Vehicular Ad-hoc Network (VANET): Review

Muhammad Rizwan Ghori, Kamal Z. Zamli, Nik Quosthoni, Muhammad Hisyam, Mohamed Montaser
Faculty of Computer Systems and Software Engineering,
University of Malaysia Pahang,
Gambang Campus, Kuantan, Malaysia

***Abstract*—Wireless technology is advancing rapidly with time. People are doing research nowadays mostly in the field of telecommunication. VANET is the most growing research area in wireless communication. With the advancement and maturity of the VANET, there will be a great revolution in the field of wireless communication in terms of fast handovers, network availability, security, safety with the use of advanced applications etc. VANET technology is advancing with the passage of time but there are many issues that has to be addressed to make the network more vigorous. In view of aforesaid, in this paper we have studied and discussed various research works related to the applications, protocols and security in VANET. Moreover, after reviewing the existing works, we have analyzed them and found the pros and cons for the future research.**

***Index Terms*—VANET, Applications, Security, Protocols**

I. Introduction

Vehicular Ad-hoc Network (VANET) has become one of the most important research area in the field of wireless communication. Before going into the details of VANET it is necessary to discuss its historical background. As shown in Fig. 1, WANET is the parent field of all the ad hoc networks. VANET is a sibling of MANET which organizes its communication system itself without any dependency on any other infrastructure. The most common use of MANET is in military because of its easy and basic communication method just like a data sharing between various computers. VANET is similar to MANET along with some alterations. VANET comprises of the mobile nodes (MN), road side units (RSU) (Yong et al. 2016). Mobile nodes are the sensors embedded in the vehicles that are called as on board units (OBU) for the signal processing (data sharing) to and from RSUs. RSUs are fixed installed units that are the gateway for the communication between MN and the servers or internet. There are a lot of services provided by VANET but the most important among all is the road safety services for the reduction of road accidents by data sharing through internet.

There are two sorts of communication in VANET that is Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) (Lu et al. 2012). The Fig. 2 is depicting the aforesaid scenarios.

II. VANET Applications

Over the years there has been many researches on developing applications and usage models for VANET type of communication. As more people spend time on the road, hence, more requirement of internet connection to communicate with each other, to receive real time news, traffic information and weather reports etc. Moreover, some of the latest applications developed related to VANET are online file sharing, real time video updates and entertainment via connection to the internet through RSUs or V2V type of connections. Moreover, the VANET applications are categorized as safety and comfort

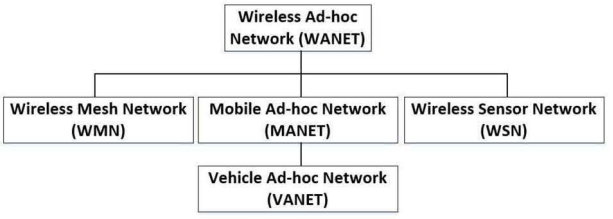

Fig. 1. Classification of Ad-hoc Networks

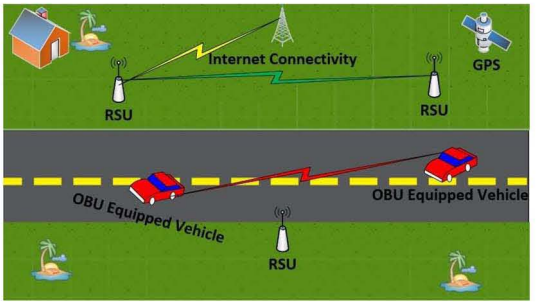

Fig. 2. VANET Communication System

Table 1. VANET Safety Applications

Name	Description
Traffic signal violation	Send alert to vehicles associated to dangerous situation
Intersection collision warning	Send information about the road intersection points
Turn assistance	Assist the driver in turning of vehicle
Blind spot warning	Alert the presence of another vehicle in the blind spot
Pedestrian crossing information	Send information of pedestrian crossing in the path
Lane change warning	Ensue that the intended lane is clear for entry
Forward collision warning	Alert the driver of a slower car in front
Do not pass warning	Alert the driver about overtaking safety
Post-crash	Alert of a crash that has happen
Emergency service vehicle	Provide clear path for emergency vehicle like ambulance
Curve speed	Warns vehicle about road curves ahead
Wrong way	Alerts a vehicle of the wrong way movement
Work zone	Alert of work zone area up ahead

978-1-5386-5696-9/18/$31.00 ©2018 IEEE

applications (Hassan et al. 2016).

A. Safety Applications

These applications aim to save human lives on the road. The aim of these applications is to deliver the safety related information to the required receiver in time to avoid any accident. The safety related applications are shown in Table 1 and some are described as follows.

1) Information Messages (IM): IMs consist of work zone messages while driving on the highway, toll collection point and speed limit messages etc.

2) Assistance Messages (AM): This is the kind of information which will assist the driver during the journey. AM includes the messages related to the lane switching, cooperative collision avoidance (CCA) and navigation. CCA message considered to be the most critical in terms of helping the driver by warning him or her to reduce the speed for avoiding any uncertain condition.

3) Warning Messages (WM): WMs include information like traffic signal a head, toll point or any bad road condition warnings.

B. Comfort Applications

The main objective of these applications is to give passenger/driver comfort and traffic efficiency. Moreover, aforesaid applications can be called as value added services. These applications include an automatic toll collection, site based services like location of shopping malls, restuarants etc. and internet connectivity facility. Some of the applications related to the comfort of the users are shown in Table 2,3 and 4.

III. Security in VANET

In VANET communication security is the main concern. The reason of more security issues in ad-hoc network as compared to the other wireless communication is because of rapid change of topology, small sized devices etc. Due to dynamic nature of the topology, it is difficult to maintain security as there is no pre-existing infrastructure for ad-hoc networks like the cellular framework etc. that can control the security of the network. Like all other computing systems, VANET also have the same data security issues like integrity, confidentiality, authenticity, and availability (La and Cavalli 2014).

Table 2. Travelling Comfort Applications

Applications	Description
Service announcement	Provide information about the restaurant and other rest areas during the journey
Remote diagnostic	Provision of connectivity between the vehicle and vehicle maker or workshop for the remote diagnosis
Entertainment	User can watch real time audio and video in the vehicle
Remote passenger health update	Application for use in an ambulance via wireless body sensor network (WBSN). Patient health information can be transferred directly from the ambulance to the hospital for correct diagnosis

Table 3. Efficient Travelling Applications

Applications	Description
Map download	Provide facility to download map for routing
Navigations	Provision of navigation application to find the route related to any destination

A. Data Confidentiality in VANET

Confidentiality can be called as the privacy. It is basically to prevent the sensitive information from reaching the wrong person. According to Azees et al (2016), there are many threats on data confidentiality of VANET which are discussed as follows.

1) Man in the Middle Attack: Malicious vehicle can come in between the V2V or V2I communication and can give false information to the communicating parties for getting control over the network. But on the same time genuine interacting cars will think that they are communicating with themselves without getting any false alarm.

2) Social Attack: This is the sort of attack in which the hacker transfers an immoral messages to the vehicle driver to irritate him or her. The ultimate goal of the attacker is to force the driver to respond to that message in an annoying way so that the driving quality of the vehicle in VANET gets effected.

3) Traffic Analysis Attack: The said attack is called as a passive attack. With the result of this attack, an attacker can come in between the communication and gets the information for personal purposes.

4) Eavesdrop Attack: Eavesdropping is the attack on the VANET against the confidentiality in order to get the unauthorized access to get the confidential data. Insider or outsider malicious users can save the information of the road end users and can take advantage from the particulars of the users while they are unaware of the said data collection.

5) Illusion Attack: Illusion attack creates incorrect sensor reading or traffic information where an attacker node broadcast false messages in terms of alarm or warning of the traffic to the nearest neighbour nodes. This creates illusion situation for the traffic flows and number of vehicles. Drivers with normal behaviours will change their driving route according to the false illusion messages received and surely this situation will lead to more severe situation such as accidents.

There are some works done related to the confidentiality of data in VANET. Lu et al (2012) proposed a model for achieving confidentiality with the help of efficient management of key for location based services (LBS). LBS will not be available for the user if he or she does not join the VANET.

Table 4. Other Value Added Services

Applications	Description
Electronic toll collect	Vehicle communicates with the toll gate for payment process before the vehicle reaches the gate
Parking availability	Information about parking availability especially in major urban areas
Route Diversion	Helps in diverting the vehicle route in case of traffic jam or congestion for time saving

978-1-5386-5696-9/18/$31.00 ©2018 IEEE

As per the author, to achieve the confidentiality for LBS, the users of the vehicle shares a secure session keys for encryption of certain contents. Moreover, Karimireddy and Bakshi (2016) presented a model based on identity in which the confidential sort of data is encrypted with the help of symmetric and public key encryption techniques.

B. Data Authentication in VANET

Data Authenticity is to confirm the persons identity like it can be achieved with the help of user id and password etc. Authentication is the measurement to ensure that only a genuine user enter the system after passing through the identification process. Moreover, this process is considered to be the first layer of protection against the malicious users (Mishra et al. 2016). Some of the attacks related to authentication are discussed below.

1) GPS and Tunnelling attack: In VANET, there is a table maintained related to the information about the location of the vehicle with the geographic locations and identity by using Global Positioning System (GPS) satellite. For introducing the attack the malicious user practices the GPS simulator which generate more strong signals as compared to the original satellite signals to cheat the vehicles by misguiding them. Moreover, tunnelling attack is another attack related to GPS. Because of the temporary fading of the signal in the tunnel, the attacker can insert the wrong information related to the position of the vehicle before it exit the tunnel and gets legitimate positioning information (La and Cavalli 2014).

2) Replay Attack: In VANET, the users are uniquely identified by Internet Protocol (IP) and Media Access Control (MAC) address. However, these are insufficient estimation to stay away from the attackers as they can spoof the IP and MAC to get the identity of the genuine user to enter into the system and hide (Azees et al. 2016). After getting the identity the malicious user can send the message on behalf of the genuine user to create any chaos/traffic jam or any other activity for own benefits. The malicious desire can be achieved with the help of message alteration or replay. The said attack occurs when an attacker retransmit the previously transmitted information to take leverage of the message during the time of sending. By replaying the information, it will lead to illusion and false messages to create accident situation.

3) Sybil Attack: According to Sari et al (2015), it is a kind of attack where a hackers node will create its different identities in the form of multiple nodes. This fake node cheats neighbour nodes in the VANET by providing false alarm or information such as traffic jam and accidents. It also can create fabricated information in a form of additional number of vehicles on the road. This attack will effect the geological routing because one identity can exist in many locations. Thus, the integrity of the information can be compromised.

4) Masquerading Attack : Masquerading is like a physical attack on the network. As in VANET, nodes can easily go in and out from the network. Each node has its own MAC and IP address. Attackers can use these addresses for getting an identity of other nodes. Afterwards, the hacker node can broadcast messages on behalf of the real vehicle node to make the attack successful.

Table 5. Authentication in VANET (Comparative Study)

References	Paper	Comments
Wang et al. 2016	Two Factor Authentication	Secure Technique
Shao et al. 2016	Dynamic Threshold and Signature Authentication	Signature can be copied (Disadvantage)
Jiang et al. 2016	Anonymous Batch Authentication	No Authentication for CRLs (Disadvantage)
Xie et al. 2016	Bi-Linear Pairing IBS	Not secure for Sybil and Replay attacks
Vijayakumar et al. (2016)	Dual Key Management for Group Communication	Competitively Secure
Malik and Pangay (2016)	Enhanced IRE	Only Suitable for DOS attacks

5) Identity Disclosure Attack : Identity disclosure attack is made by the insider with passive and malicious appearance. It can keep watching on the targeted nodes and can use this attack to get the Identity of the nodes.

6) Worm Hole Attack: Worm hole attack is difficult to detect and prevent because the attacker nodes will create a tunnel between the end nodes and the malicious nodes. Packets are broadcasted to the network inside the tunnel. The dangerous situation is when the attacker nodes can use this position to do harm such as gaining unauthorized access, disturb routing, or perform DoS attack.

7) Related Works: Many researchers have put forward their effort for providing authentication in VANET. Wang et al. (2016) presented a model consisting of Certificate Authorities decentralization for reduction of its work load and two factor authentications by using biological password for assurance of the security. Moreover, Shao et al. (2016) proposed an authentication model for VANET based on the dynamic threshold and signature authentication of the signers. Another scheme was proposed by Jiang et al. (2016) with the help of anonymous batch authentication. In the said scheme, the authenticity and privacy is achieved without broadcasting the certificate revocation list (CRL) to every vehicle to reduce the overhead and to ensure the privacy. Xie et al. (2016) proposed another model for privacy preserving with the help of bilinear pairing for the construction of identity-based signature to ensure integrity and authentication. Vijayakumar et al. (2016) proposed a model of dual key management for group communication. In the said system, the author divided the communication in groups such as primary, secondary and unauthorized users. Primary users get the services from the controller while secondary users get them from primary users as they cannot communicate directly with the controller. Lo and Tsai (2016) presented privacy scheme with the help of algorithms for setting up a connection and verification of the users without using one way hash function and pairing operations. Subsequently, Malik and Panday (2016) proposed an enhanced version of intermediary re-encryption authentication (IRE) method to overcome the attacks faced by (IRE) like denial of service, eavesdropping etc. Additionally, cloud assisted privacy preserving authentication model was proposed by Rajput et al. (2016) consisted of a

978-1-5386-5696-9/18/$31.00 ©2018 IEEE

total of five phases such as vehicle enrolment, pseudonyms issuance, region credentials issuance, message broadcast and pseudonym resolution and revocation. Moreover, a comparitive study summary is shown in Table 5.

C. Data Availability in VANET

Availability can be defined as the system should always be available for the use. It can be best assured with timely hardware equipment maintenance and keeping up the system with upgrades to avoid any conflict. Some of the attacks on the availability in VANET are discussed as follows.

1) Denial of Service: According to Karimireddy and Bakshi (2016), the main objective of this attack is to prevent the genuine nodes from accessing the services and resources of the VANET. DoS will happen when an attacker joins the network and takes over the control of the vehicle resources or jam the communication between nodes and the road side unit (RSU). The attack occurs when a network is jammed and flooded, thus the connecting nodes or vehicles cannot access it.

2) Malware Attack: Malware attack is done by putting malware such as viruses and worms into the VANET and this surely can cause disturbance in its operations. Malware attack can be introduced by the insider rather then the outsider whenever the on board unit (OBU) and road side unit (RSU) are doing the patches or software updates.

3) Black Hole Attack: Black hole is an area in network where no node exist. Attack of black hole is possible with the attacker malicious move by introducing itself as a path to connect with other nodes in the VANET, thus it cheats the routing protocol. Because of the fake established route, the attacker nodes could hold the packets, drop them or forward to which ever node.

4) Spamming Attack: Spamming type of attack enables an attacker to send many spam messages in the network for excess bandwidth utilization. Moreover, the transmission latency will increase because of the existence of spam messages in VANET.

5) Related Works: An event driven congestion control algorithm was proposed by Shukla et al. (2016). The said program monitors the safety messages in the network and triggers the congestion control mechanism whenever any safety message will be detected. Moreover, after the detection, the algorithm will launch the method for freezing the queue for all the MAC transmissions apart from the safety messages queue. Another intrusion detection system was made by Alheeti et al. (2016) which used a feed forward neural network (FFNN) for the detection of black hole node or vehicle. Addtionally, compartive table summary is shown in Table 6.

Table 6. Availability in VANET (Comparative Study)

References	Paper	Comments
Shukla et al. 2016	Event Driven Congestion Control	Good approach used for Congestion Control
Alheeti et al. 2016	IDS by using FFNN	Only specific to Black Hole Attack (Disadvantage)

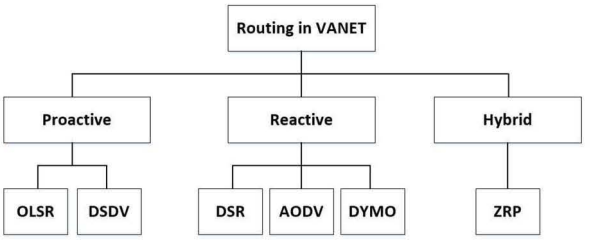

Fig. 3. Classification of Ad-hoc Routing Protocols

IV. VANET Routing Protocols

Routing Protocols describes a routing method for two routers/nodes in a computer network to communicate with each other. Moreover, routing algorithm is used to select the correct route for the packet. Among the challenges like security as discussed in previous sections, correct use of routing protocols as well is a great challenge for VANET. In VANET, the routing protocols are influenced by many factors like road and traffic condition, obstacles such as buildings etc. and many more environmental factors (Gupta and Chaba 2014). Other factors include the vehicle mobility and network disturbances etc. Adhoc routing protocols are divided into three main groups as shown in Fig. 3.

A. Proactive Routing Protocols

These protocols uses the destination sequence distance vector (DSDV) designed by using Bellman Ford Algorithm. With this algorithm, all the nodes keeps the information related to the next node. It means all the nodes in DSDV constantly maintain the information related to the other nodes to ensure that there is no interruption in the path. Example of these protocols is DSDV and optimized link state (OLSR).

1) Optimized Link State Protocol (OLSR): It is basically a refined version of link state protocol. The working of link state protocol is such that any change in a topology will be broadcasted to all the nodes in a network which will increase the network overhead. OLSR handles with two kinds of messages like hello and a message to control the topology.

Hello messages are used to find the data about the connection status. While topology control message is used to broadcast its own neighbour information with the help of multi point relay (MPR) selected list. Because of the use of MPR, the overload has reduced as it was in the case of pure link state protocol.

2) Destination Sequenced Distance Vector Protocol (DSDV): This protocol is a modification of Bellman Ford Algorithm. This algorithm resolved the problem of looping in routing by maintaining the sequence number information of each node.

B. Reactive Routing Protocols

This type of protocols do not possess the information about all the nodes (Zhang and Sun 2016). It only keeps the

978-1-5386-5696-9/18/$31.00 ©2018 IEEE

information of the nodes that comes in the route. The example of reactive protocol is DSR and AODV.

1) Dynamic Source Routing (DSR) Protocol: DSR is a productive protocol for routing. It is basically made for multi-hop WANET. It is a self-organizing and configuring protocol that does not require any administration. The two-main function of the said protocol is route discovery and maintenance. The said functions work with each other for node discovery and route maintenance.

2) Ad-hoc On-Demand Distance Vector (AODV) Protocol: As it is also an on-demand routing protocol. Methodology behind the AODV is that the nodes will transmit the information related to the topology only on demand. Each node in a network acts like a router which gets the route information whenever there is a need to send data (Sallam and Mahmoud 2015).

3) Dynamic MANET On Demand (DYMO) Protocol: DYMO is another on demand protocol designed after AODV. DYMO routing prtocol can be implemented as pro active as well as reactive (Spaho et al. 2012) . Moreover, route discovery methodology is on demand when ever required.

C. Hybrid Routing Protocol

Hybrid is a composite of proactive and reactive routing protocols which reduced the overhead and delays occurrence due to the periodic sharing of topology information (Jain and Jeyakumar 2016). With the hybrid approach, the efficiency and scalability feature of network has improved. On the other hand, the drawback of hybrid approach is high latency for navigating new routes. The common protocol based on hybrid approach is Zone Routing Protocol (ZRP).

D. Comparitive Study

For this paper, after reviewing many studies related to the routing protocols in VANET, we have come out with a comparitive study as shown in Table 7. According to the study, AODV protocol proven to be the best for VANET in which the movement of nodes is quite fast.

Table 7. Summary of Comparative Study

References	Protocols	Performance Results
Sallam and Mahmoud 2015	AODV and OLSR	AODV is better in more dense and high mobility area
Kaur and Malhotra 2015	AODV, OLSR and ZRP	ZRP proved to be the best in terms of node density and packet sizes
Zhang and Sun 2015	AODV and DSR	AODV performance is better with high mobility nodes then DSR
Gupta and Chaba 2014	AODV, DSR, OLSR and DSDV	AODV is among the best with high mobility nodes
Spaho and Ikeda 2012	DSDV and DYMO	DYMO has better performance than DSDV
Prokop 2011	AODV, DSR and DYMO	DYMO proven best AODV can be used as second choice

V. Conclusion

In this paper, we have reviewed several research papers related to VANET applications, security and routing protocols. VANET is lagging behind in terms of security. Many researchers worked for the provision of authentication to VANET. But, not much work is done related to the confidentiality and availability. So, there is a requirement to have more work related to the VANET security as it has become the main requirement of users. Moreover, related to routing protocols, many researchers have studied this issue thoroughly and proven that AODV is the most suited protocol for the VANET.

References

[1] **Alheeti et al.** (2015), *On the detection of grey hole and rushing attacks in self-driving vehicular networks*, in Proc. of 7th Computer Science and Electronic Engineering Conference (CEEC), pp. 231-236.

[2] **Azees, M.**, Vijayakumar, P. and Deborah, J. (2016), *Comprehensive survey on security services in vehicular ad-hoc networks*, in Proc. of International Journal of IET Intelligent Transport Systems, vol. 10, pp. 379-388.

[3] **Gupta, P.** and Chaba, Y., (2014), *Performance Analysis of Routing-Protocols in Vehicular Ad Hoc Networks for Cbr Applications Over Udp Connections*, in Proc. of International Journal Of Engineering And Computer Science, vol. 3, pp. 6418-6421.

[4] **Hassan, A.S.A.**, Hossain, M.S and Atiquzzaman, M. (2016). *Security Threats in Vehicular Ad Hoc Networks*, in Proc. of International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 404-411.

[5] **Jain, J.** and Jeyakumar, A. (2016), *An RSU Based Approach : A solution to overcome major issues of Routing in VANET*, in Proc. of International Conference on Communication and Signal Processing (ICCSP), pp. 1265-1269.

[6] **Jiang, S.**, Zhu, X. and Wang, L. (2016), *An Efficient Anonymous Batch Authentication Scheme Based on HMAC for VANETs*, in Proc. of EEE Transactions on Intelligent Transportation Systems, vol. 17, pp. 2193-2204.

[7] **Karimireddy, T.** and Bakshi, A. (2016), *A Hybrid Security Framework for the Vehicular Communications in VANET*, in Proc. of International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1929-1934.

[8] **Kaur, A.** and Malhotra, J. (2015), *On The Selection of Qos Provisioned Routing Protocol Through Realistic Channel for VANET*, in Proc. of International Journal of Scientific and Technology Research, vol. 4, issue. 07.

[9] **Lo, N.W.** and Tsai, J.L. (2016), *An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor NetworksWithout Pairings*, in Proc. of IEEE Transactions on Vehicular Technology, vol. 17, pp. 1319-1328.

[10] **Lu, R.**, Lin, X., Liang, X. and Sheen, X. (2012), *A Dynamic Privacy-Preserving Key Management Scheme for Location-Based Services in VANETs*, in Proc. of IEEE Transactions on Intelligent Transportation Systems, vol. 13, pp. 127-139.

[11] **La, V.H.** and Cavalli, A. (2014), *Security Attacks and Solutions in VANET: A Survey*, in Proc. of International Journal on AdHoc Networking Systems (IJANS), vol. 4, no. 2.

[12] **Malik, A.** and Panday, B. (2016), *Performance analysis of enhanced authentication scheme using re-key in VANET*, in Proc. of 6th International Conference - Cloud System and Big Data Engineering (Confluence), pp. 591-596.

[13] **Mishra, R.**, Singh, A. and Kumar, R. (2016), *VANET Security : Issues , Challenges and Solutions*, in Proc. of International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 1050-1055.

[14] **Prokop, M.** (2011), *Routing Protocol Evaluation Development of a Fully Functional Simulation Environment for Vehicular Ad Hoc Networks*, Msc. Thesis, Rochester Institute of Technology Kate Gleason College of Engineering, Newyork, USA.

[15] **Rajput, U.**, Abbas, F., Wang, J., Eun, H. and Oh, H. (2016), *CACPPA: A Cloud-Assisted Conditional Privacy Preserving Authentication Protocol for VANET*, in Proc. of 16th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, pp. 434-442.

978-1-5386-5696-9/18/$31.00 ©2018 IEEE

[16] **Sallam, G.** and Mahmoud, A. (2015), *Performance Evaluation of OLSR and AODV in VANET Cloud Computing Using Fading Model with SUMO and NS3*, in Proc. of International Conference on Cloud Computing (ICCC), pp. 1-5.

[17] **Sari, A.**, Onursal, O. and Akkaya, M. (2015), *Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)*, in Proc. of International Journal of Communications, Network and System Sciences, pp. 552-566.

[18] **Shakyawar, K.** and Tiwari, S.K. (2016), *Throughput And Packet Delay Analysis For Improvements In VANET*, in Proc. of International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 4070-4073.

[19] **Shao, J.**, Lin, X., Lu, R. and Zuo, C. (2014), *How to Ensure the Availability of Communication Channel for Event Driven Message in VANET*, in Proc. of Fourth International Conference on Communication Systems and Network Technologies, pp. 331-335.

[20] **Shukla, K.**, Jha, C.K. and Shukla, A. (2015), *On The Selection of Qos Provisioned Routing Protocol Through Realistic Channel for VANET*, in Proc. of International Journal of Scientific and Technology Research, vol. 4, issue. 07.

[21] **Spaho, E.**, Ikeda, M., Barolli, F., Xhafa, F., Younas, M and Takizawa, M. (2013), *Performance Evaluation of OLSR and AODV Protocols in a VANET*, in Proc. of IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), pp. 577-582.

[22] **Spaho, E.**, Ikeda, M., Barolli, F., Xhafa, F., Biberaj, A. and lwashige, J. (2012), *Performance Comparison of DSDV and DYMO Protocols for Vehicular Ad Hoc Networks*, in Proc. of IEEE 26th International Conference on Advanced Information Networking and Applications, pp. 629-634.

[23] **Vijayakumar, P.**, Azees, M. and Deborah, J. (2016), *Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks*, in Proc. of International Journal of IET Intelligent Transport Systems, vol. 17, pp. 1015-1028.

[24] **Wang et al.** (2016), *2FLIP A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET*, in Proc. of IEEE Transactions on Vehicular Technology, vol. 65, pp. 896-911.

[25] **Yong, X.**, Libing, W.U., Yubo, Z. and Jian, S. (2016), *Efficient and Secure Authentication Scheme with Conditional Privacy-Preserving for VANETs*, in Proc. of Chinese Journal Electronics, vol. 25, Issue. 5.

[26] **Zhang, J.** and Sun, Z. (2016), *Assessing multi-hop performance of reactive routing protocols in wireless sensor networks*, in Proc. of IEEE International Conference on Communication Software and Networks (ICCSN), pp. 444-449.

978-1-5386-5696-9/18/$31.00 ©2018 IEEE