SECURITY STUDY OF ROUTING ATTACKS IN VEHICULAR AD-HOC NETWORKS (VANETS)

Youssef KHAYATI[1] , Tomader MAZRI[2]

[1] University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco - youssef.khayati@uit.ac.ma
[2] University Ibn Tofail, National School of Applied Sciences Kenitra, Morocco - tomader.mazri@uit.ac.ma

KEY WORDS: Vehicular Cloud Computing(VCC); VANET; Security; Wormhole; DDoS; Black hole etc.

ABSTRACT:

The Vehicular Ad-hoc Network (VANET) is a fast-growing and highly motivated area of research to provide Intelligent Transport Systems (ITS) services to end-users; these services are also responsible for providing an efficient driving environment. in VANET networks, several routing protocols have been designed, but still networks are vulnerable to many threats in the presence of malicious nodes. Today, security is a major challenge in various VANET applications where a bad message can directly or indirectly affect human lives. In this paper, we examine some routing attacks such as Black hole & Wormhole attacks, as well as available solutions for such attacks in existing VANET protocols.

1 INTRODUCTION

VANET is a evolved from the mobile ad hoc network (MANET) where each node (vehicle) moves freely in the network coverage area and provides various types of communications such as inter-vehicle communication, vehicle-to-vehicle communication and road-to-highway communication. In a last few years routing in VANET has been widely studied and discussed. The routing protocols in VANET can be classified into unicast, multicast, broadcast and geocast. Routing in the VANET network is a very difficult task due to its high level of mobility and the frequent disturbance topology of the links. Vehicular communications are very insecure in the face of various threats; security is therefore an important aspect of VANET deployment to make Intelligent Transport System (ITS) services available to every end-user.

VANETs must respect security challenges such as authentication, confidentiality, integrity, availability and non-repudiation to ensure secure communication against attackers on the road(Raya and Hubaux n.d.).

After our review of the various publications, we found that most of the existing works focused mainly on effective approaches that ensure the protection of routing protocols in VANET. These approaches are based on algorithms and cryptography to avoid attacks in VANET. These approaches have some drawbacks, it is difficult to use them in the real world, it is too expensive to deploy, also these approaches need a very strong system which are proposed another challenge of power consumption. According to our observation, the world is moving towards integrating security solutions, such as integration of cloud computing in VANET. Vehicular Cloud Computing(VCC) gives a very strong platform represented mainly in security and also on the ease of handling with attacks.

In this paper we have studied three well known attacks that are threatening the VANET network, we are focused on DDoS attack, Blackhole attack and Wormhole attack. We studied the proposed solutions against these attacks, then we observed the possibility to integrate Cloud computing in VANET. And then we made a comparison between the proposed solutions and compared also between Cloud computing and VCC.

2 ROUTING ATTACKS AGAINST VANET

2.1 Distributed denial-of-service DDoS attack

The DDOS attack is one of the dangerous attacks in ITS, there are two forms to implement the DDOS attack. Internal and external. Both are the same objective; it is preventing the network from doing productive work by sending false data packets. But the difference between the two is that the internal attacker directly sends useless/false messages to a targeted node, but the external attacker exploits the legitimate nodes to shape a group of nodes, Once the weaknesses of the nodes are discovered, they are exploited, the malicious code is then executed on those nodes called "handlers". These infected machines can now not only launch the attack, but also infect other nodes and turn them into zombies or slaves. then, the attacker commands his army of infected nodes to launch the attack at the same time. So VANET loses crucial information and disrupts its normal operation, as it runs in real time(Bansal, Sharma, and Prakash 2015).

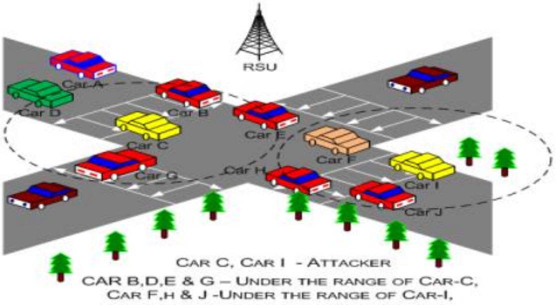
RSU
Car A
Car D
Car B
Car C
Car E
Car F
Car G
Car H
Car I
Car J
CAR C, CAR I - ATTACKER
CAR B,D,E & G – UNDER THE RANGE OF CAR-C,
CAR F,H & J -UNDER THE RANGE OF CAR-I,

Figure 1. DDOS Attack in VANET(Upadhyaya n.d.)

2.2 Wormhole attack

In this type of attack,an attacker overhears the data transferred o ver the wireless communication channel that can lead to serious threats (Afzal and Kumar 2020). In the wormhole attack, a malicious vehicle receives data packets at a point in the network and forwards them to another malicious vehicle using a high-speed wormhole link (tunnel), and

This contribution has been peer-reviewed.
https://doi.org/10.5194/isprs-archives-XLIV-4-W3-2020-267-2020 | © Authors 2020. CC BY 4.0 License.

consequently the communication of the source to the destination is through these malicious vehicles. The impact of this attack is that it prevents the discovery of valid routes and poses a threat to the security of the transmission of data packets(Sirola, Joshi, and Purohit 2014). The wormhole attack is the most serious of attacks because it can happen even if no nodes on the network are compromised. wormhole attack can occur in all scenarios where there is no centralized unit controlling all the nodes in the network.

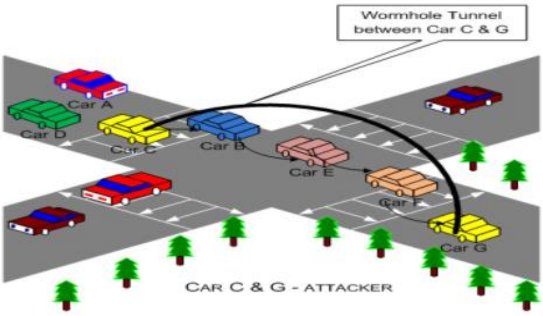

Figure 2. Wormhole Attack(Upadhyaya n.d.)

2.3 Black hole attack

This is one of the security attacks that happen in VANET. In this attack, an attacker node transmits the packet through itself. The effect of this type of attack is therefore very dangerous for the vehicle network. The Black Hole attack is caused by a malicious node that claims have an optimal route to the destination that indicates that the package should be routed by him by transmitting false routing information. In this way, the attacking node will always have the ability to respond to the route request and thus to intercept the data packet and preserve it. In the flood-based protocol, the malicious nodes response will be received by the requesting node before the response from the real node is received, so a malicious and forged route is created(Bibhu et al. 2012). The impact of this attack is that the malicious node can either destroy or abuse the packets intercepted without transmitting them or forward it to the unknown address.

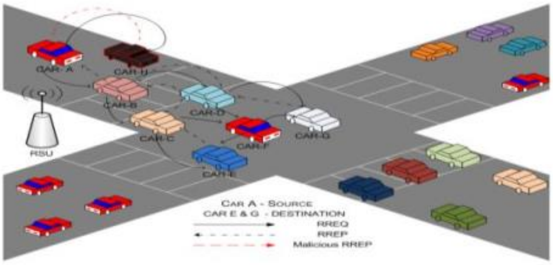

Figure 3. Black Hole Attack in VANET(Upadhyaya n.d.)

3 RELATED WORK

3.1 Denial of service DDoS attack

Much research has been developed to defend against DDoS and DoS attacks in vehicle ad hoc networks.

In paper (Bansal et al. 2015) Pooja Bansal et Al. Proposed a new algorithm for detection DDOS attack. This algorithm uses the concept of "protection node". A node will be chosen based on its importance and uses a hierarchical architecture to divide the node into several levels. When a DDOS attack is launched by the malicious vehicle in the network, the packet delivery ratio will be reduced(Bansal et al. 2015). The paper will be based on two assumptions; the first is triggered in the network and the second is based on the average speed of the vehicles in the network; they take the following steps for the detection strategy. As the first step uses (LPN Selection) This method based on the selection of the LPN node is a three-way handshake process, such that the higher-level node sends a (LPNREQ) request to the lower-level node, and the destination node stops further requests from another node. Then the receiver sends an (LPNACK) back to the sender. The second step uses (Appointment of LPN) In hierarchical architecture, nodes are classified based on their importance. Lower-level nodes are used to protect higher-level nodes, and neighboring nodes are used to protect same-level or lower-level nodes. Each higher-level node has a lower-level Local Protection Node (LPN). In the third step uses (Detection Phase) When DDOS is triggered in the network, the PDR (Packet Delivery ratio) value is reduced(Bansal et al. 2015). If the threshold value becomes equal to the PDR value, the LPN node reports all adjacent vehicles on the network with a "monitoring mode" message. And the vehicles that is receiving the reported message report their neighbors. The malicious vehicle that floods the network with raw packets will be detected. Then the RPN (Remote Protection node) vehicle in the vicinity of the malicious vehicle will be selected to filter the normal traffic with the malicious vehicle. And with the RSU keeps the history of all nodes. When a new vehicle joins the network, information about the malicious node is sent to the newly entered vehicle. And the last step uses (Behavior Based Profile Creation) An anomaly-based detection methodology is used to create profiles that represent the normal behavior of vehicles. Profiles are created by monitoring characteristics (bandwidth consumption, vehicle speed, packet sending rate) over a period of time. If one of the characteristics of an attribute changes, an alert is then generated to the RSU about the anomaly.

In paper (Sinha and K. Mishra 2014) Aditiya Sinha proposed a QLA (Queue limiting algorithm) solution for VANET protection against DoS attack such that each node assigns a queue. With this algorithm each node is limited to receive packets from other nodes. If the victim node receives a high number of the packets, the queue will only accept a limited number of messages and the others are rejected.

In paper (Haydari and Yilmaz 2018), the authors propose a new method for real-time detection and mitigation of low and high rate DDoS attacks in ITS, by using communication between vehicles and RSU; the functionality of RSU is like a network center in a VANET and monitors it to detect possible threats; in the detection phase, they use the ODIT (Online Discrepancy Test) method, which is based on two algorithms, the CUSUM (Cumulative Sum) test and GEM (Geometric Entropy Minimization) and combines the nonparametric nature of GEM with the rapid detection capability of CUSUM; the proposed model was performed on a real road scenario using three software packages, SUMO, OMNET++ and Veins. The experimental results show that the proposed method quickly detects low and high rate DDoS attacks, successfully identifies the attack locations and mitigates the attack by blocking data traffic from the attack locations.

3.2 Wormhole attack

Different solutions have been developed to help detect and prevent wormhole attacks in wireless ad hoc networks(Kaur, Batish, and Kakaria 2012).

In(Anon 2009), Safi et Al. presents a packet leashes defense method against wormhole attack. In(Yih-Chun Hu, Perrig, and Johnson 2006), the notion of packet leashes as a general detection mechanism and thus defense against wormhole attacks is introduced. The leash is any information added to a packet designed to reduce the maximum allowed packet transmission distance. Leashes are conceived to protect against wormholes on a single wireless transmission; when packets are transmitted on multiple hops, each transmission requires the use of a new leash. Two types of leashes exist: geographic leashes (Anon 2009) and temporal leashes. The geographic leashes are used to avoid wormholes and try to fix the weak point of geographic leashes by some changes or modifications. For the authentication of leashes, (Anon 2009), Safi et. Al will also use the HEAP system. This is less problematic compared to related systems. A geographic leash ensures that the recipient of the package is at a certain distance from the sender. Since the packet can move at the speed of light, A time leash ensures that the packet has an upper lifetime limit, which limits the maximum travel distance. Both types of leashes can prevent wormhole attack because they allow the receiver of a packet to detect if the packet has travelled further than the leash allows.

In (Kaur et al. 2012) provide a plan in which use a special package called a “decision package”. When the route has been traced between the origin node and the destination node, a RREP packet (Gupta, Kar, and Dharmaraja 2011) provides the origin node with information about all nodes in the path. To identify the wormhole attack in the origin node of the path, they generate a decision packet that contains the identities of all nodes whose route was formed between the origin node and the destination node in the path recently identified. Every node in the network transmits the decision packet instead of the nodes involved in forming the route from the source to the destination. Other neighboring nodes process the nodes and update the information in the decision packet. To update In this way the distance between the nodes can be calculated.

In paper (Singh et al. 2019), the authors propose a wormhole attack detection system based on Machine learning which determines the behavior of vehicles in VANETs. This system uses the trace files produced by the simulator which consists of both normal and abnormal (under wormhole attack) behavior of nodes in value-added transport networks. they used two simulators to model the VANET scenario : Simulation of the Urban Mobility Model (SUMO) and NS3 as a network simulator. Based on the proposed simulation, they generated a set of data that will be used to learn the attack. In order to prepare the dataset, they transfer all data link statistics to a file using NS3's flow monitoring tool. The different characteristics that are extracted are as follows : source and destination IP, transmitted and received bytes, rejected bytes, delay sum, jitter sum, lost packets, rejected packets, FirstRxBytesTime - FirstTxBytesTime, and throughput.
The results that is obtained after the experiment is as follows: they divided the data set into training and test data. The training data represents 70% of the total number of instances, and the test data represents 30% of the total number of instances. For KNN, the value of k, the number of closest neighbors, is 4, and the value of k is set to 4 based on the accuracy they obtained in the experiment. The precision of the model is the number of correctly ranked test instances relative to the total number of test instances. Both SVM and k-NN worked well and detected the attack with 99% accuracy.

3.3 Black hole attack

Much research has been developed to defend against Black-hole attack.

In paper (Abdulkader et al. 2005) ZAID A. ABDULKADER and Al. Propose a routing algorithm called Lifetime Improving Ad-hoc on demand Distance Vector routing (LI-AODV) that detects and suppresses black-hole attacks in a VANET network, at first the sending node sends the RREQ to its neighboring nodes and it receives the RREP from all the neighbors. They use path rater to choose the best path to the destination. After choosing the best path, and after the node behavior function, the source node notifies the malicious behavior, and if the best path has malicious nodes, it chooses another path for packet transmission. and they are introduced a security algorithm called HMACSHA3-384 to prevent black hole attacks on the network.

In paper (Zhu et al. 2013), the authors developed an approach on the handshaking mechanism to defend against Black Hole attacks. The proposed method is divided into two models, the random waypoint model and the city model. As well as the handshaking mechanism to ensure secure transmission over the network. Under this approach, the nodes will produce the same dynamic ID on the network, which will be same for all nodes. according to the RREQ message is sent over the network, the value of the link establishment is first compared and if it matches, the network proceeds with the transmission to the node. and with the use of random path point model to produce the ID in the group, the malicious node will not know the ID. As a conclusion this approach is effective to easily find the malicious node.

In the paper (Khatoun et al. 2015) propose a monitoring system to track the behavior of the neighbors and to make a decision based on the reputation score of each vehicle. This system is based on three considerations, first step a system based on the reputation score to detect the nodes where packets frequently fall, second step each vehicle contains an observation table to memorize the behavior of the neighbors, and the last step based on a watchdog system which allows to check the modification of the information in the reception packets. they proposes to use confidence tables between nodes, these tables contain confidence values for nodes that are located at the distance of a single hop, and after the node detected the amount of packets that are sent by each node. the confidence tables are sent to the network operation center to refine the nodes according to these confidence values and according to some fuzzy logic, if the tables contain confidence values below a certain threshold, they are rejected, these nodes are probably malicious and are therefore removed from the network.

3.4 Vehicular cloud computing (VCC) in VANET

In the paper (Ahmed et al. 2019) Ahmed and Al. gave an explanation on the insertion of VCC (Vehicular Cloud Computing) in the VANET network for communication between vehicles. They also talked about the services that are provided by VCC in the networks and explained well about their added value.

In the paper (Anon n.d.), the authors reviewed a study on the use of cloud computing in VANET networks to share information and real-time communication between vehicles, which communication is generated by virtual cloud servers of each connected vehicle. They made a comparative analysis of different protocols such as AODV, DSR, DSDV, to determine what is the best protocol for cloud transmission. In addition they explained about the recent progress of VCC for communication in VANET network.

The paper (Garg et al. 2019) proposes an advanced in-vehicle communication technique where it is proposed to replace RSUs by advanced computing platforms. There after the communication between V2V and V2E is secured is designed using the Quotient filter, it is a probabilistic data structure. For VANETs an intelligent safety framework is equipped with advanced computing nodes and 5G technology has been designed to improve communication and computing capabilities in the modern environment of intelligent cities. with experience It has been demonstrated that the use of edge nodes as an intermediate interface between the vehicle and the cloud reduces access latency and avoids congestion of the backbone network, allowing quick decisions to be made according to the traffic scenario in the vehicle's geographical area. the proposed system is highly energy-efficient with minimum delay to conventional vehicle models.

In the paper (Limbasiya and Das 2019) proposes a secure message confirmation method that helps RSUs to verify the different messages obtained from several vehicles in the VCC structure. This proposed system is protected against different cyber-attacks, i.e. identity theft, replay, modification, plain text and man-in-the-middle. and also, it is able to correctly verify a large number of messages at the same time. The proposed protocol is also efficient in terms of experimental time, energy consumption, memory required for communication and storage of data collectively.

4 COMPARATIVE ANALYSIS

In our table we have compared the proposed solutions for detecting and preventing security attacks in VANET networks.

TABLE I. DETECTING AND PREVENTING SECURITY ATTACKS IN VANET

Security Attack	Proposed Solution	Detection(D) Prevention(P) Of Attacks		Based On	P D R	Simulation	Reference
		D	P				
DDoS	Algorithm	Yes	Yes	ND	H	ND	(Bansal et al. 2015)
DDoS	Queue Limiting	Yes	Possible	ICMP	ND	NS-2.31	(Sinha and K. Mishra 2014)
DDoS	framework	Yes	Yes	ND	ND	SUMO, OMNET++ and Veins	(Haydari and Yilmaz 2018)
Wormhole	Packet leashes & HEAP	Yes	Yes	AODV & AODV++	ND	ND	(Anon 2009)
Wormhole	Decision Package	Yes	Non	ND	ND	ND	(Kaur et al. 2012)
Wormhole	SVM and k-NN	Yes	Yes	AODV	ND	SUMO&NS3	(Singh et al. 2019)
Black-hole	Algorithm Life-time Improving Ad-hoc	Yes	Yes	AODV	M	OMNet++	(Abdulkader et al. 2005)
Black-hole	handshaking mechanism	Yes	Yes	ND	ND	ND	(Zhu et al. 2013)
Black-hole	Monitoring System	Yes	Yes	ND	ND	NS-2.35	(Khatoun et al. 2015)

ND: Not determined, M: Medium, H: High, PDR: Packet Delivery Ratio.

According to our analysis of the three attacks against VANET, we have seen that these attacks are always threatening the VANET network, the proposed solutions for each attack is always focused on detecting these attacks, but most of the solutions need a computer system with a very high process capacity, is especially each attack needs a very complicated . analysis to detect them all this propose a problem of energy consumption. The world today is focused on electric vehicle to protect also our nature; and to see an autonomous vehicle connected and also 100% electric, this propose a problem on these solutions.

In this table we compared some characteristics between cloud computing and VCC

TABLE I.I: comparison between CC and VCC characteristics

Characteristic	Description	CC	VCC	Reference
Elastic application on request	Get the service needed and applications can run and use resources dynamically	Yes	Possible	(Buyya et al. 2009),(Anon n.d.)
Virtualization	Multiple requests can be served by one machine but claim to be separate machines.	Yes	Yes	(Stumpf et al. n.d.)
Anytime, anywhere	The availability of the services for each moment from anywhere.	Yes	No	(Buyya et al. 2009)
Network as a Service	Provision of communication and network services	Yes	Yes	(Arif et al. 2012)
Storage as a Service	Provide shared storage and offer it to the user as a storage service provider.	Yes	Yes	(Arif et al. 2012)
Cooperation as a Service	With carpooling, information and entertainment services are provided.	Possible	Yes	(Mousannif and Khalil n.d.)
Planned and unplanned disaster management	Managing disasters using roads and vehicles.	Possible	Yes	(Eltoweissy, Olariu, and Younis n.d.)
Management of major traffic events	Large-scale traffic management.	Possible	Yes	(Eltoweissy et al. n.d.)
Trust and Authentication Management	Provide trust management and authentication to boost confidence.	Yes	Yes	(Anon n.d.)
Cloud Mobility	Clouds or Cloud providers serve on the move.	No	Yes	(Dinh et al. 2013)

The VCC solution is inspired by traditional cloud computing and mobile cloud computing (MCC)(Ahmad et al. 2017).

With VCC, authorized users are given dynamic access to the resources of a group of coordinated vehicles. And vehicle resources, such as detection and internet, computing and storage, are shared for traffic management and road safety decision-making. Resources and services are subscribed to on demand. and Cloud computing uses the underutilized resources of vehicles for a short period of time. VCC is a hybrid technology that uses vehicle resources for traffic management and road safety(Ahmad et al. 2017). VCC enables each vehicle to perform a task necessary to manage the movement of the vehicle on the road, giving vehicles the additional ability to assess traffic conditions and make more appropriate decisions as they travel. With the VCC we hope that the challenge of the attacks in VANET is overcome, especially if the communication is done in general with the VCC, and integrate all the characteristics of VANET in the VCC.

For our vision, and our comparison of the proposed solutions against attacks, we have seen that the use of VCC against attacks in VANET is more efficient than other solutions. In our new work and always in the direction of securing the VANET network, we will focus on VCC and 5G and use the NS3/2 and SUMO simulator to study the confidentiality of VCC for VANET, and propose solutions to improve the VCC.

5 CONCLUSION AND FUTURE WORK

In the VANET network, security will always remain a very complicated challenge. and users need security on the road in the future vehicle network. the implementation of VANET presents a great challenge due to its high mobility, the topology of frequent link disruptions and several security attacks. The main weakness of the ad hoc vehicle network is that it has no centralized infrastructure, which poses a security challenge against attacks. It is difficult to control the attackers, but in future work, we hope to focus on the VCC and 5G and integrate their security against attacks on the VANET, to identify attacks on the network. and we will control the attackers and their attacks.

REFERENCES

Abdulkader, Zaid A., Azizol Abdullah, Mohd Taufik Abdullah, and Zuriati Ahmad Zukarnain. 2005. “LI-AODV: LIFETIME IMPROVING AODV ROUTING FOR DETECTING AND REMOVING BLACK-HOLE ATTACK FROM VANET.” . . *Vol.* 14.

Afzal, Zehra, and Manoj Kumar. 2020. “Security of Vehicular Ad-Hoc Networks (VANET): A Survey.” *Journal of Physics: Conference Series* 1427:012015.

Ahmad, Iftikhar, Rafidah Md Noor, Ihsan Ali, Muhammad Imran, and Athanasios Vasilakos. 2017. “Characterizing the Role of Vehicular Cloud Computing in Road Traffic Management.” *International Journal of Distributed Sensor Networks* 13(5):155014771770872.

Ahmed, Bilal, Asad Waqar Malik, Taimur Hafeez, and Nadeem Ahmed. 2019. “Services and Simulation Frameworks for Vehicular Cloud Computing: A Contemporary Survey.” *EURASIP Journal on Wireless Communications and Networking* 2019(1):4.

Anon. 2009. “[No Title Found].” in *2009 Second International Workshop on Computer Science and Engineering*. Qingdao: IEEE.

Anon. n.d. “Netra2019.Pdf.”

Anon. n.d. “Olariu S. Hristov T. and Yan G. The next Paradigm Shift : From Vehicular Networks to Vehicular Clouds, Pages 645–00. Basagni MC S, Giordano S, Stojmenovic I, Editors. Mobile Ad Hoc Networking : Cutting Edge Directions. 2nd Ed. NJ, USA : John Wiley & Sons, Inc., Hoboken, 2013.”

Arif, Samiur, Stephan Olariu, Jin Wang, Gongjun Yan, Weiming Yang, and Ismail Khalil. 2012. “Datacenter at the Airport: Reasoning about Time-Dependent Parking Lot Occupancy.” *IEEE Transactions on Parallel and Distributed Systems* 23(11):2067–80.

Bansal, Pooja, Shabnam Sharma, and Aditya Prakash. 2015. “A Novel Approach for Detection of Distributed Denial of Service Attack in VANET.” *International Journal of Computer Applications* 120(5):28–32.

Bibhu, Vimal, Kumar Roshan, Kumar Balwant Singh, and Dhirendra Kumar Singh. 2012. “Performance Analysis of Black Hole Attack in Vanet.” *International Journal of Computer Network and Information Security* 4(11):47–54.

Buyya, Rajkumar, Chee Shin Yeo, Srikumar Venugopal, James Broberg, and Ivona Brandic. 2009. “Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility.” *Future Generation Computer Systems* 25(6):599–616.

Chang, Fang-Rong, He-Lai Huang, David C. Schwebel, Alan H. S. Chan, and Guo-Qing Hu. 2020. “Global Road Traffic Injury Statistics: Challenges, Mechanisms and Solutions.” *Chinese Journal of Traumatology* 23(4):216–18.

Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang. 2013. “A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches: A Survey of Mobile Cloud Computing.” *Wireless Communications and Mobile Computing* 13(18):1587–1611.

Eltoweissy, Mohamed, Stephan Olariu, and Mohamed Younis. n.d. “Towards Autonomous Vehicular Clouds.” 16.

Garg, Sahil, Amritpal Singh, Kuljeet Kaur, Gagangeet Singh Aujla, Shalini Batra, Neeraj Kumar, and M. S. Obaidat. 2019. “Edge Computing-Based Security Framework for Big Data Analytics in VANETs.” *IEEE Network* 33(2):72–81.

Gupta, Saurabh, Subrat Kar, and S. Dharmaraja. 2011. “WHOP: Wormhole Attack Detection Protocol Using Hound Packet.” Pp. 226–31 in *2011 International Conference on Innovations in Information Technology*. Abu Dhabi, United Arab Emirates: IEEE.

Haydari, Ammar, and Yasin Yilmaz. 2018. “Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems.” Pp. 157–63 in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*. Maui, HI: IEEE.

Kaur, Harbir, Sanjay Batish, and Arvind Kakaria. 2012. “An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks.” (2248):4.

Khatoun, R., P. Gu, R. Doulami, L. Khoukhi, and A. Serhrouchni. 2015. “A Reputation System for Detection of Black Hole Attack in Vehicular Networking.” 5.

Limbasiya, Trupil, and Debasis Das. 2019. “Secure Message Confirmation Scheme Based on Batch Verification in Vehicular Cloud Computing.” *Physical Communication* 34:310–20.

Mousannif, Hajar, and Ismail Khalil. n.d. “Cooperation as a Service in VANETs.” 17.

Raya, Maxim, and Jean-Pierre Hubaux. n.d. “Securing Vehicular Ad Hoc Networks.” 30.

Singh, Pranav Kumar, Rahul Raj Gupta, Sunit Kumar Nandi, and Sukumar Nandi. 2019. “Machine Learning Based Approach to Detect Wormhole Attack in VANETs.” Pp. 651–61 in *Web, Artificial Intelligence and Network Applications*. Vol. 927, *Advances in Intelligent Systems and Computing*, edited by L. Barolli, M. Takizawa, F. Xhafa, and T. Enokido. Cham: Springer International Publishing.

Sinha, Aditya, and Santosh K. Mishra. 2014. “Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack.” *International Journal of Computer Applications* 86(8):14–17.

Sirola, Priyanka, Amit Joshi, and Kamlesh C. Purohit. 2014. “An Analytical Study of Routing Attacks in Vehicular Ad-Hoc Networks (VANETs).” 3:9.

Stumpf, Frederic, Fraunhofer-Institute Sit, Christian Meves, Benjamin Weyl, and Marko Wolf. n.d. “A Security Architecture for Multipurpose ECUs in Vehicles.” 20.

Upadhyaya, Ajay N. n.d. “ATTACKS ON VANET SECURITY.” 12.

Yih-Chun Hu, A. Perrig, and D. B. Johnson. 2006. “Wormhole Attacks in Wireless Networks.” *IEEE Journal on Selected Areas in Communications* 24(2):370–80.

Zhu, Xiaojun, Fengyuan Xu, Edmund Novak, Chiu C. Tan, Qun Li, and Guihai Chen. 2013. “Extracting Secret Key from Wireless Link Dynamics in Vehicular Environments.” Pp. 2283–91 in *2013 Proceedings IEEE INFOCOM*. Turin, Italy: IEEE.