Volume: 5, Issue: 3
Page: 83-91
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

Software Defined Network Based VANET

Glena Aziz & Shavan Askar

Abstract:
As the number of cars is growing, there is also a rapid growth in the number of road side accident. Much of these incidents have occurred by an error made by a driver. New protocols and architecture are rapidly being created for intelligent transport networks by researchers all over the world. To guarantee passengers' safety, several companies are now encouraging an ad hoc vehicular network (VANET). In another side, before practically adopting VANET technology, there are many concerns related to this field that need to be discussed. A number of attacks can occur in the event of no or weak protection, which can be affected by the performance and reliability of the process. In order to make VANET networks more successful, it implements software defined networking (SDN) technology. This technique was briefly called SDN-VANET. The SDN in VANET framework enables us to prevent from the limitations and complexities of basic VANET structures. Through handling the whole network from a single remote controller, it allows them to reduce the overall burden on the network. In this article we describe SDN-based VANET, its working, benefits, challenges and services, applications, and security attacks.

IJSB
Literature review
Accepted 1 February 2021
Published 3 February 2021
DOI: 10.5281/zenodo.4497640

Keywords: *Network Security, transport networks, VANET, software defined networking (SDN).*

About Author (s)

Glena Aziz Qadir Information System Engineering, Erbil Polytechnic University, Erbil, Iraq. Email: glena.mei20@epu.edu.iq.
Shavan Askar (Corresponding Author), Assistant Professor, Erbil Polytechnic University, Erbil, Iraq. Email: shavan.askar@epu.edu.iq.

1. Introduction

While travel modes change during the times, to improve their performance, new strategies and processes are added. At present, for driving, cars and other vehicles are used. When the car numbers grow, moreover, the percentage of road injuries become high as well. There are several causes for road crashes, such as driver negligence and technical defects in the car. Secure means of transport are needed in the modern world in order to avoid incidents that can cause significant harm to human lives. In order to solve these difficulties, the investigator researched the wireless network domain. Within the MANET technology, scientists have improved an area known as the ad hoc vehicular network. A VANET device can travel freely to any position, resulting in minor communication modifications. Nodes transmit information to other vehicles. To ensure the link and the suitable flow of knowledge, the equipment on the nodes must constantly transmit data. These machines are made up of a powerful machine that transfers proper information without waiting and can be linked to the web (Chadha, 2015). Any time, several nodes may be linked to one node that is a tool on the car. Communication, both components of VANET connect via wireless, that governs multiple methods of interaction, such as stability, latency and information transfer distance. In wireless networking, distinct protocols of routing are used. VANET's topology of the network is quick and extremely dynamic maximum speed of vehicles. Furthermore, VANET asks for higher network bandwidth (Saini, Alelaiwi, & Saddik, 2015).

The transmitting of accurate knowledge is now realized a critical effort because of signal interruptions, VANET connectivity opportunities, and the dramatic shifts in topology. In VANET, however, signal propagation is a crucial problem as the risk of disconnection increases as the Automobile alters its location. For Vehicular networks, dedicated short-range communication protocol is utilized in order to resolve the issue of disconnection between nodes. DSRC gives a fast transfer rate of data and is used in encryption applications. Vehicles can exchange protected information through this means of communication to avoid any mishap as well as post-accident inquiry (Chahal et al., 2017). VANET has drawn researchers to develop methods, software, and simulation tools in various fields. Researchers and entrepreneurs, however, are facing many challenges. Through creating new networking protocols, specialized hardware, data security, and privacy strategies, people from various countries are helping to get rid of these obstacles (Yousefi, Siadat, & Fathy, 2006). In the area of the VANET method, a Software Defined Network (SDN) methodology is implemented to improve the speed of the whole network (Xiaoqiong, Hongfang, & Kun, 2019). The content of the paper is arranged as follows: section one, background. Section two, SDN-based VANET. Section three, services of SDN-based VANET. Section four, the security attacks and challenges of SDN-based VANET. Section five, presents the applications of the SDN based VANET. Section six, presents literature review. And in the final section the paper is concluded (Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Keti & Askar, 2015). Chim et al.,(2016) improved an approach that discussed the security and privacy problems of V2V in vanets. This system uses a one-way hashing algorithm between the vehicle and the RSU and a hidden key. This approach may also overcome privacy issues that can happen through communications. Vighnesh et al., (2016) implemented a new sender authentication method, using hash chaining and authentication code to verify the car, to improve VANET security. This system guarantees encrypted contact between the automobile and the RSU, and a master key encrypts sensitive data. The RSU attaches its identity before sending packets to the authentication node, which will reduce the possibility of rogue rsus manipulating VANET.

Zhu (2019) proposed a technique that fixes the DOS attack issue against signature-based authentication. Reauthentication should be conducted before signature verification to tackle

DOS threats. The reauthentication process, which takes advantage of the use of a one-way hash chain and a rekeying method, is used in this scheme.

2. Background

2.1 What is VANET

The VANET is a part of the MANET that used for ensuring the safety of the passengers in contact with the car. Decision making is made possible by VANET. Transmission is carried out by a wireless network between multiple cars and RSU. This approach is used to express a high rate of expertise that offers data to travelers and improves road safety (Naik, Khan, & Mishra, 2018). The (CALM) architecture offers these facilities. It offers air interface paradigms for vehicle to infrastructure, vehicle to vehicle, and infrastructure to infrastructure. Many types of networking systems may be used for transmitting purposes, such as wimax, GSM, and DSRC (Ku et al., 2014).

2.1.1 On-Board Unit (OBU): The on-board device is attached to the vehicle and is used with other shells and RSUs for exchanging of information.

2.1.2 Application Unit. AU is installed in a vehicle containing a program or user interface that harnesses the communication abilities of the OBU. AU is connected with the OBU by a wireless or wired connection, which is always situated inside the same physical unit. As a private computer or as a remote personal assistant, AU can be used.

2.1.3 Roadside Unit: is a physical structure at the side of the road or the intersections that is forever fixed. To provide communication between cars, RSU devices are linked to an Internet source. The RSU can be prepared for one or more network equipment, depending on its functionality (Shrestha et al., 2018).

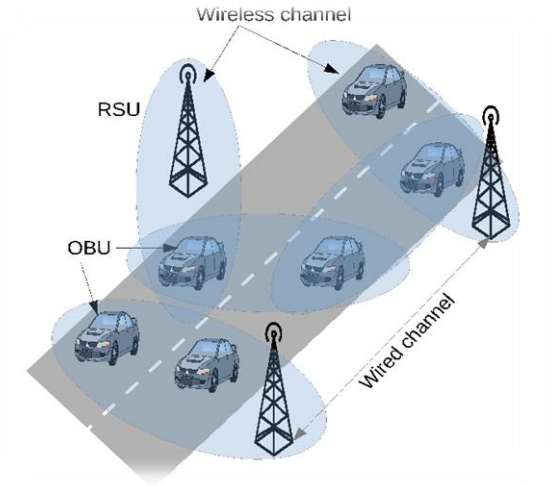

Figure2: architecture of VANET

2.2 What is SDN

SDN is described as a new technology for networks that can resolve the shortcomings of old conventional networks that have been used for several years (Benzekki et al., 2016). SDN is an approach to the architecture, implementation, and operation of networks separating the data plane from the control plane. Separation of the control plane from the data plane main features of SDN (Sezer et al., 2013).

2.2.1 SDN architecture

The general SDN architecture based on network planes and interactions between them. The SDN systems are separated into three planes. (Cabaj et al., 2014).

2.2.1.1 control plane

For monitoring and managing network services on the control plane, a centralized agent called a controller is used. The controller wants to improve total network efficiency by optimizing the use of network services (Jaballah, Conti, & Lal, 2020). The state of all SDN

switches is stored and monitored by the data obtained by each car, like position, speed and connection to the network. The acquired topological network data relies on the GPS. Such data may be used by a controller to identify the routing decision and then identify the most effective route for transmitting information packets and reaching the destination (Aladaileh et al., 2020).

2.2.1.2 data plane

The data plane is a network infrastructure used to relay data and is designed using elements of the network to provide communication. Network components include vehicles and rsus that include openflow (OF) switches. The cars are known to be the major components, while the stationary components are rsus. Diverse implementation policies are implemented by SDN switches. The vehicle note is sent to the SDN controller to boost the network configuration. The route, position, and speed are included in the full records of the vehicle. Such details will be placed in the OF flow table in the given RSU (Shafiq, Rehman, Kim, & Computing, 2018).

2.2.1.3 application plane

Service plane, which is the network facilities and software to third-parties. These SDN applications connect with the SDN controller via an application-control interface to articulate their specific protection, qos, or resource usage specifications (Nkenyereye et al., 2019; Shafiq et al., 2018).

2.2.1.4 Management plane

The management plane is responsible for activities beyond the monitoring, program, and data planes that are best managed. It should be segregated from consumers and hidden. The operations agency performs activities such as network initialization or configuration of specifications for the network. In order to deter some kind of network threats and to secure the entire network, it must not be configurable on the outside (Cabaj et al., 2014).

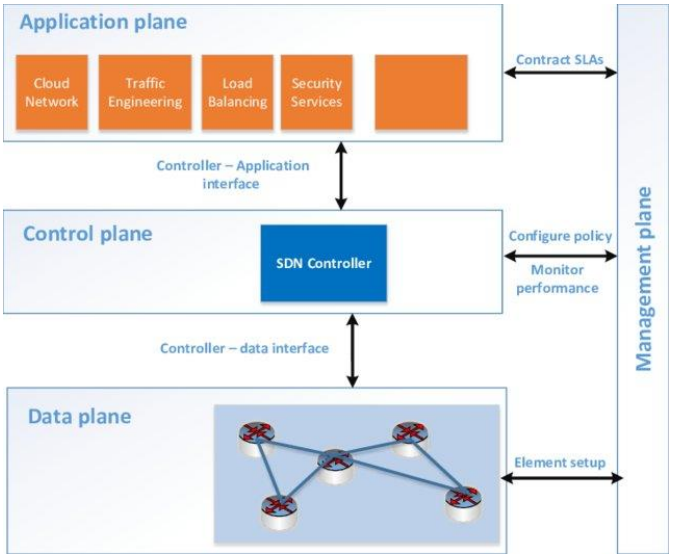

Figure1: SDN architecture overview

3. SDN in VANET

3.1 SDN in VANET benefits and services

3.1.1 Path selection

The interpretation of SDN allows the system to make more logical routing decisions. In VANET, data traffic is always unbalanced due to the shortest routing direction. Once the SDN controller senses this state, the data process can be diverted to maximize the utility of the network and reduce congestion. (Ku et al., 2014).

3.1.2 Channel and Frequency Determination

For data transmission, wireless networks at differing frequencies are needed. The SDN system makes it easy to establish an acceptable channel for the SDN controller to transfer data. Dynamically, the SDN controller defines the frequency that is most beneficial at a given time for data transmission. Using a particular frequency channel, emergency warnings are received by the (Yassine et al., 2020).

3.1.3 Power selection

SDN-based VANET would have the knowledge to decide if it is a reasonable choice to change the capability of wireless interfaces and therefore their range of communication. The SDN controller, for instance, collects neighboring wireless SDN node data and decides that the node density is too small and orders all nodes to maximize bandwidth to allow more rational transmission of packets and to minimize interruption (Ku et al., 2014).

3.1.4 VANET Security Service Supported by SDN

An example of the use of VANET technology is improving street safety. By comparison, the adoption of street security is close to the use of software-defined VANET to optimize management owing to the introduction of traditional strategies. With the reference point, SDN is then used to hold the farthest frequency point (Al-Heety et al., 2020).

3.1.5 DN-based On Demand VANET monitoring Service

An area where a SDN based VANET can be transmitted is the Emergency Vehicle Control Benefit. In traditional models, a monitoring warrant must be filed by a claimant. The SDN controller on an SDN-based system makes this appeal. Basically, to enter the requesting nodes, the SDN controller inserts flow rules for surveillance data. The SDN controller also adds guidelines for the same tracking content if there are a few requests, like when many police request for feeds for video monitoring, so that the same copy is sent to various receivers. (Hussein et al., 2014).

4. SDN Based VANET security and challenges

4.1 In SDN Based VANET Attackers

The system may be targeted by multiple types of hackers, including authorized network users, while external attackers are system intruders and therefore have little power to strike. Rational hackers target the device for personal benefit. Without any personal advantage, the purpose of cyber hackers is to interrupt the system. Active attackers generate a wrong message in order to build a cluster of information, while passive attackers just feel the existence of the system. Whenever synchronization function autonomous of the controller, these issues must be taken into consideration by the device architecture (Tomovic, 2016).

4.2 Security Attacks

4.2.1 Session Hijacking: When the session opens, the authorization process is performed. It is simple to hijack the session after the link has been created. The hackers collect specific knowledge about the session throughout this sort of attack and then become the public network among the nodes.

4.2.2 Revealing Identity: In several situations, the driver in the verification process, use personal details. It is simple, thus, for hackers to access the device.

4.2.3 Tracking Position: It is possible to use the position of the car to trace it and gather data about both the passengers and drivers.

4.2.4 Eavesdropping: The network layer is influenced by this form of attack, which then facilitates access to sensitive information.

4.2.5 Denial of Service: it is a famous attack is this one. Hackers block connections to networks via a single node. There are two main ways of carrying out this assault:

4.2.5.1 Jamming: throughout this strategy, the intruder accesses information about the frequency at which the recipient absorbs the messages and then sends the message at the same frequency with the aim of blocking the valid messages.

4.2.5.2 Distributed DOS attack: many attackers attack a single node in this form of assault to block it from accessing resources. (Wang & Sawhney, 2014) For this issue, there are many approaches. The key approach is that there are as many rules as possible in the node's memory. The approach is successful because it eliminates decision-making times and tends to improve the total performance of the system. (Wang & Sawhney, 2014) DDOS may target a control plane where thousands of messages are continuously sent to one or more vehicles through multiple cars on the system. Multiple requests are produced and submitted to the controller since all rules are not usable on the switch, which would then use enormous computing capacity, creating a pause in the outcome or the lowering of requests. The use of many controllers in the region where the congestion level is high is the best response to this form of attack (Chigan, & Wong, 2008).

4.3 SDN in VANET Challenges

These topics are protected by real-time restrictions. First, within 100 meters of the maximum transmission delay, safety-related signals are conveyed. It is necessary to achieve authentication in real time. The second concern concerns the obligation for information consistency, where malicious operations may be conducted by the authentication node that can cause incidents. Therefore, a mechanism must be established to ensure continuity. To eliminate any inconsistencies, the relation between the data collected is chosen. Poor error tolerance is the third problem. On the basis of imaginable efficiency, various VANET protocols based on SDN have been developed. In a short period of time, the method used in the protocols must take action. A small issue or pause within the algorithm may cause harm. Main transmission is the last obstacle. The network security that SDN-based VANET utilizes rely on the key that needs to be secured for ensuring the safety of the documents. The major issue in the creation of security protocols is the exchange of key protocols. Under the conventional VANET system, the SDN-based system allows maintain a solution to the problems (Jaballah, Conti, & Lal, 2019; Kumar & Chand, 0002; Askar et al., 2011).

5. Application of SDN- VANET

5.1 Comfort Applications

These applications used for having information about environment, traffic, and the closest location for oil stations, hospitals, hotels, and restaurants, people use comfort applications. Using the Internet, passengers and drivers can exchange messages (Saini et al., 2015).

5.2 Safety Applications

To enhance the protection of vehicles, travelers and drivers, these types of applications are used. The simple reason for the proposal is to save the drivers and passengers from any accident and to make a protected area for transport. This software receives data from the sensors and other vehicles that are driving about. The key safety and security feature depends on the amount of sensors used to collect data and the program used to process data. (Shafiq et al., 2018; Sulaiman & Askar, 2015; Fares & Askar, 2016).

5.3 Intersection Collision Avoidance

In order to allow the drivers, make choices, it is used when crossing an intersection. The RS captures information from cars traveling next to it and processes the data in the event of any chance of warning or any sort of mishap. A alert message is transmitted to drivers near the altering area so that they can make the proper deciding to stop the car (Saini et al., 2015).

5.4 Stop Movement Sign alert

These are utilized to alert users not to cross the intersection or there may be harmful situations. The communication between the RSU and the sensors of the vehicle requires this. This program warns the driver that other cars are near to the junction, so he has to pause a couple times. Once the other car has crossed the turning point, the driver is given a green flag to cross the intersection (Arif et al., 2020).

5.5 Alert in the Blind Merge Case

This framework feature is used to warn drivers when the visibility at the junction point of a lane is not good. It is used at the intersect stage to gather the data and deliver a result if it is dangerous and alerts the driver to This function of the application is used to alert drivers when visibility is not good at the junction point of the lane. (Shafiq et al., 2018).

5.6 Alert for Job Areas

To reduce their vehicle speed, This structure would transmit a warning message to cars near the work area.(Shafiq et al., 2018)

5.7 Forward Cooperative Crash Alert

This function of the program is used to help vehicles prevent a collision with the other vehicles that are driving ahead. The V2V form of contact is involved in this application function. It offers the risk level ahead of you in the outcome type. (Arif et al., 2020)

5.8 Road Condition Alert

Obus Process the data of the sensors and relay study Outcomes for RSU then rsus send alert signals to all vehicles going into a poorly conditioned area to enable vehicles to stop during the use of the sensors to collect information about the situation on the road. Application This prevents cars from incident-induced emergency breaks through using the emergency stops of the car (Saini et al., 2015).

5.9 Alert for Lane Change

This function of the application is used to warn the driver that changing the lane is dangerous because the gap on the other lane between the existing car and the vehicle is too narrow. This sort of device incorporates information from the cars that drive about. In this form of alert program V2V communication is involved. (Arif et al., 2020)

5.10 Train Ahead on Railway Track

Because of the passing of the train in front, this system feature is utilized to warn the driver. This allows others to be contacted. About your car and the RSU. The RSU is used for the propagation of an alarm signal to all vehicles in their specific zone area. (Shafiq et al., 2018)

6. Conclusion

The aim of this article is to maintain a complete research of SDN-based VANET frameworks to allow readers efficiently manage this field. In this article, we discuss the SDN-based VANET architecture, structures, and operations, and also how SDN-based VANETs allow better connectivity than simple traditional VANETs. In addition, security threats may be controlled by the SDN controller. It is ensured in this survey that this new vehicle infrastructure helps a great deal in managing and controlling the whole vehicle networks that were not previously possible.

References

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Aladaileh, M. A., Anbar, M., Hasbullah, I. H., Chong, Y.-W., & Sanjalawe, Y. K. J. I. A. (2020). Detection Techniques of Distributed Denial of Service Attacks on Software-Defined Networking Controller–A Review. 8, 143985-143995.

Al-Heety, O. S., Zakaria, Z., Ismail, M., Shakir, M. M., Alani, S., & Alsariera, H. J. I. A. (2020). A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET. 8, 91028-91047.

Arif, M., Wang, G., Geman, O., Balas, V. E., Tao, P., Brezulianu, A., & Chen, J. J. A. S. (2020). SDN-based VANETs, Security Attacks, Applications, and Challenges. 10(9), 3217.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 1*6th European Conference on Networks and Optical Communications*, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Benzekki, K., El Fergougui, A., Elbelrhiti Elalaoui, A. J. S., & networks, c. (2016). Software-defined networking (SDN): a survey. 9(18), 5803-5833.

Cabaj, K., Wytrebowicz, J., Kuklinski, S., Radziszewski, P., & Dinh, K. T. (2014). SDN Architecture Impact on Network Security. Paper presented at the FedCSIS (Position Papers).

Chadha, D. J. I. J. I. R. C. C. E. (2015). Reena,"Vehicular Ad hoc Network (VANETs): A Review,". 3(3), 2339-2346.

Chahal, M., Harit, S., Mishra, K. K., Sangaiah, A. K., Zheng, Z. J. S. c., & society. (2017). A survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases. 35, 830-840.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters, International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Hussein, A., Elhajj, I. H., Chehab, A., & Kayssi, A. (2017). SDN VANETs in 5G: An architecture for resilient security services. Paper presented at the 2017 Fourth International Conference on Software Defined Systems (SDS).

Jaballah, W. B., Conti, M., & Lal, C. J. a. p. a. (2019). A survey on software-defined VANETs: benefits, challenges, and future directions.

Jaballah, W. B., Conti, M., & Lal, C. J. C. N. (2020). Security and design requirements for software-defined VANETs. 169, 107099.

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. *6th International Conference on Intelligent Systems, Modelling and Simulation*, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Ku, I., Lu, Y., Gerla, M., Gomes, R. L., Ongaro, F., & Cerqueira, E. (2014). Towards software-defined VANET: Architecture and services. Paper presented at the 2014 13th annual Mediterranean ad hoc networking workshop (MED-HOC-NET).

Kumar, V., & Chand, N. (0002). Data Scheduling in VANETs: A Review. International Journal of Computer Science & Communication, 1, 399-403.

Li, Z., Chigan, C., & Wong, D. (2008). AWF-NA: A complete solution for tampered packet detection in VANETs. Paper presented at the IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference.

Naik, L., Khan, R., & Mishra, R. J. I. J. o. A. E. R. (2018). Comparative performance analysis on revised MANET routing protocols. 13(5), 2443-2451.

Nkenyereye, L., Nkenyereye, L., Islam, S., Choi, Y.-H., Bilal, M., & Jang, J.-W. J. S. (2019). Software-defined network-based vehicular networks: A position paper on their modeling and implementation. 19(17), 3788.

Saini, M., Alelaiwi, A., & Saddik, A. E. J. A. C. S. (2015). How close are we to realizing a pragmatic VANET solution? A meta-survey. 48(2), 1-40.
Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., . . . Rao, N. J. I. C. M. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. 51(7), 36-43.
Shafiq, H., Rehman, R. A., Kim, B.-S. J. W. C., & Computing, M. (2018). Services and security threats in sdn based vanets: A survey. 2018.
Shrestha, R., Bajracharya, R., Nam, S. Y. J. W. C., & Computing, M. (2018). Challenges of future VANET and cloud-based approaches. 2018.
Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.
Tomovic, S., Radonjic, M., Pejanovic-Djurisic, M., & Radusinovic, I. J. V. (2016) Software-defined wireless sensor networks: opportunities and challenges.
Violence, W. H. O. D. o., Prevention, I., Violence, W. H. O., Prevention, I., & Organization, W. H. (2009). Global status report on road safety: time for action: World Health Organization.
Wang, Q., & Sawhney, S. (2014). VeCure: A practical security framework to protect the CAN bus of vehicles. Paper presented at the 2014 International Conference on the Internet of Things (IOT).
Xiaoqiong, X., Hongfang, Y., & Kun, Y. J. Z. C. (2019). DDoS attack in software defined networks: a survey. 15(3), 13-19.
Yassine, M., Shojafar, M., Alazab, M., & Romdhani, I. (2020). Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications.
Yousefi, S., Siadat, M., & Fathy, M. (2006). Vehicular Ad hoc Networks (VANETs): Challenges and perspectives.

Cite this article:

Glena Aziz Qadir & Shavan Askar (2021). Software Defined Network Based VANET. *International Journal of Science and Business, 5*(3), 83-91. doi: https://doi.org/10.5281/zenodo.4497640

Retrieved from http://ijsab.com/wp-content/uploads/688.pdf

Published by

IJSAB International