Grenze International Journal of Engineering and Technology, Special Issue

A Survey on Detection and Prevention of Security Attacks in VANET

Naveen R[1], N.S.V Chaitanya[2], Nikhil Srinivas M[3] and Dr. Nandhini Vineeth[4]
[1-3]Department of Computer Science, BMS College of Engineering, Bangalore, India
Email: [1]naveenkumarr97@gmail.com, [2]nsvc99@gmail.com,[3]nikhil.srinnivas577@gmail.com
[4]Assistant Professor, Department of Computer Science, BMS College of Engineering, Bangalore, India
Email: [4]nandhiniv.cse@bmsce.ac.in

***Abstract*—In the current generation, road accidents and security problems increase dramatically worldwide in our day to day life. In order to overcome this, Vehicular Ad-hoc Network (VANETs) is considered as a key element of future Intelligent Transportation Systems (ITS). With the advancement in vehicular communications, the attacks have also increased, and such architecture is still exposed to many weaknesses which led to numerous security threats that must be addressed before VANET technology is practically and safely adopted. Distributed Denial of Service (DDoS) attack and Sybil attacks are the significant security threats that affect the communication and privacy in VANET. As simulators are being used in our work, we have discussed OMNET++ which is a new modernized latest mobility and network simulators as well as data network simulator. This is also integrated with the road traffic simulator SUMO with Veins, an open-source framework for VANET simulation. An in-depth survey of a new innovative technology called as Vehicular Cloud Computing (VCC) which has an enormous impression on ITS by utilizing the assets of vehicles such as the internet, storage, Global Positioning System (GPS), computing power for creating a quick judgment including the transmission of information between the cloud and VANET. In addition to providing the usage and approach of vehicular cloud, a short survey of the routing protocols, major security threats, attacks and even security solutions for cloud computing have also been surveyed. An extensive survey has been done on the architecture of VANET, existing protocols, prevalent security attacks etc. and after analysing the pros and cons of the existing algorithms, the objective of this our work is to design an algorithm to detect and avoid various kinds of attacks using Vehicular Cloud computing. An analysis has also been done by applying four protocols on an existing scenario of real traffic simulator using OpenStreetMap and the best suitable protocol has been selected for further application.**

***Index Terms*— VANETs, Security attacks, DDOS attacks and Sybil attacks, Vehicular Cloud Computing (VCC), SUMO, OMNET++ and Veins, IEEE 802.11p, Routing Protocols.**

I. INTRODUCTION

Vehicular Ad-hoc Network (VANET) provides a smart transportation system owing to Vehicle to Infrastructure (V2I) and Vehicle to Vehicle (V2V) message dissemination with an objective to provide safety on roads. VANET in comparison to Mobile Ad-hoc Network (MANET) points to an exceptional kind of

Grenze ID: 01.GIJET.6.2.6

networking with high mobility nodes which are vehicles. Major applications of VANET include electronic brake light, parking management and point crash notification. The topology in VANET varies according to vehicle movement scenario such as traffic light, highway and urban road scenario. The contribution to the area of VANET by the research community on various layers is on the rise. The simulator close to the real-time set up for VANET is the preferred choice of researchers as it involves less cost in comparison to really set up. The recent updates about security attacks in VANET. Trust and Privacy are explained in Ref. [1].
Nearly 1.25 million people die each year and on an average 3,287 deaths, a day is observed according to the world health organization. Many engineers from a different area of studies such as vehicle designers and road engineers help in the reduction of the number of road accidents. VANETs are applicable in both rural and urban. Constraints of VANET is that the velocity of vehicles are purely depending on the speed limit of the roads they travel. Traffic signs and signals are bound to be followed by all vehicles which make VANET less difficult than MANET.
This paper's key contributions can be summarized as follows: researching the main VANET network attacks like DDoS attacks and vulnerabilities in VANET. Exploring machine learning's success in reducing VANET Security attacks. Summarize and categorize the findings of recent research on the securing of VANET has been discussed.
The organization of the rest of the paper is as follows. In Section 3, an overview of detection and prevention techniques, existing mechanism in VANET system has been explained. Further, Discussion and comparative analysis are done in Section 3. Finally, Section 4 provides the Conclusion and Future Work of the relative study.

II. LITERATURE SURVEY

A. Vulnerabilities in VANET

The new threats and vulnerabilities of the security are classified in VANET. The systematic and compressive analysis of VANET securities and their breaches are done in Ref. [2]. The vulnerabilities and threats based on the security requirements in VANETs are classified around 20 different categories of threats are presented along with various attacks and security procedures in VANET. Fig.1 shows the classification of the security attacks in VANET. Each attack is provided with a security procedure. The paper presents attacks based on security requirements such as availability, confidentiality, integrity and attacks on non-repudiation discussed in depth.

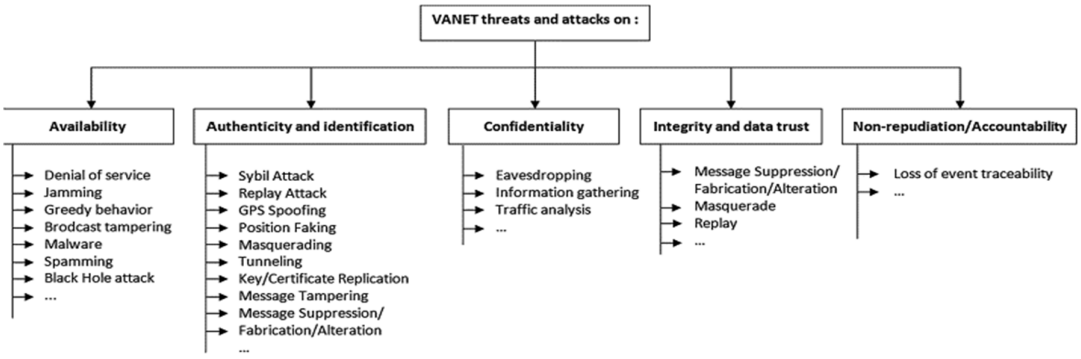

Figure 1. Classification of security attacks in VANET

In Ref. [3], the author proposed a Multiple Malicious Nodes detection (MMNDA) algorithm to detect both the genuine and irrelevant packets by considering the velocity and frequency of the vehicle nodes. The suggested method is better for detecting the multiple nodes rather than a single node as proposed in the existing system and the lifetime of the network has been increased. Hence Proposed algorithm shows that increased mechanism for detecting DDOS and Sybil Attacks with less packet loss ratio and high network lifetime and also RSU can communicate with a number of nodes at the same time.
An algorithm is found to detect malicious node which acts as a genuine vehicle during the session of hijacking attack in VANET. In Ref. [4], authors proposed an algorithm to form a cluster in the vehicular network and the RSU assigns random ids to all the nodes in the cluster, then the session starts by measuring time gap between the nodes, the distance and traffic flow (TF). A Machine Learning algorithm is used to

determine the registered table, where a vehicle is considered an honest vehicle if TF value is less than or equal to 1 and it is added to the registered table. A vehicle is tagged as malicious node if TF value is greater than 1. This result in high throughput, less end to end delay by detecting a malicious node and a smaller number of dropped packets.

The State-full network connection is required to maintain a reliable connection between V2V and V2I. In Ref. [5], authors introduced a system here is integrating the classic IEEE 802.11p standard and hybrid LTE network that forms a hybrid Cloud-VANET. This gives an efficient routing protocol with high reliability, less congestion and low network overhead in VANET. The suggested system uses the SUMO and OMNET++ to simulate the network scenario which demonstrates that a hybrid cloud-VANET develops the transmission authorization by hitting a low SNIR loss and a low ratio of data and packet loss over the network. The proposed system shows that network connectivity is improved in all traffic densities and is capable of implementing applications like shared storage and Streaming video. This hybrid Cloud VANET with IEEE 802.11p-LTE based on VANET can be used for future analysis.

B. Distributed Denial of Service Attack in VANET

In Ref. [6], authors Introduced a system which is centralized Software-defined network (SDN) architecture in VANET. In this network, the LTE which is used as a controller for a long-range network interface, in order to receive and request flow rules and it also controls all the vehicles and the RSU in the network. The author proposed a new algorithm called Sentinel, a new defence procedure which is used to find the source of spoofed packets and mitigate these attacks by creating a flow tree. The analysis of packet flow with respect to time is used to detect flooding attack. Results of the mitigation method are promising. Even in different situations such as dense traffic network, the algorithm was able to detect and mitigate the attack. In the detection phase, it helps us by avoiding false detections using generated flow rules and several packets being processed together. When the algorithm truly detects an attack, it starts the process by mitigating the attack which is achieved by building a flow tree to localize the bots. Sentinel is able to mitigate attacks even in the scenarios suck as high-speed vehicles which didn't affect the results of the algorithm. The classical classification of the algorithm is replaced by new data classification which uses machine learning. Finally, this algorithm achieves a mitigation of 78% in all scenario.

To overcome infrequent connections between vehicles and to increase the availability of VANETs, we need to efficiently mitigate DDoS attacks by using robust network detection system which is explained in Ref. [7]. The Proposed algorithm is used to detect a DDoS Attack in VANET. In this algorithm, we use big data technologies to detect DDoS attacks on the system. This detection system has two components, they are- real-time network traffic collection module and network traffic detection module. To perfectly achieve this system, HDFS is used to store massive attack patterns. Spark is used to detect and increase the processing of packets. In order to evaluate the algorithm for accuracy, which is divided into datasets containing NSL-KDD and UNSWNB15, Random Forest classifier algorithm is used to classify results. When experiments are practically tested out, they show an accuracy of 99.95% and 98.75% in the two datasets respectively.

In Ref. [8], A greedy approach is used which detects and mitigates the DDOS attacks by creating the attack topology and network congestion in VANET. In this section, each node bandwidth consumption in the network is analysed and previous data is evaluated to set the threshold for each node. If the threshold is high it means that a node is detected. This node is sent to mitigate by separating that detected node from network. This proposed technique for detecting malicious nodes in the network is less complex than the previous algorithm. The proposed method is demonstrated by developing the NS2 simulation, by creating a set of nodes. Finally, the proposed system shows that it is better than the previous techniques in these respective areas such as overhead, packet loss and better throughput. This methodology is used to represent DDoS attacks especially in V2V communication i.e. vehicle to vehicle communication.

To detect both low rate and high rate of DDOS attack in VANET, the authors in Ref. [9] proposed a system which mainly focuses the communication between the vehicle and RSU which acts as a centre of the network system. To detect the Online Discrepancy Test (ODIT) which supports two algorithm such as Cumulative Sum (CUSUM) test and Geometric Entropy Minimization (GEM). The obtained result simulated using the Traffic Simulator SUMO which is integrated with Network Simulator OMNET++ and Real-world Traffic Simulator Veins to analyse. Finally, the proposed system detects the location of the attack and to prevent this attack by blocking the data traffic from attack location.

In Ref. [10], the authors proposed a Multivariant Stream Analysis (MVSA) for detection and prevention of the Distributed Danial of Service attacks in VANET Security system. The V2V communication with RSU has been used for the transmission. The proposed system reads the network trace, measures the average of the

payload and frequency of each stream class is calculated at different time frames. And, time to live (TTL) is calculated by considering the vehicle node. By using the detected traces, the method finds the stream weight and classifies the packages into attacked or legitimate nodes. Finally, the performance of the proposed algorithm is done by using the network simulator NS2 which demonstrate the efficiency and effectiveness of the proposed system.

The detection of the DDOS attack discussed in Ref. [11]. The author proposed the System SDVN (Software Defined Vehicular Network) which is effectively detect the DDOS attack. The proposed framework contains the three models such as attack detection module, detection trigger module, flow table item collection module which is the first module for detecting based on PACKET_IN message. The machine learning module called SVM, which is a classifier is used to train the sample and build a detection model to find to detect the DDOS nodes in the network. The system generates the manual DDOS attack traffic using the Scapy and hping3. The result shows that after the simulation done is classification recognition has a lower false alarm rate and decreases the time to start attack.

C. Sybil Attack in VANET

The Nodes in Vehicles gains an identity of another node called a Sybil attack. In Ref. [12], proposed an algorithm to detect Sybil attack in VANET. The proposed algorithm uses the Encrypted and decrypted algorithm which is focused on the hybrid public key infrastructure and RSU Chain Stamp concept to provide the secure communication in VANET. By using public Key Cryptography mechanism, the result of Simulation of key generation and exchange via public key infrastructure algorithm in the real-time environment; obtaining real-time certificates of authentication from authority is difficult. The proposed simulation confirms that if any node attempts to interrupt the communication between two or more vehicular nodes, then it will be identified based on the suggested model.

In Ref. [13], To solve this problem, this paper proposes a Sybil nodes detection method based on RSSI sequence and vehicle driving matrix - RSDM. To detect the Sybil nodes the evolution of the difference between the RSSI sequence and the driving matrix is done by RSDM. The proposed system performs well with the highest detection rate and a lower error rate. The result is by simulation which gives the detecting the Sybil attack node by the accuracy of more than 90% and 0% error rate with the less false positive rate (FPR) and (False Negative Rate (FNR).

In Ref. [14], authors proposed a two-phase security-based mechanism to provide a reliable solution to identify and block the attacked nodes by detecting Sybil attack to provide safety, reliability and secure the application efficiently. The first phase PKI (Public Key Infrastructure) is used to give the secure communication based on identification certificate authority (CA), Second method Hash Function mechanism is used to detect the Sybil attack by analysing the collecting data assets is hash set. Hence, this type of merged techniques had given a great result and prevention of the data in the VANET communication system.

Vehicles communicate with Roadside Units (RSUs) in VANET system. In Ref. [15] the author proposed a scheme for detecting Sybil attacks based on RSUs support. Two vehicles passing by multiple RSUs at the same time is a very rare coincidence and the two vehicles will be having two different identities (IDs) considered for detecting the Sybil attack nodes in the VANET. The Suggested method uses routine communication between nodes and RSUs to detect the attackers. Then After the result is analysed by using the simulation tools which gives the best result with the highest throughput, False positive report and less network overhead. The proposed methods detect the Sybil attack with an accuracy of nearly 100% with 0% error rate.

D. Vehicular Cloud Computing (VCC) in VANET

In Ref. [16], authors have given a brief explanation about using Vehicular Cloud Computing (VCC) in VANET for the communication between the vehicles. Also explained about the Framework for working on VANETs. Then, discussed on various cloud services provided by VCC in VANETs and given a complete explanation on the VCC architecture. The author explained the research challenge and future work on each cloud services provided by the VCC. In this paper, the Comparative analysis on the different simulator frameworks such as Network simulator, Traffic Simulator and VANET Simulators and Frameworks for the VANETs communication is explained. Finally, the Different Vehicular Datasets is given for the future analysis on the security issues on VANET.

To avoid the security issues in Vehicular cloud computing (VCC) on VANETs, in Ref. [17], the author presented an alternative solution that the new decoy Technology (DT) and user behaviour profiling (UBP) used to overcome the security in data, trust and privacy on VCC. When attackers attack the system, the

proposed mechanism sends the decoy files which can't be differentiated by the attacker's file, hence preserves the security. Here, the authors have used the 50 vehicles for the simulation and the result obtained was differentiating between the original or unauthorized. Finally, it shows using the both DT and UBP mechanism together for the analysis which gives more accurate results with the simulation in the VANET security system.

In Ref. [18], the authors gave a brief review of using cloud computing in VANETs for the communication between the vehicles and sharing the information in real-time by generating the virtual cloud servers on each vehicle node. In this paper, the comparative analysis on a different protocol such as (AODV, DSDV, DSR) for the transmission of the messages between the vehicle node is given and analysed which protocol is the best for the transmission in the cloud. Then the author explained the recent advancement in the VCC for the communication in VANET.

The Vehicular cloud computing providing the various application in VANET such as customized and infinite storage space, distributed computing and timely tracking of the traffic services. In Ref. [19], the author proposed a mechanism call Message Recovery Signature (MSR) for the traffic data aggregation. This mechanism helps in securing the VANET security property such as Availability, confidentiality, the integrity of the information processing in the VANET system. The comparative analyses by simulating in GMP and PBC provides the proposed scheme provide the cost less computational time than any other scheme. Hence the suggested scheme can be used in the vehicular cloud to aggregate the traffic data to provide additional traffic services.

To approximate the job completion time for the transmission of the packages in VANETs using the vehicular cloud, authors in Ref. [20] proposed a method which calculates and estimate the time required to complete one job per transmission. The simulation is done by creating the three-lane highway with Access points (APs) placed every 2000 meters. Each Aps has a coverage area of 200 meters. The five-parameter logistic speed density function is used to determine the vehicular speed and gives the average processing time about 20 to 30 minutes. Finally, the maximum relative error is less than 0.24%, with an average of 0.05% for uniform distributed job duration, and less than 1.96%, with an average of 0.1% for the exponential distribution.

III. Proposed method and Comparative Analysis

A. Comparative analysis of the existing methods

In this section, the summarization of section III is showed in Table 1, and also discussed and analysed of recent literature reviews in the VANET Security fields.

From Table 1, we can see that the different solution provides for detecting and preventing the various security attacks, mainly DDOS attacks and Sybil attack in VNAET system. Then analysed the accuracy given by each method prosed by authors. Most of the uses the Machin learning algorithm to detect DDOS and Designed their own framework to detect the Sybil attack. Simulation is done by using the Simulation of Urban Mobility (SUMO) and NS3/2 and also OMNET++ for the traffic simulation.

B. Proposed method: Best Reliable Rooting Protocol for the transmission process in VANET.

To continue further work on detecting and preventing the DDOS attack and Sybil attack using the Vehicular cloud computing (VCC), the best reliable routing protocol is required for the transmission in the real-world scenario. To achieve that, we have implemented system which generates the real-world scenario by selecting the specified area from the OpenStreetMap Framework. where number of vehicles, Trucks, Traffic Signals and pedestrians were selected. Then, we analysed the generated scenario in Urban simulator called SUMO.

After that, by using SUMO a Mobilty.tcl file was generated to analyse the communication between the nodes by using the four different routing protocol such as (Ad hoc On-Demand Distance Vector) AODV, Dynamic Source Routing (DSR), Destination-Sequenced Distance-Vector DSDV, Optimized Link State Routing Protocol (OLSR) with the Network Simulator NS3. The four-routing protocol was used for the transmission between the nodes and recorded the obtained results for each protocol which has the parameters such as Throughput, source node address, destination node address etc. Finally, we have done the graphical analysis on the obtained result over the simulation duration. For the given simulation duration, the DSR protocol was giving the high throughput and less network over head in VANET communication system as shown in the Fig.2. We are considering the DSR protocol for the further work on the Detecting and preventing the Security attacks in VANET by using VCC.

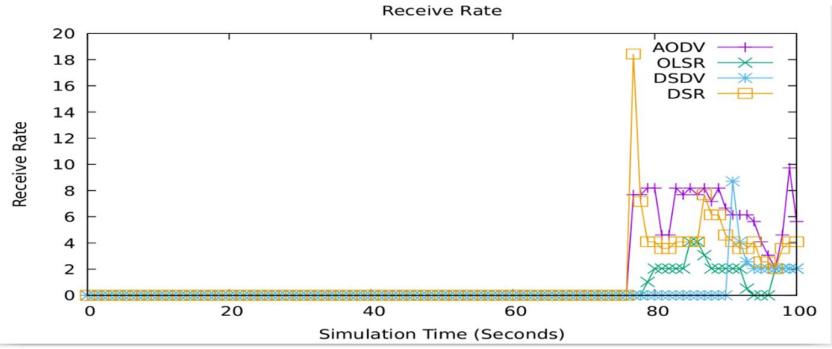

Figure 2. DSR routing protocol gives the good throughput than other protocol

TABLE I. SOLUTIONS FOR DETECTING AND PREVENTING SECURITY ATTACKS IN VANET

Reference No and Year	Proposed Method	Security Attacks	Detection (D) /Prevention (P) of Attacks		Simulation Tools Used	Accuracy
			D	P		
[3] 2019	MMNDA	DDOS and Sybil attacks	Y	Y	NS-2	Improved Version
[4] 2019	Algorithm	Malicious node	Y	N	NS2	95%
[6] 2018	Sentinel	DDOS	Y	Y	SUMO, OOMNET++, VEINs, net convert.	78%
[7] 2019	Spark-ML RF-Based	DDOS	Y	N	SPARK	99.95%
[8] 2018	Congestion Algorithm	DDOS	Y	Y	NS2	85%
[9] 2018	Framework	Real-Time DDOS	Y	Y	SUMO, OMNET++, Veins	99%
[10] 2018	MVSA	DDOS	Y	Y	NS2	>90% and the Error rate is 10%
[11] 2018	SVM-ML	DDOS	Y	Y	Floodlight	>97%
[12] 2018	RSU Chain Stamp	Sybil Attack	Y	N	N/A	80%
[13] 2019	RSSI sequence and driving matrix	Sybil Attacks	Y	N	SUMO, OMNET++, Veins	>90%
[14] 2019	Hash Function	Sybil Attacks	Y	Y	NS-3	N/A
[15] 2018	RSU-ID Based	Sybil Attacks	Y	N	SUMO, NS3, MATLAB	Near 100%

IV. CONCLUSION AND FUTURE WORK

This report highlights how the VANET environment can be improved by improving the driving experience, navigation services, road safety and other roadside services. Due to the characteristics of the VANET system and its architecture, VANET is vulnerable to many security attacks. There is a need to develop security solutions in the VANET environment. Many previous security efforts have applied the same old traditional security solutions without considering any special aspects of VANETs. We have studied the security challenges faced by VANETs and their architecture for our literature, which have helped us to come up with this solution to detect and prevent DDoS.

All recent studies in this field focus more on DDoS and Sybil attacks, such as how to detect and prevent them, from the security point of view of VANET. In addition, the report provides various security solutions for various attacks in VANETs using machine learning capable of detecting patterns in attacks. As part of our future work, we create an environment by using simulation tools that help us produce datasets that are greater than general and public datasets by using VCC (Vehicular Cloud Computing). By using this dataset, we can

create a real-time context that lets us detect threats. We put forward to provide a solution for detecting and prevent DDoS attacks in VANET along with its prevention rate, detection rate and its own design.

REFERENCES

[1] Zhao Jun Lu, Gang Qu, Senior Member, IEEE, and Zhenglin Liu, "A Survey on Recent Advances in Vehicular Network Security, Trust, and Privacy," TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS 2018.

[2] Nice Mathew, V. Uma, "VANET Security -Analysis and survey," International Conference on Control, Power, Communication and Computing Technologies (ICCPCT), 2018.

[3] Sushil Kumar, Kulwinder Sing Mann, "Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs," International Conference on Automation, Computational and Technology Management (ICACTM) Amity University 2019.

[4] Jeevitha R, N. Sudha Bhuvaneswari "Malicious node detection in VANET Session Hijacking Attack," ICECCT.2019.8869452 IEEE 2019.

[5] Mohammad Syfullah, Joanne Mun-Yee Lim, "Data Broadcasting on Cloud-VANET for IEEE 802.11p and LTE Hybrid VANET Architectures," 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017.

[6] Gabriel de Biasi, Luiz F. M. Vieira, Antonio A. F. Loureiro, "Sentinel: Defense Mechanism against DDoS Flooding Attack in Software Defined Vehicular Network," IEEE 2018.

[7] YING GAO, HONGRUI WU, BENJIE SONG, YAQIA JIN, XIONGWEN LUO, XING ZENG, "A Distributed Network Intrusion Detection System for DDoS Detection in VANET," VOLUME 4, 2019.

[8] Charu Guleria, Harsh Kumar Verma. "Improved Detection and Mitigation of DDoS Attack in Vehicular ad hoc Network," 4th International Conference on Computing Communication and Automation (ICCCA) 2018.

[9] A. Haidari, "Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems," no. September 2018.

[10] R. Kandasamy et al., "A Multivariant Stream Analysis Approach to Detect and Mitigate DDoS Attacks in Vehicular Ad Hoc Networks," vol. 2018, 2018.

[11] Y. A. O. Yu, L. E. I. Guo, Y. E. Liu, J. Zheng, and Y. U. E. Zong, "An Efficient SDN-Based DDoS Attack Detection and Rapid Response Platform in Vehicular Networks," IEEE Access, vol. 6, pp. 44570–44579, 2018.

[12] Mukesh Soni, Anuj Jain, "Secure Communication and Implementation Technique for Sybil Attack in Vehicular Ad-Hoc Networks," Proceedings of the Second International Conference on Computing Methodologies and Communication (ICCMC 2018) IEEE Conference Record # 42656; IEEE Xplore ISBN:978-1-5386-3452-3.

[13] Wei Li, Dongmei Zhang, "RSSI Sequence and Vehicle Driving Matrix Based Sybil Nodes Detection in VANET," 11th International Conference on Communication Software and Networks, 2019.

[14] Salman Ali Syed, B.V.V.S Prasad, "Merged technique to prevent SYBIL Attacks in VANETs," IEEE 2019.

[15] Hamid Hamed, Shapour Golbahar Haghighi, "Sybil Attack Detection in Urban VANETs Based on RSU Support," 26th Iranian Conference on Electrical Engineering (ICEE2018).

[16] Bilal Ahmed, Asad Waqar Malik, Taimur Hafeez and Nadeem Ahmed, "Services and simulation frameworks for vehicular cloud computing: a contemporary survey," EURASIP Journal on Wireless Communications and Networking (2019).

[17] Mhidi Bousselham, Nabil Benamar, Adnane Addaim "A new Security Mechanism for Vehicular Cloud Computing Using Fog Computing System," 2019.

[18] Netra k. G. Manjunath, Achyut Shankar "An effective Vehicular Ad hoc Network using Cloud Computing: A Review," 2019.

[19] Jian Shen, Dengzhi Liu, Xiaofeng Chen, Jin Li, Neeraj Kumar, Pandi Vijayakumar "Secure Real-time Traffic Data Aggregation with Batch Verification for Vehicular Cloud in VANETs," 2019.

[20] Aida Ghazi Zadeh, Puya Ghazi Zadeh, Ravi Mukkamala and Stephan Olariu, "Towards Approximating Expected Job Completion Time in Dynamic Vehicular Clouds," 12th International Conference on Cloud Computing (CLOUD) 2019.