DOI: https://doi.org/10.57233/ijsgs.v10i2.673 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 10 (2) WEBSITE: https://fugus-ijsgs.com.ng

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY
(A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA)

An Enhanced Timestamp-Based Security Mechanism to Detect Sybil Attack in vehicle ad hock network (VANETs)

[*1]Aliyu Abdullahi, [2]UMar Iliyasu, [3]Yusuf Surajo

[*1]Computer Science Department, Umaru Musa Yaradua University, Katsina, Nigeria
[2.3]Computer Science Department, Federal University Dutsin-ma, Katsina, Nigeria

Corresponding Author's Email: aaboko007@gmail.com

Received on: April, 2024 **Revised and Accepted on:** May, 2024 **Published on:** July, 2024

ABSTRACT

Within the VANET subset of Mobile Ad-hoc Network (MANET), automobiles can communicate with one another via roadside infrastructure or vehicle-to-vehicle communication. However, because nodes move around and topologies might alter at random, there could be a potential of attacks in a VANET. One well-known attack is the Sybil attack, in which the attacker assumes many wrong identities to interfere with the VANET's ability to function. Numerous solutions have been put forth in the literature to identify Sybil attacks. The authors of the recent work have developed a timestamp-based Sybil node discovery method. Every vehicle on the road in VANET is given a unique certificate by RSU, which is included in this work timestamp. We applied the Ad-hoc On-Demand Distance Vector (AODV) Routing protocol and timestamp as a hash function of the public key with addition of the speed of the vehicle in the planned work for node detection and data transmission. In addition, we used the NS2 simulator for Sybil node detection.

Keywords: VANETs, V2V, V2I, Sybil Attack, AODV.

1.0 INTRODUCTION

Researchers and academics are becoming increasingly interested in VANET due to the current developments in network topologies and trends. Through vehicle-to-vehicle communication, the Vehicular Ad-hoc Network (VANET), a variation of the Mobile Ad-hoc Network, can increase traveler protection. While VANET establishes and facilitates communication between moving vehicles, Mobile Ad-hoc Networks (MANET) allow connection between standby devices, which either move slowly or not at all.

Equally, the VANET creates and maintains the connection between fast-moving cars, based on the IEEE 802.11p standard, nodes are cars that communicate in the vehicular domain utilizing the dedicated short-range communication (DSRC) protocol. In VANET, (Velayudhan *et al*., 2020), physical infrastructure is not required to connect cars.

Users of VANETs can enjoy entertainment services like playing audio and video. People's safety and security are at risk from certain security hazards. Because the nodes in a VANET move in and out of range so frequently and quickly, it is challenging to establish a reliable end-to-end communication link in their highly dynamic environment. Another significant worry is how long it takes for messages to arrive on the VANET. Data dissemination security in VANET is crucial since any roadside event could have catastrophic consequences. (Chaubey *et al*., 2020, Rashid *et al*., 2018). Wherein VANET developers deal with several difficulties.

These difficulties can range from picking the best architecture to establish a stable VANET connection. Two other major difficulties are data integrity and protecting against new security threats. In a Sybil attack, the attacker can adopt multiple identities and fabricate the appearance of traffic jams.

The goal of the VANET system is to provide a platform for a range of services that can enhance the efficiency and safety of passengers as well as infotainment, driving assistance, transportation regulation, etc. VANET needs precise and timely (no delay) data transfer to offer these services. Vehicles (mobile nodes) and a few steady adjacent Road Side Units (RSU) exchange information. Vehicles within the vicinity of 100–500 meter are connected by VANET; if a vehicle is outside of the vicinity, it cannot connect to other vehicles. Mostly VANET supports two types of communication which are:

1.1 Vehicle-to-Vehicle (V2V)

In this vehicle establishes a self-network and does not require any infrastructure for communication. This network can cover a distance of up to 500 meters from the initiator vehicle's location. Within that range, a vehicle can use an On Board Unit (OBU) to establish a connection with other cars on the network without

making use of VANET's features. Vehicles exchange information about malevolent vehicles, safety messages, and vehicle IDs in V2V communication. On the other hand, Road Side Unit (RSU)-based prepared infrastructure is entirely dependent on Vehicle-to-Infrastructure.

1.2 Vehicle-to-Infrastructure (V2I)

RSUs can communicate with vehicles via V2I communication, sending messages about network management, road conditions, hotels nearby, and internet availability.

Because vehicles pass across VANETs so quickly, there is a high degree of vehicle connection and disengagement, which causes topologies to constantly change. As topologies change, attackers have a perfect opportunity to launch a network attack. As a result, security is also a top priority for VANET; it is essential to identify and mitigate attack possibilities.

Since VANET is a wireless network, it is subject to all wireless network protection risks. Since there is a lot of vehicle movement in VANETs, which means that in order to maintain effective communication, vehicles constantly swapping topologies. This increases the risk of attack during handoffs.

1.3 Aim of the Research Work

This research work aims to develop an Enhanced Timestamp-Based Security Mechanism to Detect Sybil Attacks in vehicular ad-hock networks (VANETs)

2.0 RELATED WORK

Many researchers have examined the impact of security attacks on VANET routing protocols and provided their findings about Sybil attack detection, given the susceptibility of VANET's architecture to security attacks. This section reviews and analyzes recent malicious detection systems created by various authors, with an emphasis on the Sybil raid exploration and avoidance mechanism in VANET.

According to (Cong Pu *et al*., 2022), Routing conventions are critical to communication and information delivery in an Internet of Things (IoT) system. For systems and devices connected to the Internet of Things, RPL is a popular routing protocol. However, RPL's security measures are retrospective and do not meet the demands of the complex cyber threat landscape of the present day. First, we focus on Sybil attack discovery in RPL-based IoT and present a lightweight Bloom filter and physical unclonable function (PUF) based Sybil attack discovery technique, called liteSAD. Our approach aims to lower memory consumption and discovery delay without sacrificing detection accuracy. (Cong Pu *et al*., 2022).

In wireless sensor networks (WSNs), one of the primary security challenges is the detection of Sybil attacks. Since an attacker can create numerous phony identities with fraudulent messages to seriously disrupt WSN regular operations, the attack is regarded as one of the riskier dangers. This paper suggests a unique Sybil attack detection technique called CPPR, which is based on the management of transmission power at the sensor nodes and the wireless channel profile. The physical layer improvements at the sensor nodes can help the suggested CPPR mechanism control transmission power, preventing numerous attacks and preserving a high detection ratio. (Reham, *et al*., 2022).

Presented privacy-preserving detection, which eliminates the need for vehicles to provide their information on the infrastructure. Rather than assigning a single unique identity to every vehicle, each vehicle has its own unique alias pool, with all aliases within the same pool hashing to the same value. A car can therefore conceal its identity by using any alias in its pool. (Zhou *et al*., 2020).

A hostile car in a VANET may spread false communications about road traffic, an accident ahead, a route limit, and other things, according to (Mustafa *et al*., 2022). This could force the driver to turn off course and put him at risk of an unfortunate event. VANET has displayed many problems. The accessible technologies for security services and the associated processing algorithms. The issues raised by the Sybil attack on VANET technology are covered in this article. (Mustafa, *et al*., 2022).

(Grover *et al*., 2013) developed and executed a variety of forging attacks. The percentage of delivered packets, number of collisions, and speed of the vehicles were used to analyze the attacks. Rana and associates. PKI for message authentication, integrity, and privacy was modified by (Hubaux *et al*., in 2007). A special signature technique maintains a coordination-based method for vehicle security and information flow in a dynamic network. (Daeinabi *et al*., 2014; Grover *et al*., 2013) detected and identified the Sybil node using a neighborhood list. This system states that a malicious node will be recognized as a Sybil node if an adjacent node has been detecting it for an extended period of time. The drawback of this plan, though, was how time-consuming and intricate it was. (Hubaux *et al*., 2004) conducted a survey on the unicast, multicast, geo-cast, mob-cast, and broadcast protocols for VANETs. For

DOI: https://doi.org/10.57233/ijsgs.v10i2.673 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL. 10 (2) WEBSITE: https://fugus-ijsgs.com.ng

VANET, a navigation-based system is suggested to provide drivers with real-time advice. According to (Chim *et al*., 2014), the technique helps calculate a better path in actual road-based scenarios. (Authors Sharma *et al*., 2016) suggested a system concept that leverages an effective certificate creation technique to recognize and isolate the Sybil nodes (Authors Khabazian *et al*. 2013) analyzed how automobiles in the VANET communicated over RSU using central servers and roadside servers. V2V or V2R communications are possible.

A shared key management technique was proposed by (Samara *et al*., 2010) and has advantages over distributed key management systems. Without the need for an RSU, the cars in this architecture may immediately link to one another. RSU is the one who transmits the messages. The Emergency Electronic Brake Light System was introduced by authors (Faezipour *et al*., 2012). It uses vehicle-to-vehicle (V2V) communication to spread alert messages to vehicles on the road regarding weather conditions. The authors (Faezipour *et al*., 2012) suggested a distributed and localized method for locating Sybil nodes on roadways. Two techniques were suggested for signal strength-based position verification and Sybil attack detection. The suggested scheme was analyzed through simulation. A Sybil node identification approach employing electroacoustic location and context-aware switching methodology has been proposed by authors (Han *et al*., 2017). To examine the accuracy of the suggested strategy, a simulation has been performed. To identify Sybil attacks in indoor and urban environments, authors (Xiao *et al*., 2009) presented a physical layer authentication technique. A hypothesis was put forth to identify the Sybil nodes in wireless systems, including broadband and narrowband. The network analyzer tool was used to illustrate the performance.

3.0 AN ENHANCED TIMESTAMP-BASED SECURITY MECHANISM (ETBASM)

Sybil attack detection is the main objective of the An Enhanced Timestamp-Based Security Mechanism to Detect Sybil Attacks in vehicle ad hock network (VANETs) (ETBASM). The suggested method strengthens security in VANETs by using the AODV routing protocol to validate the vehicles' identifying number, status, security key, and speed.

This study examines the Ad Hoc On-Demand Distance Vector (AODV), a sensitive routing system integrated into the NS-2 simulator. Using the NS2 simulation tool in the AODV routing protocol, an upgraded security mechanism was created for vehicle networks in various circumstances.

Time stamps are unique certificates that are issued by Road Side Units (RSU) to all vehicles on the road who want to use VANET advantages. Here, we assume that time stamps are a hash function of public keys, and for security reasons, only RSU has the authority to generate and assign time stamps to requesting vehicles. This is the manner in which the proposed algorithm uses timestamp mechanism for detecting the presence of Sybil vehicles in VANET.

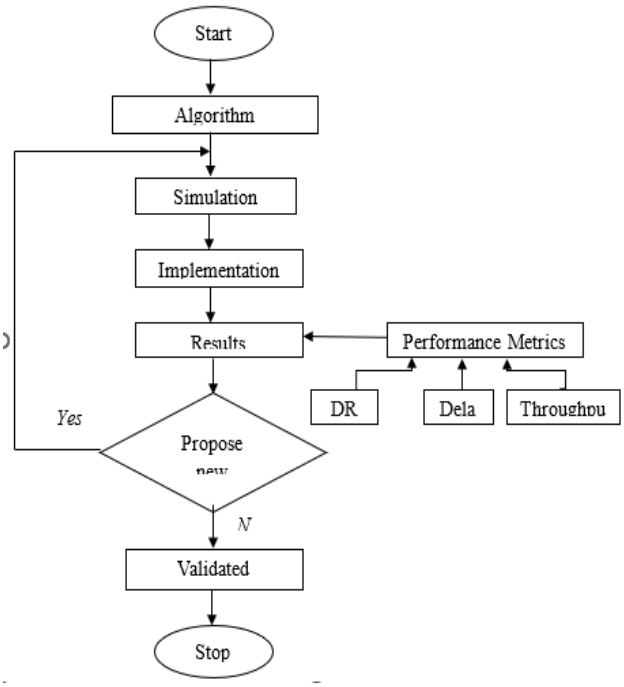


Figure 1: Flow Chat of ETBASM

Table 1: ETBASM Algorithm Parameters

Parameters	Definition
Pk_i	Public Key of Vehicle *i*
V_{est}	Estimated speed of the vehicle
Neighbours	List of Neighbours
A	Constant of fluid area
B	First constant of congested area
d_c	Critical density
d_{max}	Maximal density
C	Second constant of congested area
Length	Length of the r o a d
Density	Current density
Flow	Traffic flow of the Vehicle
RV (id)	Registered vehicleid

DOI: https://doi.org/10.57233/ijsgs.v10i2.673 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL. 10 (2) WEBSITE: https://fugus-ijsgs.com.ng

V_{real}	Real Speed of the vehicle
RSU	Road Side Unit

Pk (i) in the flowchart denotes the vehicle's identifying number that is sent to RSU for it to join the network by sending a Hello message. Next, *Pk (i)* will be verified by RSU via the Certification Authority (CA). Should the CA transmit an acknowledgment (ACK) to RSU, RSU will calculate the discrepancy between the vehicle's actual speed (*Vreal*) and its predicted speed *(Vest)*. The RSU will create and send a time stamp to the vehicle and allow communications if the value did not beyond the threshold speed *(Vth)*. However, RSU will not issue a time stamp and block the request if CA provides Negative Acknowledgment (NACK) to RSU or if the vehicle's actual speed *(Vreal)* differs from its projected speed *(Vest)* by greater than the threshold speed *(Vth)*.
The proposed system has the following assumptions:

1. A registered distinct public key is provided to each car by the Certification Authority (CA), and distributes a distinct public key to manufacturers, who then allocate these keys to vehicles, hard-coding them into the vehicles' communication devices.
2. It is difficult that a vehicles cross a several RSU at similar time.

Since VANET is a secure network, automobiles are not permitted to access VANET services without proper authentication and verification. When a vehicle enters the VANET environment, it transmits its public key (Pki) to RSU for the purpose of initial authentication.

RSU uses Certification Authority (CA) public key authentication: Since all keys provided for automobiles are listed with the Certification Authority. The difference between the vehicle's actual speed *(Vreal)* and its predicted speed *(Vest)* will be calculated by RSU if the Certification Authority issues an acknowledgment (ACK) to RSU. RSU will create a timestamp (a hash function of the requested vehicle public key) and issue one to the car if the value is less than the threshold speed *(Vth)*. On the other hand, RSU will not issue a Time Stamp and will not block the request for a set amount of time if the Certification Authority issues a Negative Acknowledgment (NACK) to RSU, or if the difference between the vehicle's real speed *(Vreal)* and its estimated speed *(Vest)* exceeds the threshold speed *(Vth)*. However, if RSU consistently receives request messages from the same public key, it will mark the requesting public key as suspicious, generate an alert message, and broadcast that public key as suspected.

Cars obtain a license to use VANET services and connect with other cars as soon as they obtain a Time Stamp from RSU. VANET cars must update the hop count and add their own time stamp to message packets in order to communicate.

Upon receiving the request packet, the vehicle searches through its routing table for the destination. If the destination is found, it responds; if not, it updates its timestamp and public key in the message packet, reduces the hop count, and sends the packet out into the network. The destination vehicle immediately returns the message to the source vehicle and adds its timestamp to the message packet after locating the destination. The table of timestamps associated with each public key is maintained exclusively by RSU by mapping the public key of the requesting vehicle. RSU will search for its table of timestamps allocated to each public key as indicated in Table 2 as soon as it receives the public key and time stamp from the source vehicle.

Table 2: List of Assigned Timestamp

SN	Public Key	Timestamp (hash function of Public key)
1	ck1213n	dkjj1152cmwchb
2	zzaj132	bbdcdc55155njd
3	……	……

The suggested method takes into account both internal and external Sybil attacks on the vehicle network. The identity number, status, security key, and speed value are established in an unambiguous manner below the threshold value of a registered vehicle. Initially, registered cars contacted the RSU with a Hello message to join the network. Considering the automobiles' identification number, status, security key, threshold value, and timestamp, the algorithm verifies that they are real. The NS2 simulator and the AODV routing protocol were used to implement ETBASM.

Algorithm: ETBASM Algorithm

Input: *Pk (id), Sec_key (id), RV (id), STV(id),* $V_{real}, V_{est}, V_{th}$

Output: Allow communication (accept) or Block Sybil attack

DOI: https://doi.org/10.57233/ijsgs.v10i2.673 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL. 10 (2) WEBSITE: https://fugus-ijsgs.com.ng

Step1: Vehicles registration on RSU

Step 2:*V(id)* communicatesto RSU with "*Hello Message*"

RSU ask to send *Pk (id)*security key and *V(id)* send *Pk (id)* to RSU

Step3:If(*Pk (id)* = = *RV (id))***Then**

RSU request for $V_{real}(id)$and *V(id)* send V_{real} to RSU

If ($|V_{real}(id) - V_{est}| < V_{th}$) **Then**
Generate and assign Timestamp to the VehicleV(id) &
Allow V(id) to communicate

else

Vehicle is detected as Sybil vehicle

end if

else

Vehicle is detected as Sybil vehicle

end if

Step4:If V(id) = = detected as Sybil vehicle **Then**

Add_To_Attacker_List(V(id));

Remove_Attacker(V(id));

end if

Figure 2: ETBASM Algorithm

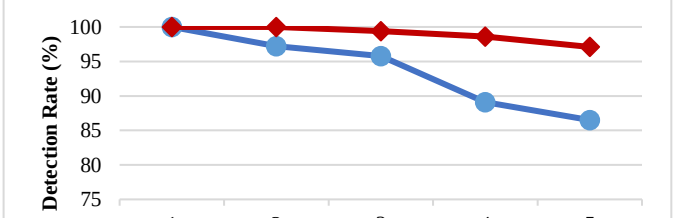
4.0 RESULTS AND DISCUSSION

The simulation experiment was conducted to validate the effectiveness of the ETBASM algorithm, the Analysis was conducted to compare the performance of the proposed Enhanced Timestamp-Based Security Mechanism (ETBASM) with one of the recently proposed Security Mechanism to Detect Sybil Attack in VANETs (TBASM) (Faisal and Zaidi, 2020). Analysis conducted by (Faisal and Zaidi, 2020) revealed that TBASM performs better than existing AODV protocols for detecting Sybil attacks in VANET, therefore in this work the performance of ETBASM is compared with that of TBASM.

The performance metrics used for the evaluation of the proposed ETBASM and TBASM are: **(1) Detection Rate (DR)**, represents the percentage of malevolent vehicles properly identified as hateful to the total number of illegitimate vehicles. **(2) Throughput,** is the numeral of successfully received packets per unit time and it is usually measured in bits per second (*bps*), Kilobit per second (*Kbps*), Megabit per second (*Mbps*), Gigabit per second (*Gbps*), and so on. **(3) Delay**, refers to the amount of time it takes for a packet to travel from one communication endpoint to another and it is usually measured in fractions of seconds such as milliseconds (*ms*), microseconds (μs) and so on. These measurements are used to compare the vehicular network's performance both with and without the Sybil attack in terms of detection rate. During the simulation, the results have been analyzed using 5, 10, 15, 20 and 30 mobile nodes.

4.1 Detection Rate (DR) Comparison Of ETBASM And TBASM

The results presented in Figure 3 and Table 3 show that, detection rate of ETBASM is higher than TBASM when the number of Sybil attackers increases. This is because RSU in ETBASM is using estimation speed from macroscopic traffic Model-based scheme that enable it to detect more Sybil attackers. However, both ETBASM and TBASM show a lower decrease in detection rate when the number of Sybil attackers increases; this is due to the fact that as there are more cars on the network—both legal and illegal—the amount of packets they exchange rises correspondingly. Due to packet collisions and a drop in detection rate, this leads to information loss.



DOI: https://doi.org/10.57233/ijsgs.v10i2.673 ISSNp: 2488-9229; ISSNe: 3027-1118
IJSGS FUGUSAU VOL. 10 (2) WEBSITE: https://fugus-ijsgs.com.ng

Figure 3: Detection Rate Comparison of ETBASM AND TBASM

Table 3: Detection Rate Comparison of ETBASM AND TBASM

Number of Sybil Attackers	Detection Rate (%)	
	TBASM	ETBASM
1	100	100
2	97.2	100
3	95.8	99.4
4	89.1	98.6
5	86.5	97.1
Average	**93.72%**	**99.1%**

4.2 Throughput Comparison of TBASM And ETBASM

Variations in network topology, scarce network resources, and vehicle speed all impact throughput. A malevolent danger that compromises communication dependability is present along with additional variables that negatively impact throughput. When the number of vehicles in the network increases, ETBASM's throughput surpasses TBASM's, according to an analysis of the throughput shown in Fig. 4 and Table 4.

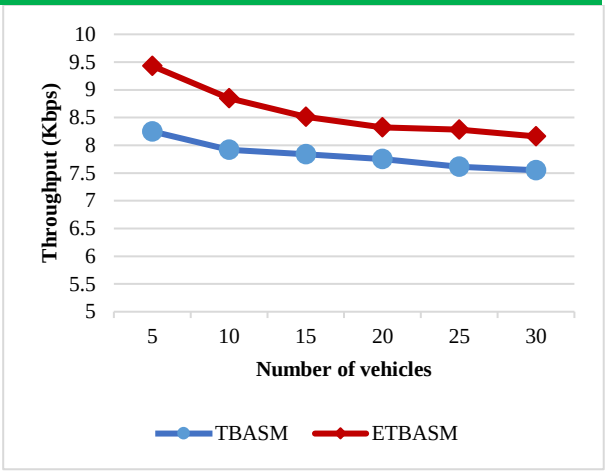


Figure 4: Throughput Comparison of ETBASM and TBASM

Table 4: Throughput Comparison of ETBASM and TBASM

Number of Vehicles	Throughput (Kbps)	
	TBASM	ETBASM
5	8.25	9.43
10	7.92	8.85
15	7.84	8.51
20	7.75	8.32
25	7.61	8.28
30	7.55	8.16
Average	**7.82**	**8.59**

4.3 Delay Comparison Of TBASM and ETBASM

Results presented in Figure 5 and Table 5, show the delay of TBASM AND ETBASM, it can be observed from the graph that the delay of ETBASM is higher than that of TBASM, this is because ETBASM performs additional computation for estimation speed using Macroscopic Traffic Model-Based approach, as such it affects the overall delay encountered by the packets.

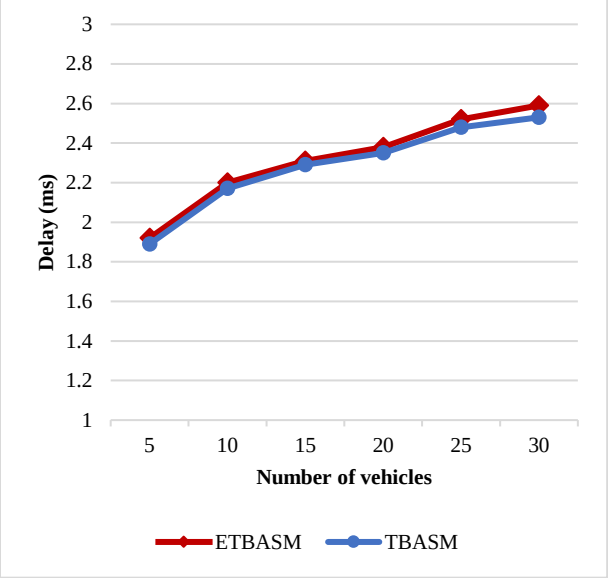


Figure 5: Delay Comparison of ETBASM and TBASM

Table 5: Delay Comparison of ETBASM and TBASM

Number of Vehicles	Delay (ms)	
	TBASM	ETBASM
5	1.89	1.92
10	2.17	2.2
15	2.29	2.31
20	2.35	2.38
25	2.48	2.52
30	2.53	2.59
Average	**2.29**	**2.32**

5. CONCLUSION

In this paper, an enhancement for detection of Sybil attack has been conducted. And detection rate, throughput, and delay comparisons of ETBASM and TBASM algorithms are presented. In VANETs, Sybil attackers can assume the identities of other vehicles and utilize them to further their objectives. Mobility is essential for accurately simulating VANETs. In further research, we will examine methods to identify the attacks that have been provided.

REFERENCES

Daeinabi A., Rahbar A. G. (2014) "An advanced security scheme based on clustering and key distribution in Vehicular ad-hoc networks," Journal of Computers & Electrical Engineering, vol. 40, no. 2, pp. 517{529, Feb. 2014. https://doi.org/10.1016/j.compeleceng.2013.10.003

Sharma A. K., Saroj S. K., Chauhan S. K., & Saini S. K. (2016) "Sybil attack prevention and detection in vehicular ad hoc network," in International Conference on Computing, Communication and Automation (ICCCA'16), pp. 594-599, ISBN: 978-1-5090-1666-2/16/$31.00 ©2016 IEEE

Asma Parveen (2020) "VANET's Security, Privacy and Authenticity: A Study" Proceedings of the First International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISET 2020, 16-17 May 2020, Chennai, Indiahttp://dx.doi.org/10.4108/eai.16-5-2020.2304038

Azeem Irshad (2022) "Security Hardened and Privacy Preserved Vehicle-to-Everything (V2X) Communication" Hindawi, Security, and Communication Networks Volume 2022, Article. Pages https://doi.org/10.1155/2022/9865621

Chien-Ming Chen, Shuangshuang Liu (2021) "Improved Secure and Lightweight Authentication Scheme for Next-Generation IoT Infrastructure" Hindawi Security and Communication Networks Volume 2021, Article ID 6537678, 13 pages, https://doi.org/10.1155/2021/6537678.

Samara G., Al-Salihy W. A. H., Sures R. (2010) "Efficient certificate management in VANET," The 2nd International Conference on Future Computer and Communication, vol. 3, pp. 750-754, 2010. 10.1109/ICFCC.2010.5497419

Grover J., Laxmi V., M. S. (2013) "Attack models and infrastructure support detection mechanism for position forging attack in vehicular ad hoc networks," CSI Conference Transactions on ICT, vol. 1, no. 3, pp. 261{279, Sep. 2013. 10.1007/s40012-013-0025-1

Hubaux J. P., Luo J., Capkun S. (2004) "The security and privacy of smart vehicles," IEEE International Conference on Security & Privacy. vol. 2, no. 3, pp. 49-55, 2004. 10.1109/MSP.2004.26

Xiao L., Greenstein L. J., Mandayam N. B., & Trappe W. (2009) "Channel-based detection of Sybil attacks in wireless networks," IEEE International Conference on Information Forensics and Security, vol. 4, no. 3, pp. 492-503, Sep. 2009. 10.1109/TIFS.2009.2026454

Al-shareeda M. A., Anbar M., Hasbullah I. H., Manickam S., Abdullah N., & Hamdi M. M. (2020) "Review of prevention schemes for replay attack in vehicular ad hoc networks (vanets)," in 2020 IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), 2020, pp. 394-398: IEEE. 10.1109/ICICSP50920.2020.9232047

M. A. Jubair, (2019) "Bat optimized link state routing protocol for energy-aware mobile ad-hoc networks," Symmetry, vol. 11, no. 11, p. 1409, 2019. https://doi,org/10.1007/978-981-99-1410-4.

Faezipour M., Nourani M., Saeed A., & Addepalli S. (2012) "Progress and challenges in intelligent vehicle area networks," Journal of Communications ACM, vol. 55, no. 2, pp. 90{100, Feb. 2012. 10.1145/2076450.2076470

Hamdi M., Audah L., Rashid S., Mustafa A., Sameer A., & Abood M. (2020) "An Overview on Quality of Service and Data Dissemination in VANETs" International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). 10.1109/HORA49412.2020.9152828

Inam M., Li Z., Ali A., Zahoor A. (2019) "A novel protocol for vehicle cluster formation and vehicle head selection in vehicular ad-hoc networks", International Journal of Electronics and Information Engineering, vol. 10, no. 2, pp. 103{119, 2019. 10.6636/IJEIE.201906 10(2).05)

Khabazian M., Aissa S., Mehmat-Ali M. (2013) "Performance model of safety message broadcast in vehicular ad hoc network," IEEE International Conference on Intelligent Transportation Systems, vol. 14, no. 1, pp. 380{387, Mar. 2013. 10.1109/TITS.2012.2213595

Hamdi M. M., Audah L., Rashid S. A., & Al-shareeda M. A. (2020) "Techniques of Early Incident Detection and Traffic Monitoring Centre in VANETs: A Review," Journal of Communications, vol. 15, no. 12, 2020. 10.12720/jcm.15.12.896-904.

Zhou M., Han L., Lu H., & Fu C. (2020) "Distributed collaborative intrusion detection system for vehicular Ad Hoc networks based on invariant," Elsevier, vol. 172, p. 107174, 2020. https://doi.org/10.1016/j.comnet.2020.107174

Mohamed Riadh Kadri, Abdelkrim Abdelli, Jalel Ben Othman, & Lynda Mokdad (2023) "Survey and classification of Dos and DDos attack detection and validation approaches for IoT environments" Elsevier B.V. https://doi.org/10.1016/j.iot.2023.101021

Mourade Azrour, Jamal Mabrouki, and Rajasekhar Chaganti (2021) "New Efficient and Secured Authentication Protocol for Remote Healthcare Systems in Cloud-IoT" Hindawi Security and Communication Networks. https://doi.org/10.1155/2021/5546334

Velayudhan N. C., Anitha A. (2020), "Sybil Attack in VANET Operating in an Urban Environment: An Overview," SPRINGER on Advances in Communication Systems and Networks, pp. 433-442, 2020. 981153991X

Chaubey N. K., Yadav D. (2020) "A taxonomy of Sybil attacks in vehicular ad-hoc network (VANET)," in IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks: Journal of International Academy Publisher IGI Global, 2020, pp. 174- 190. DOI: 10.4018/978-1-7998-2570-8.ch009

Reham Almesaeed, Eman Al-Salem (2022) "Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks" Springer, Original Paper Published: 06 January 2022. https://doi.org/10.1007/s11276-021-02871-0

Rashid S. A., Hamdi M. M., Alani S. (2020) "An overview on quality of service and data dissemination in VANETs," in 2020 International Congress on Human-Computer Interaction,Optimization and Robotic Applications (HORA),2020, pp. 1-5: IEEE. 10.1109/HORA49412.2020.9152828

Sami Abduljabbar Rashid, Lukman Audah, Mustafa Maad Hamdi, and Sameer Alani (2020), "Prediction Based Efficient Multi-hop Clustering Approach with Adaptive Relay Node Selection for VANET" Journal of Communications Vol. 15, No. 4, April 2020. 10.12720/jcm.15.4.332-344

Sandeep N. Kugali and Sneha Kadadevar (2020). "Vehicular ADHOC Network (VANET):-A Brief Knowledge" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181Vol. 9 Issue 06, June-2020 ICASISET 2020, May 16-17, Chennai, India Copyright © 2021 EAI DOI 10.4108/eai.16-5-2020.2304038.

Sayed A. Nouh, Manal S. Gamal, Abdurrahman A. Nasr, (2020), "VANET Security: Defense and Detection, a Review" Journal of Al-Azhar University Engineering Sector Vol.15, No. 56, July, 2020, 810-827. DOI: 10.21608/auej.2020.103823

Shambel Tseggaye Getaneh (2019) "Enhanced Security Mechanism to Detect Sybil Attacks in VANETs". A Thesis Paper Submitted to Department of Information Technology in Partial Fulfillment of the Requirements of the Degree of Master of Science in Computer Networks and Security.

Syed Mohd Faisal, Taskeen Zaidi (2020), Timestamp-Based Detection of Sybil Attack in VANET: International Journal of Network Security. DOI: 10.6633/IJNS.202005 22(3).05.

T. W. Chim, S. Yiu, L. C. K. Hui and V. O. K. Li, "VSPN: VANET-based secure and privacy preserving navigation," in IEEE Transactions on Computers, vol. 63, no. 2, pp. 510{524, Feb. 2014. DOI: 10.1109/TC.2012.188

Taoufik Yeferny and Sofian Hamad (2020) "Vehicular Ad-hoc Networks: Architecture, Applications, and

Challenges" International Journal of Computer Science and Network Security, VOL.20 No.2, February 2020. https://doi.org/10.48550/arXiv.2101.04539.