAODV), Old-Prevention (SAODV) and Proposed SDSR prevention performance is evaluated. The performance of proposed security system is better because at receiver end identified the packets dropping and set the threshold of dropping and also identified the attacker infection existence in network that shows the attacker effect and also affected the routing performance of network. The proposed SDSR performance is measured through performance metrics and a result shows the improvement in performance..

Keywords

VANET, SDSR, Security, Routing, RSU, SAODV, Attacker.

1. INTRODUCTION

VANETs (Vehicular Ad Hoc Networks) are a special and an important type of MANETs. These networks offer communication between number of vehicles (Vehicle to Vehicle Communication) travelling on streets and between vehicles and infrastructure (Vehicle to Infrastructure Communication). VANET architecture [1] mainly consists of roads, streets, vehicles, road Side Units (RSU), Certification Authority (CA), etc. RSU acts as a router which is used for storing information and computation. It is installed with sensors to trace the vehicles speed and broadcasting messages. CA is the Certification Authority which gives certificate to the vehicles by signing with its private key. The certificate shows the levels of trust on that vehicle by CA. The attackers [2] like Blackhole, Wormhole first identified as suspicious then confirm as attacker due to presence of active malicious action. Vehicles are installed with Global Positioning System (GPS) by which the vehicle knows its own position as well as it can trace the positions of other vehicles. It is also installed with an On Board Unit for wireless communication. Further it is installed with Electronic License Plate (ELP) by which one can get the unique number of a vehicle. The main purpose behind VANETs is delivering more safety to the drivers in the roads. Different types of information will be sent via VANETs i.e. traffic signal violation warning, curve speed warning, pre-crash sensing, traffic jam warning and many more. Since mobility is the main feature of VANETs, then any corresponding simulation model should consider the effects of mobility, different mobility patterns, and of course apply an appropriate mobility model that presents different aspects of the movement experienced [3]. Furthermore, the concept of mobility should be understood when dealing with mobility models as it is categorized into macro and micro mobility. Macro mobility describes and deals with motion constraints such as road topology, street characteristics, traffic lights and signs, nodes flow, density and distribution, i.e. any street elements that may limit or affect mobility. On the other hand, micro mobility defines the movement of individual vehicles and its behavior with nearby vehicles, i.e. car-2-car interaction and car-to-street interaction such as overtaking and acceleration/deceleration [3]. The security is also major concern from number of attackers in presence in VANET. The one of them is blackhole attacker. The proposed SDSR is securing the network from attacker and removes the attacker presence. Koucheryavy [4] have categorized VANETs into safety-related and comfort-related applications. Such applications are significant for the following reasons. Safety related applications are important as they related directly to the driver’s safety on the road. An example of this kind of application is an emergency notification system such as a braking alarm that provides drivers with warning-related information. In December, 2003, the US FCC has allocated 75 MHz of spectrum in the 5.9 GHz band for a variety of Dedicated Short Range Communications (DSRC) to improve highway safety and efficiency [5].

2. VANET CHARACTERICTICS

All Compared with other types of MANET, VANET have the following unique characteristics. These characteristics are critical in the study of security, privacy, and trust management in VANET as we will show in the following sections[6].

2.1.1 Mobility

Vehicles in VANETs are normally moving at high speed. Therefore, a little delay in V2V communication.

2.1.2 Dynamic Network Topology

The topology of VANETs changes quickly due to high mobility of the vehicles. This makes the VANETs vulnerable to attacks and it is difficult to identify malicious vehicles.

2.1.3 Real-time Constraints

The transmission of information in VANETs has a particular time limit range. This is designed to give the receiver sufficient time to make decisions and take corresponding actions promptly.

2.1.4 Computing and Storage Capability

It is ordinary to process large amount of information among vehicles and infrastructures in VANETs. Thus, the computing and storage capability is absolutely a challenging issue.

2.1.5 Volatility

It is normal that the connections between two nodes in VANETs occur just once because of their mobility. The connections between nodes would remain for a limited period of time within a few wireless hops. Thus, it would be difficult to ensure the security of personal contacts in VANET.

3. ROUTING IN VANET

In MANET currently, there are mainly two types of routing protocols in MANETs, namely, topological routing and geographic routing [7, 8, 9]. In topological routing, mobile nodes utilize topological information to construct routing tables or search routes directly. In geographic routing, each node knows its own position and makes routing decisions based on the position of the destination and the positions of its local neighbors.

The investigation of topological routing has lasted for decades, and a variety of topological routing protocols have been developed. Generally, the topological routing protocols can be further divided into two categories, namely, proactive routing and reactive routing. In proactive routing, route information is propagated periodically in the network.

Thus, each node can maintain a routing table containing route entries to other nodes. When packets arrive at an intermediate node, the next hop can be selected by looking up the routing table. Destination-sequenced distance-vector (DSDV) routing is referred to as a well-known example of proactive routing. In reactive routing, no routing table is maintained at the nodes. When needed, the source node triggers a route search procedure to discover the routing path to the destination. Both ad hoc on-demand distance vector (AODV) routing and dynamic source routing (DSR) are referred to as representative examples of reactive routing. By exploiting the strength and avoiding the weakness of each type, hybrid topological routing protocols are proposed, for example, Zone Routing Protocol (ZRP), which maintains a k-hop routing zone proactively and triggers the inter-zone route discovery reactively.

4. LITERATURE SURVEY

In this section we presents the previous research of different authors that are work on security in VANET.

In this paper [10], they discuss the secure scheme in VANET which can help the network to maintain a reliable secure connectivity among nodes (vehicles) and its significant role of routing protocol and attacks for vehicular ad hoc networks. The important aspect of VANET is computation and control to improve safety, security comfort of everybody life by reducing accidents, congestion control, fuel in traveling. When a node receives an AODV control message, either to create or to update a route for a particular destination, it searches its routing table for an entry to the destination. If there is no route entry, it creates a new one with the sequence number contained in the control packet, or else the sequence number is set invalid. Draw backs on this research are:-

1. Throughput and Packet dropping metrics are only mentioned but their performance is not evaluated .
2. The number of vehicles sending connection establishment packets for establish connection between leading vehicles is not mentioned.
3. The quantity of receiving packets are not mentioned
4. The security scheme is based on packets delivery i.e. 0 or 1. if the packets receive it means 1 but drop it means 0 but how sure the packets are drop due to attacker**.**

In this paper [11], the conviction calculation is based on position of vehicle. Sender vehicle broadcasts its route request message (RREQ) for finding the secure location within the communication range in the network. Sender vehicle receives the route reply message (RREP) from various vehicles then source vehicle computes ratio of vehicles to find out that weather a particular location is trusted or not.

In this paper [12], they have understood a VANET in which nearby vehicles can communicate into the same direction only and with those vehicles which are available within the network range. Geographical positioning and timing related conditions are fulfilled with global positioning services receivers.

In this paper [13], they consider the security against DoS attacks. Actually the mobile vehicles or nodes in VANET share a wireless medium as well a radio signal can be pretentious, causing the service to be corrupted. There are a collection of different attack strategies that an attacker can carry out in order to obstruct. For each intermediate node the value of the PDR (Packet Delivery Ratio) is intended in different time instant.

In this work [14] we look at the connectivity of vehicular adhoc networks in urban situations. We collect realistic mobility traces from operational taxies during May in 2010 in Beijing and utilize the mobility data collected in Shanghai in February of 2007 from the SG project. By analyzing the large volume of trace data, we surprisingly find that the vehicle isolation probability between taxies follows an exponential distribution other than the results stated in former works.

In this paper [15] the author is mainly concentrates on the hole generation attack, in which the malicious or attacker drivers inside the network breaks the links by reducing their own speed or boosting their speed to create holes. Proposed a novel Robust Routing Protocol (RRP) for sending the message securely in between source to destination by surviving it from hole generation attack.

5. PROPOSED APPROACH

It has been observed that although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and efficient routing security. There are limitations on all solutions. They may be of high computational or communication overhead The proposed security scheme against hole attack through RSU unit collect and analyze audit data for the entire network. So according to that above definition we conclude VANET is distributed nature and can’t trust to any of the mobile devices because we cannot manage the every time of topology changes on the network. This is very big challenge. So that particular point we create the trust based routing against the malicious attack in VANET.

A. Proposed Algorithm

```
Input:
    $V_n$: n vehicles in network
    $T_m$: m traffic monitoring system
    $RSU_i$: no of i road side unit
    $B_l$: black hole attack
    $M_r$: monitoring & preventer node $\forall$ $RSU_i$
    $S_i$: message sender $\forall$ $V_n$
    $R_k$: message receiver $\forall$ $V_n$
    $I_l$: intermediate vehicle $\forall$ $V_n$
    $R_{req}$: route request
    $R_{rep}$: route reply
    $h_{seq}$: higher sequence number
    $C_p$: capture packet
    $D_p$: drop packet
    $a_{bn}$: abnormal behavior ($h_{seq}$, $C_p$, $D_p$)
    $P_t$: DSR for routing
    $\gamma$ : $RSU_i$ control range
Output: Throughput, PDR, delay, location, Collision info, attack percentage
Method 1: Attack Detection/Behavior Monitoring
$T_m$ watch the activity of assigned route
$T_m \leftarrow RSU_m$
If $V_k$ receive $R_{req}$ & not forward to $V_{k+1}$ Then
    Watch $V_k$ activity by $T_m$ node
        If $V_k$ generate the fake $H_{seq}$ of $R_{req}$ Then
        $T_m$ trace $V_k$ $a_{bn}(h_{seq})$
            If match $a_{bn}(h_{seq})$ Then
                $V_k \leftarrow B_l$ set by $T_m$
                $T_m$ Send feedback to
$M_r$           module
            Else
            In real time watch $V_k$ by $T_m$
        End If
    End if
Else If $V_k$ receives message of $S_i$ & $V_k$ != R & not forward Then
    $T_m$ trace $V_k$ $a_{bn}(C_p, D_p)$
    $V_k$ create loop
    If match $a_{bn}(C_p, D_p)$ Then
        $V_k \leftarrow B_l$ set by $T_m$
        $T_m$ Send feedback to $M_r$ module
    Else
        In real time watch $V_k$ by $T_m$
    End If
End If
Method 2: Attack Prevention
 $M_r$ take response from $T_m$
$M_r$ re-analysis the activity of $B_l$
    $M_r \leftarrow RSU_m$
If $V_k$ as $B_l$ Then
    $M_r$ check $S_i$ to $V_k$ Hop count , $C_p$, $D_p$, $H_{seq}$ field
    If $V_k$ as $a_{bn}(h_{seq}, C_p, D_p)$ & hop count = = $\infty$ Then
        $M_r$ take confirmation $V_k$ as $B_l$ Block $V_k$
        Send negative response of $V_k$ to all $V_{n-1}$
        $S_i$ call forward DSR($S_i$, $R_k$, $R_{req}$)
        $RSU_i$ provide safe route to $S_i$ $\nexists$ $V_k$
        $RSU_i$ communicate with $V_n$ or $RSU_j$
        $RSU_i$ synchronize $V_n$ in respective zone
        Avoid congestion through $T_m$ module
    End If
End If
```

Here the Blackhole attacker is create the gaps of information delivery' in between vehicles by that the vehicles speed are slowed and the infection is affected the performance of normal vehicles. The proposed scheme is applied with V to RSU communication for maintaining the security and forwarded the attacker vehicle information to all rest RSU and their surrounding vehicles. The proposed prevention scheme is block the attacker malicious activities and provides secure communication in VANET.

6. RESULT ANALYSIS

The performance of proposed security scheme with DSR routing protocol is measured with previous SAODV and Blackhole AODV(BAODV). The number of nodes scenarios is same in all modules. The performance of proposed security scheme is showing the better performance.

6.1 Throughput Performance Analysis

In Vehicular networks, throughput or network throughput is the successful message delivery over a communication channel up to destination vehicle. This data may be delivered over a physical or logical link, or pass through a certain vehicle in the network. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. In this graph we compare the throughput performance of Blackhole AODV (BAODV), Secure AODV (SAODV) and proposed Secure DSR (DSR). If malicious vehicle come into network and transmit data then in that case result will be degradable but if we apply SDSR scheme on attack so again throughput performance is better. The throughput at the time of black hole node in the network is minimum in all node density scenarios, that decrease the performance. The performance of SAODV is recovers the network performance but proposed scheme is also improves performance.

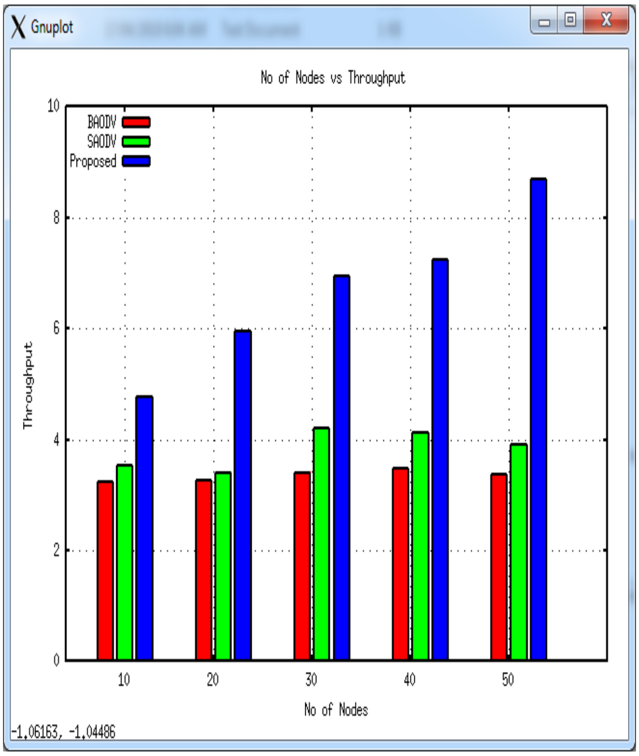

Fig.1 Throughput Analysis

6.2 Packet Drop Performance Analysis

The number of traffic status packets are drop in network because of attacker misbehavior. The routing protocol existence is also important in VANET and the vehicles are continuously sends and receive traffic data in network for better driving facility on roads. In this graph only data drop in presence of BAODV, SAODV and SDSR is evaluated. Here the assailant presence is drop about 22500 packets of data in network of total data of traffic is receives in network. This data is drop due to vehicles are busy in retransmitting the request due to attacker misbehavior by that data packets are dropped. But after applying secure SDR communication, the security criteria is enhanced for reliable communication and data drop is reduced as compare to previous security SAODV scheme also. The more data dropping is shows in 40 and 50 nodes scenario.

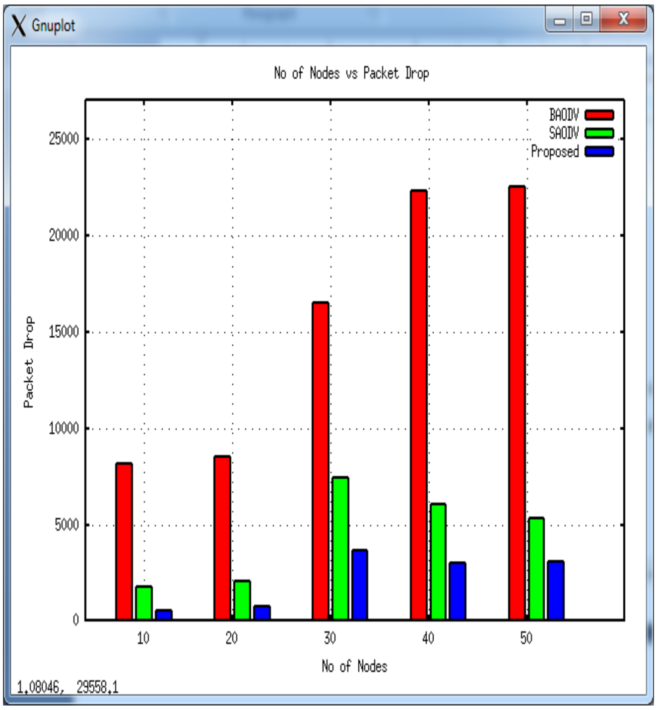

Fig.2 Packet Drop Analysis

6.3 PDR Performance Analysis

The proper communication is necessary in network but it is very important in real time traffic system. The vehicles wrong information is misguides the trailing vehicles and because of that the road traffic is In VANET only short information (about traffic status and something un-happened on roads like accidents) are deliver to nearby vehicles. In this graph the PDR performance of BAODV, SAODV proposed SDSR communication is assessed and observe that the proposed scheme is really effective to identified the Blackhole assailant presence. The PDR performance as compare to SAODV is better and provides 97% successful delivery at destination. The attacker performance in network not more than 18% because most of the data are dropped in network e.g. is also the enhance NRL (Normal Routing Load) and end to end delay (NRL and end to end delay always minimum better). The attacker existence is absolutely blocked by proposed security for providing secure communication between vehicles.

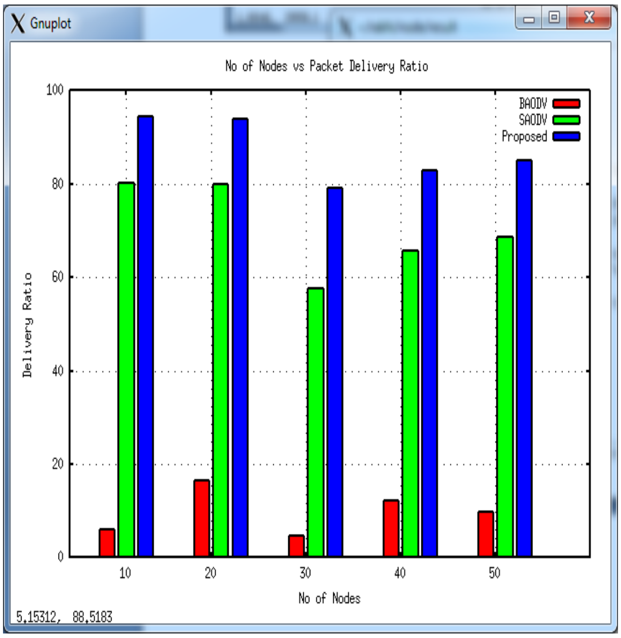

Fig.3 PDR Analysis

6.4 Packet Receiving Performance Analysis

The communication is VANET complete the request of sender vehicles and maintain the traffic in roads. In this graph BAODV data receiving is negligible as compare to SADV and SDSR. that means black hole attack case data loss is maximum and if we apply proposed SDSR with data receiving is high, that shows in all node density scenarios. That shows receiving in case of malicious nodes is really insignificant in between source to destination that conclude network under the infection. The attacker vehicle consumes the data packets in network and decrease the actual performance of the network but in proposed scheme performance is increases means that shows better receiving as compare to SAODV.

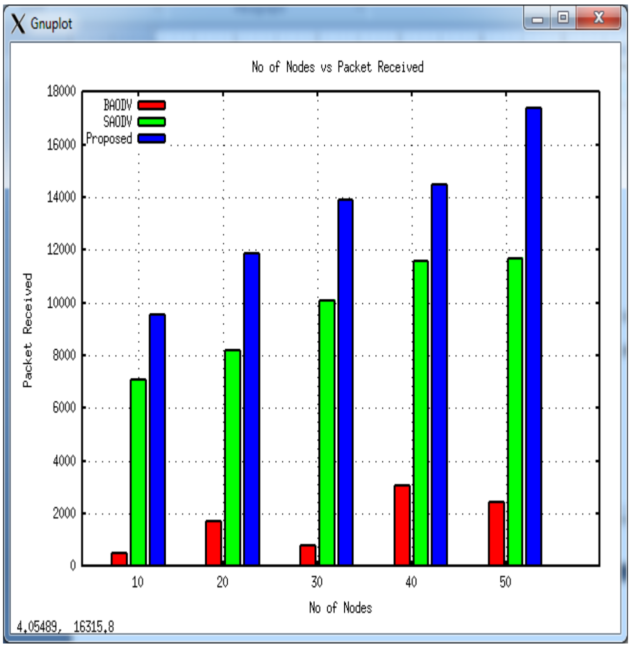

Fig.4 Packets Receiving Analysis

6.5 Delay Performance Analysis

The delay reason in road traffic is vehicles in road is more and the traffic status information is nor delivered to vehicles properly. The follower vehicles are continuously sends the traffic request for recognizes the traffic status. The vehicles are drive on that path according to the traffic information of beginning vehicles. Traffic information is also destructive if it will be deliver in network e.g. perform misbehave due to presence of by Blackhole attacker (BAODV). In this graph the delay performance is measured and observed that the delay performance of BAODV is always high in all node density scenarios . The delay enhancement is more in also SAODV but minimum in proposed SDSR scheme. The proposed security scheme against Blackhole attacker is secure the network performance and providing the request packets delivery as equal to normal VANET performance.

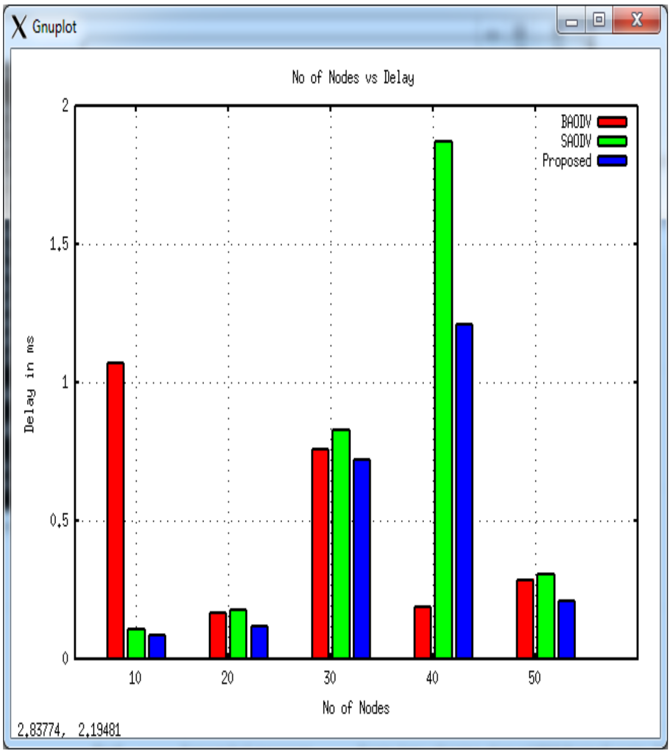

Fig.5 Delay Analysis

7. CONCLUSION AND FUTUREWORK

The RSU unit is observe the traffic status information sending by the vehicles in limited range to identified the further traffic status from leading vehicles. The RSU monitoring is detect the attacker presence and after that prevent it. In this paper a range of facet of VANET like its environment, standards and network architecture has been converse. In VANET for receiving and generating traffic request routing is perform an important part which used for more prominent and expedient communication. The security in VANET is improves the throughput and PDR. The improvement in packets receiving is also enhance the performance by reducing delay and overhead .While attack creates a more harsh condition, it is necessary to investigate the effect of attack on routing protocols which makes more protected vehicular environment. The proposed SDSR is reduces the packets dropping and due to attacker presence the dropping is completely cover-up and removes attacker infection from network.

The attacker presence in VANET is very effective to find out it by applying the location identification system or Global

Positioning Ssystem (GPS) to identified the malicious vehicle actual or current location. The location based scheme is also improves the more performance in term of delay and overhead.

8. REFERENCES

[1] Sourav Kumar Bhoi, Eabitra Mohan Khilar, "A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services", International conference on Communication and Signal Processing, April 3-5, 2013.

[2] Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J-L. bin Ab Manan. "Classes of Attacks in VANET." IEEE Saudi International Electronics, Communications and Photonics Conference (SIECPC), 2011, pp. 1-5, 2011.

[3] Sarah Madi, Hend Al-Qamzi, "A Survey on Realistic Mobility Models for Vehicular Ad Hoc Networks (VANETs)", IEEE 10th IEEE International Conference On Networking, Sensing And Control (ICNSC), 2013.

[4] Jakub Jakubiak and Yevgeni Koucheryavy, “State of the Art and Research Challengies for VANETs”, Proceedings of the 5th annual IEEE CCNC, pp.912-916, 2008.\

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

[6] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, “VANET Security Surveys,” Computer Communication, Vol. 44, pp. 1–13, May 2014.

[7] Anas Abu Taleb, "VANET Routing Protocols and Architectures: An Overview", Journal of Computer Science, 2018.

[8] Duduku, V., V.A. Chekima, F. Wong and J.A. Dargham, "A Survey on Routing Protocols in Vehicular Ad Hoc Networks", International Journal Innovative Research of Computer Communication Engineering, pp.12071-12079, 2015.

[9] Jair Jose Ferronato, Marco Antonio, Sandini Trentin, "Analysis of Routing Protocols OLSR, AODV and ZRP in Real Urban Vehicular Scenario with Density Variation", IEEE Latin America Transactions Volume: 15 , Issue: 9, pp.1727 - 1734, 2017.

[10] A.P. Jadhao, Dr.D.N.Chaudhari, "Security Aware Routing Scheme In Vehicular Adhoc Network", IEEE Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018), 2018.

[11] Kumud Dixit Priya Pathak Sandeep Gupta, "A New Technique for Trust Computation and Routing in VANET", IEEE, 2016.

[12] Trupil Limbasiya, Debasis Das, "Secure Message Transmission Algorithm for Vehicle to Vehicle (V2V) Communication", IEEE, 2016.

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

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

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

[16] https://www.isi.edu/nsnam/ns/