International Journal of Advanced Science and Technology
Vol. 29, No. 7s, (2020), pp. 5284-5292

Secure Software Defined Vehicular Network (SDVN)

Umesh K Raut, Dr. Manoj K Rawat
[1]*Research Scholar ,* [2] *Professor*
[1,2] *Computer science and engineering Oriental University, Indore (MP)*
umesh.phdcse@orientaluniversity.in , drmkrawat@gmail.com

Abstract

For Intelligent Transportation Services (ITS), new protocols and architecture are continuously being developed by researchers around the globe. Thus, to ensure the safety of drivers many countries are now adopting and investing a lot on vehicular network (VN). On the other perspective, there are many issues like integrity, Security and so on, related to this field that must be resolved before VN technology is practically adopted. In the case of no or low-security, several attacks can occur that may affect the efficiency and the reliability of the system. The search for better networking paradigms has fostered the emergence of Software Defined Networking (SDN), which allows the decoupling of the data plane from the control plane and to configure the network dynamically. SDN provides network operators with significant visibility and granularity of their networks leading to more flexibility in programming these networks. To make VN systems more efficient software defined networking (SDN) technology is introduced with VN. Typically, with every new technology paradigm, the security concerns represent a serious challenge. In this paper, we provide a comprehensive SDN security review including the different vulnerabilities and attacks that SDN suffers from. The objective is to entice the SDN community to address such issues inherently and not as an afterthought.

Keywords: *Software Define network (SDN), Vehicular Network (VN), Security, Attacks*

1. Introduction

Nowadays, in the automation industry, sensors-oriented technology plays a critical role today. Across various areas including health care, transport, education, and others, the required network-based infrastructure for sensors may be used, depending on requirements. Ad hoc vehicle network (VHN) is one of the most important domains for the Wireless Sensor Network (WSN) and Mobile Ad Hoc Network (MANET) for mobile sensing, computing and networking. These include mobile nodes, usually vehicles with access point's i.e. vehicle to infrastructure (V2I) and vehicle-to-vehicle (V2V), as well as other wireless links, such as RSAP and static networks. The network is a combination of a global positioning network (GPS) and a mobile communication system which is based on coverage criteria using a single mode or multi-hop. One of this technology's main strategies is to assist safety drivers in minimizing road accidents. Some of this network offers a main service to guarantee passenger safety on board. The main specifications of VN are high processing power, high volume, sufficient resources and an estimate of node movement.

VN requirements typically include evacuation warnings, emergency response, lane control, congestion or evasion minimization, details on traffic conditions, emergency vehicle targets such as cars and fire trucks. A robust VN security mechanism is therefore necessary to avoid malicious activities in the network. The primary safety concern of VN is to keep the data regulating vehicle. To ensure the VN transparency, the following conditions are extremely important: availability, authentication, no denial and integrity.

In VN, each node or vehicle transfers data to other nodes and can travel in any direction that frequently change its relationship. In order to maintain the link and the proper flow of data, the node devices must constantly transmit data. The aim of information sharing is to give the driver a warning about the anticipated danger, reducing the likelihood of accidents while driving.

In different fields, VN has attracted researchers to develop protocols, applications and tools for simulation. However, there are still many problems facing researchers and developers.

The development of new communication protocols, sophisticated technology, data protection and privacy techniques allows people from different countries to resolve these challenges [2].

A software defined network (SDN) technique has been implemented in the VN device region in order to improve the performance of the entire network. The reason to choose SDN is the fact that some devices, such as routers and switches and network operators responsible for events in the system, are used for communicational purposes in wireless networks. Such devices manage them. Network operators historically implemented system policies manually, which often involved regular modifications. Therefore, contact on the network was increasingly difficult to handle, leading to its collapse. In addition, the complexity of Internet applications and utilities has increased and several problems need to be addressed in order for them to operate efficiently. A programming network, which was further known as SDN, was implemented to solve this issue.

Experimental innovations concentrate on the destruction of control and data aircraft structures. In particular, VNs need to be highly flexible in adapting and providing a very low latency in any situation and usage. SDN is seen as promising to improve the management of networks. The existing network configuration also requires replacement and simplification of hardware functions. The SDN system is essentially based on a detachment from the data plane control aircraft. Data planes are represented in the SDN framework as data transfer and the entire network control plane. Both SDN-based networks implementations used wires previously, such as Twitter, Google, and Cisco. Nevertheless, the SDN method is considered an innovative way of using mobile wireless networks because of its simplicity. The absence of control and data planes allows the operation of this network even as the number of nodes on the network expands rapidly. This new SDN architecture was deployed in VN to handle network-wide contact. The main components for SDN-based vehicle network systems are the SDN and the SDN with RSU controllers as shown in following figure 1.

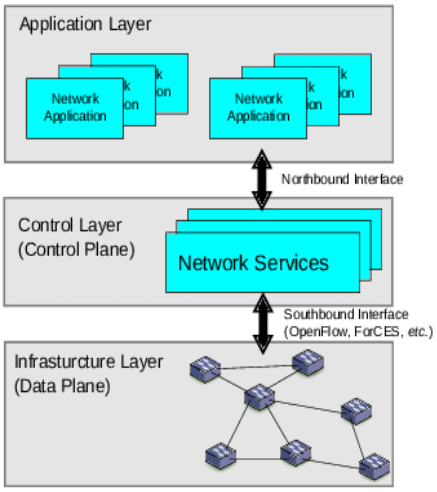

Figure 1: SDVN Network

The SDN controller controls the entire system's network behavior. The road side unit (RSU) is normally associated. The SDN-based VN vehicles are considered to be nodes. The unit (OBU) and application unit (AU) are given for these systems. They take part in the conversation collectively. The AU can be used as a personal computer or as a remote user [13]. The AU communicates with the OBU across the network and is in charge of all modes of contact. The RSU is a physical device permanently installed on the roadside or at a car park. The RSU is wired to a network to communicate with vehicles and the SDN controller. The RSU provides the appropriate services and the OBU uses the resources to host an application. The RSU is capable of connecting to the internet, allowing the AUs to connect to the internet in multiple vehicles [3].

1.1 Possible Attacks in VN Network:

The Multiple threats compromise transmission, control and device layers. The lack of protection in the transport layer triggers man-in - the-mid attacks between a switch and a

controller. These attacks can be mitigated by through physical safety network attacks, which can saturate flow tables and buffers. Rather of taking an aggressive approach, the application of reactive rules is responsible for these attacks. Multiple controllers may be avoided. Certain threats can arise from multi-controllers, software, unauthorized access, or configuration or security conflicts. While solutions are in place, high mobility calls for security systems capable of authenticating in real time. Otherwise, latency could result in traffic jams preventing SDVNs from being realized. This influences in real time raises security difficulties.

Application Level: Malicious apps can corrupt the SDN controlling mechanism and cause breaches of authorization, escalation rights, exhausting resources available, breaches of service chains, or malicious network control messages which could have destruction to the network behaviour. The application by third parties can also pose grave threats due to the heterogeneity of suppliers, lack of security interoperability and confidence issues.

Control plane: compromise switches can result in manipulation of the network or network topology view of the SDN controller or creating false links. Control plane For the spoofing of network resources or to collect confidential information, Control messages may be exploited. More general attacks are breaching SDN controller authorizations, violating network isolation or endangering accessibility to controllers. Being the only problem for decision-making, the controller makes the control aircraft particularly vulnerable to attacks and failures. Network awareness can also be used to initiate new attacks [24]. Interoperability problems can also cause vulnerabilities between multiple controllers.

APIs for communication: API protection and lack of standardization are the greatest risks. In general, the Southbound API is vulnerable to human attacks, hacks or accessibility attacks. The tailored OpenFlow and Northbound APIs for SDVN are not standardized. Also, APIs between controllers are not uniform between Eastbound and Westbound [25].

Several of the VN attacks [5][6] follow,

A. **Phony data:** In this case, square attackers calculate the moral, active insiders. This must submit incorrect information inside the network so that it can influence driver behavior.
B. **Cheating with sensing component data:** The UN assailant Agency conducts this attack as a corporate, logical and successful one. They use this assault to adjust location, speed and direction of the various nodes so that liability can be removed in the event of a malfunction.
C. **Denial-of-Service (DOS):** In this attack the attacker is malicious, active and native in this case, as the unauthorized person may want to interrupt the network by sending unwanted messages in the guidance.
D. **Replay and delete packages:** an unauthorized individual can drop valid packets in this form of attack. For example, the unauthorized an would drop all warning messages intended to notify vehicles to the accident site. Likewise, an will replay packets while the incident is occurring. AN will replay the packets.
E. **Hidden Vehicle:** In a situation where vehicles seek to conveniently cut the congestion on the wireless web, this form of attack is viable. For example, a vehicle sent its neighbor a warning message and waited for an response. When the response is received, the vehicle knows that the neighbor of the vehicle is in a much higher place to forward the warning message and avoids making different nodes.
F. **Worm Hole Attack:** This attack is hard to detect and avoid. A malicious node records packets at one point in the network and tunnels them to another location over a network of malicious nodes shared by people. The severity of the attack would increase if the malicious node only sends management messages through the tunnel and not packets of information.
G. **Sybil Attack:** A vehicle forges the identities of many vehicles during this attack. Such identities should not be used to manipulate the program in any way. In addition, these false identities create AN impression that additional road vehicles are counted in

locations. As a result of this attack, each attack can compete until the positions or identities of different nodes in the network are spotted.

II. Motivation

Safety is especially difficult because of the complexity of communication and lack of funding for infrastructure across all ad hoc network research issues. Many methods have been developed and introduced, but it is still difficult to ensure that the entire network is free of malicious attacks. The difficulty of the communication and the lack of support to infrastructure make safety extremely difficult among research problems faced by the ad hoc network. Each part of the network has a single role with the most vulnerable routing. Thus, after extensive research and networking review, we decided to guide our efforts towards SDN-based VN guidance. SDN is a revolutionary technology that remains under development and consideration. To order to solve problems relating to security, new communication protocols, advanced hardware, data protection and privacy strategies will also contribute to addressing these challenges.

III. Literature work

In this section, discuss the different related work related to SDVN in current trends number of authors proposed different security problem in adhoc network

Rong geng, Xiaojie wang and Jun liu[1]. Authors suggested two new protection approaches for VNs in this article. Secondly, a software-defined concept for simplifying network management and decomposing the monitoring and data plans constitutes the hierarchies of the network. In the protocol to protect a particular network attack and for secure and efficient VN routing also includes numerous protection schemes. Authors speak of a replay attack, which means that the attackers sent the packet to circumvent the device via its target node, primarily for the purposes of identity authentication and the breakage of authentication. The author tackles replay attacks. The replay protection framework uses, for example, the master sequence number and the maximum MAC sequence number in the list for the multifunctional module. In comparison to normal network performance and control overhead without safety, these results show that the security arrangements significantly improve the network efficiency, which has shown that the network load capability varies. Other layers are overlooked, or an adaptive and multi-level joint optimization protection algorithm can be implemented. When the sequence number is periodically restored to zero in a sequence number algorithm, the output of the algorithm is affected.

Vehicular cloud computing (VCC) may be vulnerable to many attacks because of the public existence of its network: Mr Mhidi Bousselham, Abderrahim Abdellaoui, and Habiba Chaoui[6]. There is also one of the most critical problems for maintaining security and privacy in this model. The author uses SDN technology to create a new protection strategy to protect vehicles from malicious nodes by means of pseudonyms, key management and revocation list providing authenticity, confidentiality, honesty and availability. In creating a special light weight cryptography algorithm dedicated to vehicle cloud computing, the author does not take confidentiality into account.

Introducing the latest optimization-based packet routing scheme for software-define vehicle networks, Kalupahana Liyanage Kushan Sudheera[7] has implemented a source routing flow instantiation (FI) software routing scheme. The routing system closely analyzes the reliability of the links when selecting routes and formulates the problem as a minimum cost-controlled flow. In addition, the alternative package allocation is being introduced to fix the problem of routing in a less complicated way. The goal is to find a few packages to supply quickly and safely. The FI system supplies flow information efficiently and stores flow information with no contact with the control unit in the appropriate node. The multi-hop data transfer is performed better on vehicle networks using the proposed routing scheme than both existing VANET and SDVN routing protocols. The author does not check the validity of a node.

The author proposes an architecture based on SDN which uses cloud computing and addresses the inherent VANET restrictions. Atwal Singh, Mostafa Bassiouni Ajay Guleria [8]. A logically distributed control unit is designed for smooth communication, mobility management

and QoS support. In response to SDN and Cloud Computing problems, the proposed model achieves the best efficiency and power. QoS and routing applications were introduced in order to test the proposed model. To demonstrate the efficacy of the technique the comparative experimental findings are analyzed. This study is not considered for multiple access networks which connect cars at the time and optimal data delivery strategies for the proposed model. A detailed literature review by Priyanka Prabakaran, Deva Priya Isravel, Salaja Silas[14], readers of the next generation SDN-based networks. A overview of the SDN architecture and the scope of implementation of SDNs is given. SDN characteristics are explained. Detailed overview of the different ways in which SDN enhances next generation networks. SDn integration with the intelligent home, intelligent healthcare, intelligent transport, optical networks and wireless network is addressed to improve the main challenges. The following are outlined. In addition, many more challenges are required to extend the functionality of SDN to other intelligent networks.

Bryan Parno, author Adrian Perrig[15], points out that reliable protocols need to be built in order for car networks to be viable and appropriate to consumers. The seemingly contradictory demands of customers and car producers and the Government are making safe protocols more complicated, especially in terms of maintaining a consistent identification of the vehicle and safeguarding driver privacy. Happily, these problems are being tackled through the properties of vehicle networks and the creation of new primitives, based for instance on the interconnection of the trajectories and the use of simple resonant converters. They expect to encourage other researchers to begin researching this significant and exciting subject area by the challenges outline in this article and the new possibilities for solutions in vehicle networks.

This paper proposed a stable, mutually-authenticated framework with respect to privacy security in response to the above challenges existing in VANETs by Jie Cui, Wenyu Xu, Yibo Han and HongZhong[16]. First, the vehicle must perform a reciprocal authentication procedure between TA and the vehicle before messages are transmitted to other vehicles, to ensure that any intruder can not reach the contact range in order to send false messages. Second, these details were modified to avoid the side-channel attack before the assailant acquires the data (such as internal pseudo-identity and encryption keys) stored on its tamper proof computer. Finally, because the bilinear combination in the present plan is not used, the device expense in output assessment is smaller than other schemes. Mutual authentication is therefore more suitable for large-scale VANETs. A new form of privacy protection protocol can be researched via the 5 G network, but the author has not taken this into consideration.

Ahmad Arsalan, the author of software identified by VANET called data networking (NDN) and suggested a method for timing attacks in safety-critical applications, Rana Asif Rehman[17]. At Press, detect a vehicle first to verify if it is an attacker. The SDN controller used to minimize this by using a default controller list when an attacker's vehicle is identified. This agreement ensured that the network did not forward delayed emergency packets. Such detection is often achieved at the attacker's next hop node. The results of simulation show that that delays are attributable to an increase in the number of vehicles on the attackers ' network and also to the increase in the rate of transmitting control packs. The use of the timing attack prevention (TAP) protocol often decreases the amount of double urgency messages in a network while they are dramatically increased in case of a typical VNDN timing attack. In support of the NDN and SDN administrator, the author did not focus on other security problems of VANET.

The author Yao, Lei Guo, Ye Liu, Jian Zheng, and Yu Zong[18] built a platform to detect and rapidly respond to the DDoS assault on VNs based upon software-defined networking (SDN). The proposed system does, however, provide a multi-dimensional data flow extraction technique aside from the triggers based in the OpenFlow protocol (i.e. PACKET IN). The author also constructs an efficient, global Network Flow Table based on OpenFlow and the flow table entropy functions and decides on the appropriate SVM for all flow table entries. In analysing the results of the simulation, the author verifies that the detection scheme decreases the identification and classification identification time efficiently and has a lesser false alarm.

This paper discusses improved voiceprint detection for SCH, which is required by writers Yuan Yao, Bin Xiao and Gaofei Wu[19]. It decreases observation time considerably and decreases false positive rates. In addition, they extend Voiceprint to identify sudden shifts of the

RSSI time series using several change-point detection methods. Therefore, Voiceprint will classify the unauthorized nodes that monitor power during attacks in Sybil. Although the authors suggest a solution for the power control Sybil attack, the implementation of RSSI-based detection systems is often a complicated issue. Consequently, their work in this subject will continue. The authors are not evaluating comportaments of illegal nodes that alter their transfer powers to construct a sybil attack power control model.

C. Ansere, P. Nkurunziza, J. H. Anajemba and A. O. Iwendi, M. Uddin, J. A.A. K. Bashir [20], author of this book, addresses a safety hazard in VHNs. In the attacker is inserted a malicious node with several identities. As the roadside unit (RSU) does not synchronize its clock with legitimate vehicles, it identifies unauthorized vehicles and transmits erroneous messages accordingly.

IV. Research gap

In particular, the VNs raise protection and privacy concerns due to the existence of open access communications. VNs are often made up of all types of devices and some devices are resource-restricted nodes which are necessary to protect the network while maintaining low overheads. For simple conventional networks, including structures, central controls, managers, fly changes or checks, present networking requirements cannot be discussed and complied for. To boost the network efficiency, open-access systems must be introduced in the VN market.

OBJECTIVES OF THE STUDY

- Investigation & analyze of various type of attack In Vehicular network.
- Design an algorithm for detection and mitigation of Regular SDVN.
- To implement a dynamic resource allocation method in VN.
- Design an algorithm for providing security in SDVN algorithm.
- Simulate SDVN architecture to identify security feature using existing framework.

V. Proposed methodology

In The transmission of different vehicles and the RSU by a wireless network is accomplished in the SDVN architecture. This technique is used to communicate a wide range of knowledge that provides drivers with sufficient information and enhances road safety. Communication between the data plane and the control plane is done in the SDN-based VN system. The data plane comprises the transmitting equipment while the control aircraft manages the contact flow. The control plane has many levels, each of which contributes to the network's functionality.

SDVN has promising prospects to improve the protection of legacy car networks that monitor many of the vehicle's essential safety characteristics. The resilience, unfortunately, remains elusive and expensive to date. Typically, major hardware architecture improvements are required to support new features. In the event of failed SDVN, the in-vehicle ECU network topology can be easily reconfigured with the SDN controller to add auto healing capacities. SDVN programming advantages can help prevent hardware redesign.

VNs must be reconstituted such that the conventional network structure is broken and hardware functions are streamlined. For this purpose, we have to construct VNs on openflow and DSR protocol based on software-defined networking and adjust the Hierarchical structure so as to reduce the overhead network hierarchical [13].

Cryptography is commonly used in wired and wireless networks to ensure confidentiality of information. Different protection schemes, such as encryption, have been proposed for different attacks and data packets can choose a modular system based on network conditions and security requirements [25].

In this work, we detect and protection the malicious node by using an ECDH key, sharing the data between nodes and a central control unit via RSU.

Some of the attack can occur when communication between devices and RSU is carried out. After the attack in network is detected, the central control units send the message about the

false node into the network so that the unauthorized hacking operation can avoid the information and protect the network.

On the basis of our review of the SDVN network we found that in all kinds of attacks, the common feature drives vast quantities of traffic into the network to depletion its resources. Usually a network activity pattern can be specified to determine the agreed bandwidth consumption rate in ordinary circumstances. In order to identify traffic as abnormal, sudden rises in traffic, delays, CPU usage or a sudden decrease in the efficiency of any network assets should be taken into account. In general, the form of data within the network is linked to anomalies. The first big step in identifying anomalies is to consider the existence and characteristics of the transmitted information on the network. Many of the features include packet header, delay, packet size, type of protocol, etc. Therefore it is assumed that the network characteristics determine the intrusion type. If a network is vulnerable to a particular threat, the initiative will concentrate on detecting and mitigating these threats [24].

VI. Conclusion and future work

SDN would likely replace some innovative features of current conventional networks. Nevertheless, several safety issues in VN still hinder SDN adoption. In this analysis, the vulnerabilities, attacks and solutions of the present SDVN were analyzed. A variety of new attacks are being revealed in SDVN apps. The specifications of these networks therefore need to be made more reliable and secure. This helps SDN to examine the issues facing defense. Investigations into SDVN protection have not yet begun. Since SDVN is increasing in popularity and the need for multimedia and future VN commercial use, QOS is an inevitable task, which means that a safer network is needed. In this work, new methods are provided for Secure SDVN using an ECDH key and malicious nodes can be detected using time stamp and the operation based on signal process. VN can overcome the complicated routing problem by using a set of vehicle agents (forward, backward and upgrade vehicles). This study provides a protection based on the ECDH key method and attack detection through the RSU comparison of the data store on a central control unit. Dynamic allocation of resources often used in SDN for the reduction of energy consumption. This scenario allows for large networks to reach even in high mobility networks and is still working well.

In future we are going to implement the proposed method and measure performance of system in real time scenario.

References

1. Rong geng, xiaojie wang, and jun liu, “A Software Defined Networking-Oriented Security Scheme for Vehicle Networks”, 2169-3536 2018 IEEE.
2. Sudeep Tanwar, Jayneel Vora, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S. Obaidat, “A systematic review on security issues in vehicular ad hoc network”, © 2018 John Wiley & Sons, Ltd.
3. Hammad Shafiq, Rana Asif Rehman , and Byung-Seo Kim, “Services and Security Threats in SDN Based VANETs: A Survey”, Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 8631851, 14 pages https://doi.org/10.1155/2018/8631851.
4. Mina Rahbari and Mohammad Ali Jabreil Jamali, “Efficient detection of sybil attack based on cryptography in vanet”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.
5. Heng Zhang, Zhiping Cai , Qiang Liu , Qingjun Xiao, Yangyang Li, and Chak Fone Cheang, “A Survey on Security-Aware Measurement in SDN”, Security and Communication Networks Volume 2018, Article ID 2459154, 14 pages https://doi.org/10.1155/2018/2459154.
6. Mhidi Bousselham, Abderrahim Abdellaoui, and Habiba Chaoui, “Security against Malicious Node in the Vehicular Cloud Computing using a Software-Defined Networking Architecture”, DOI: 10.1109/ICSOFTCOMP.2017.8280084, ©2017 IEEE

7. Kalupahana Liyanage Kushan Sudheera, "Link Stability Based Optimized Routing Framework for Software Defined Vehicular Networks", ieee transactions on vehicular technology, vol. 68, no. 3, march 2019.
8. Kuldip Singh Atwal, Ajay Guleria, Mostafa Bassiouni, "SDN-based Mobility Management and QoS Support for Vehicular Ad-hoc Networks" 2018 International Conference on Computing, Networking and Communications (ICNC): Mobile Computing and Vehicle Communications ©2018 IEEE
9. A. Hussein, Louma Chadad, Nareg Adalian, Ali Chehab, Imad H. Elhajj & Ayman Kayssi , "Software-Defined Networking (SDN): the security", ISSN: 2374-2917 (Print) 2374-2925 (Online) Journal homepage: https://www.tandfonline.com/loi/tsec20.
10. Basta, A., Blenk, A., Hoffmann, K., Morper, H. J., Hoffmann, M., Kellerer, W. (2017),"Towards a Cost Optimal Design for a 5G Mobile Core Network Based on SDN and NFV", IEEE Journals & Magazines, 14(4): 1061 – 1075.
11. Prabhakar Krishnan1 and Jisha S Najeem2, "A REVIEW OF SECURITY THREATS AND MITIGATION SOLUTIONS FOR SDN STACK" , Volume 115 No. 8 2017, 93-99.
12. Kallol Krishna Karmakar_, Vijay Varadharajany, Udaya Tupakulay, "Mitigating Attacks in Software Defined Network(SDN)", 978-1-5386-2855-3/17/$31.00 ©2017 IEEE.
13. Atul B Kathole, Dr.Dinesh N.Chaudhari, " Fuel Analysis and Distance Predication using Machine learning", 2019 ,International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 5 Issue: 6.
14. Khaoula Jeffane , and Khalil Ibrahimi , "Detection and Identification of Attacks in Vehicular Ad-Hoc Network", 978-1-5090-3837-4/16/$31.00 c 2016 IEEE.
15. Priyanka Prabakaran, Deva Priya Isravel, Salaja Silas, "A Review of SDN-Based Next Generation Smart Networks", 978-1-5386-9371-1/19/$31.00_c 2019 IEEE.
16. Bryan Parno, Adrian Perrig, "Challenges in Securing Vehicular Networks" DAAD190210389 from the Army Research Office, and by an NDSEG Fellowship from the Department 2017.
17. Jie Cui , Wenyu Xu , Yibo Han , Jing Zhang , Hong Zhong ,"Secure mutual authentication with privacy preservation in vehicular ad hoc networks", https://doi.org/10.1016/j.vehcom.2019.100200 2214-2096/© 2019 Elsevier Inc. All rights reserved.
18. Ahmad Arsalan, Rana Asif Rehman,"Prevention of Timing Attack in Software Defined Named Data Network with VANETs", 978-1-5386-9355-1/18/$31.00 ©2018 IEEE DOI 10.1109/FIT.2018.00050
19. Yao yu, Lei guo, Ye liu, Jian zheng, and Yue zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks", 2169-3536 2018 IEEE.
20. Yuan Yao, Bin Xiao, Gaofei Wu,"Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI", 1536-1233 (c) 2018 IEEE.
21. C. O. Iwendi , M. Uddin , J.A. Ansere , P. Nkurunziza , J. H. Anajemba , and A. K. Bashir , " On Detection of Sybil Attack in Large-Scale VANETs using Spider-Monkey Technique", 2169-3536 © 2017 IEEE.
22. Echagüe, J., Cholvi, V., Kowalski, D. R. (2018). Effective use of congestion in complex networks, Physica A: Statistical Mechanics and its Applications, 494: 574-580.
23. Kashoash, H.A.A., Hassen, F., Kharrufa, H., Kemp, A.H. (2017). Analytical modelling of congestion for 6LoWPAN networks, ICT Express.
24. Atul B Kathole, Dr.Dinesh N.Chaudhari, "Pros & Cons of Machine learning and Security Methods",2019.http://gujaratresearchsociety.in/index.php/ JGRS, ISSN: 0374-8588 ,Volume 21 Issue 4
25. Atul B Kathole, Dr.Prasad S Halgaonkar, Ashvini Nikhade, " Machine Learning & its Classification Techniques ",International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9S3, July 2019.
26. Maqsood, T., Bilal, K., Madani, S.A. (2018). Congestion-aware core mapping for Network-on-Chip based systems using betweenness centrality, Future Generation Computer Systems, 82: 459-471.

27. Cooper, S. B., DiMaio, D. (2018). Static load estimation using artificial neural network: Application on a wing rib, Advances in Engineering Software,.
28. Lieber, M., Nagel, W. E. (2018). Highly scalable SFC-based dynamic load balancing and its application to atmospheric modelling, Future Generation Computer Systems, 82: 575-590.
29. Erzurumluoğlu, A. (2018). Constructing day-balanced round-robin tournaments with partitions, Discrete Applied Mathematics, 235: 81-91.
30. Li, J., Wei, G., Ding, D., Li, Y. (2018). Set-membership filtering for discrete time-varying nonlinear systems with censored measurements under Round-Robin protocol, Neuro computing, 281: 20-26.