Academic Guru Publication House

A HANDBOOK ON
Image Processing and Wireless Communication
Volume 1
Year: 2021

AG PH Books

Security Attacks in Vehicular Networks and Survey on Recent Developments in Detection and Protection Against Threats

Dr. G. Mahendran[1*], Dr. S. Murugeswari[2]

[1]*Associate Professor, Department of ECE, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India*

[2]*Professor, Department of ECE, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India*

Abstract

In today's automobiles, security is a primary issue. Among the numerous advantages provided by contemporary vehicle systems are reduced traffic congestion, improved safety, and decreased use of gasoline and diesel fuel. Personal information may be leaked and human lives put in jeopardy by security holes in automobile systems. Vehicle networks are vulnerable to a wide range of security risks, and this article aims to examine them all in relation to the network's cyber security. To help prevent these hazards, the study also provides a literature review of current practises in this area.

Keywords: Vehicular Ad hoc Networks, Routing protocols, Security threats, Trust management

1. INTRODUCTION

The complexity of today's automobiles has skyrocketed. Modern automobiles are quickly becoming more technologically advanced as a result of the constant addition of new technologies. Each contemporary vehicle is equipped with a number of electronic control units (ECUs) that communicate with each other through a network of buses. In the short term, this may be convenient for the driver, but it also presents a greater risk of security breaches. Attackers have the potential to abuse the system in ways that are hazardous to the vehicle and its occupants. The safety of the massive amount of data sent between a vehicle and the outside world is the second source of worry (e.g., through internet, Wi-Fi, or

* ISBN No. 978-81-955340-7-4

Bluetooth). The infotainment systems, for example, provide a convenient entry point for a variety of cyber assaults.

There's a growing gap between current security threats and current safety measures, which necessitates study into security for vehicle systems. Personal information may be leaked and human lives put in jeopardy by security holes in automobile systems. Every sector of life that relies on the sharing of information is affected by cyber dangers. Internet of Things (IoT) dangers are expected to rise by 100% between 2019 and 2020, as the IoT's fast adoption raises the danger to catastrophic levels. To put it simply, a cyber-attack may have a direct impact on the physical world, potentially putting human life at risk and inflicting material damage. This is because cyber-physical systems are becoming more prevalent. In the rapidly emerging area of Connected Autonomous Vehicles, such a hazard presents a serious concern (CAV). It is possible to suffer serious or even fatal consequences if a vehicle's computerised steering systems fail. In autonomous vehicle initiatives centred on V2X communications, where the vehicle may connect with anything, such as vehicles (V2V), infrastructure (V2I), networks (V2N), clouds (V2C), devices (V2D), and pedestrians (V2P), a great emphasis is placed on cyber-security (V2P).

2. LITERATURE REVIEW

(Hidalgo et al., 2021) Increased protection of autonomous vehicle drivers from dangerous cyberattacks would significantly reduce the number of fatalities and injuries throughout the world. Consequently, when a cyber-attack targets high-risk systems like driverless cars, the European Commission has concentrated on communication security. SerIoT, an open and reference framework for real-time monitoring of traffic transmitted over heterogeneous IoT systems, emerges as a feasible option. Using this method, anomalous patterns may be detected, analysed, and, if warranted, countermeasures taken. A case study of the SerIoT project's rerouting testing in vehicular communication is presented in this article. The SerIoT's system capabilities are used to identify and mitigate potential network threats in order to provide safe and dependable communication among C-ITS components (vehicles, infrastructures, etc.). Consequently, fleet management and smart junction scenarios were selected, in which on-board units (OBU) and roadside units (RSU) communicate with each other and the traffic flow to achieve an ideal flow of traffic. Using SerIoT technologies, these devices are able to protect themselves from cyberattacks such as Denial of Service (DoS). The tests have been shown to work in a variety of dangerous circumstances. Taking the necessary steps to guarantee a smooth and safe flow of traffic is a testament to the SerIoT system's high performance.

(Kumar et al., 2021) Because they ensure the safety and security of drivers and passengers, vehicular ad hoc networks (VANETs) have drawn considerable interest in the field of intelligent transportation systems (ITS). Because of their unique properties and system design, VANETs vary significantly from mobile ad hoc networks (MANETs). Vehicle-to-vehicle and vehicle-to-infrastructure communication in a VANET are both affected by security concerns. Detecting and preventing security breaches is critical

in VANET because of malicious attacks. It's possible for a node connected to the network to inject faked routing tables into other nodes, which would have an impact on the overall network performance in a VANET network. A secure AODV routing protocol for detecting black hole attacks has been devised in this research to tackle this problem. Routing protocol enhancements have been made to AODV's RREQ and RREP protocols in the proposed technique. An additional layer of protection is provided by encrypting and decrypting data using a cryptographic function. Different network metrics, such as lose packets, end-to-end latency, packet delivery ratio (PDR), and routing request overhead, are used to show the proposed technique on an NS-2.33 simulator. Proposed routing approach outperforms AODV under black hole attack and enhances network performance, according to results.

(Sultana et al., 2021) One of the fundamental enablers of 5G technology is the development of VANETs based on Software Defined Networking (SDN). VANETs allow for a wide range of services to be provided by cars and roadside equipment by allowing them to communicate. Intelligent Transportation System (ITS) developed this new technology in order to increase traffic efficiency while providing passengers with more comfort, safety, and entertainment. Because of its rigid and inherent rules, the traditional VANET is unable to manage big, dynamic networks with complicated design. An organisation called Open Network Foundation (ONF) is encouraging the use of SDN via open standards' development in order to facilitate management of the whole network from a single point. SDN allows VANET to adapt to new services and features as they become available. The overall network functions and data packet routing are controlled by a centralised controller in the control plane. VANET's efficiency and security are both improved by SDN. With the addition of new technology and architectural components to the network, there are new security concerns to contend with. VANET, SDN, and SDN-based VANETs are thoroughly examined in this article in terms of their architecture and implementation aspects. As a follow-up, it describes how SDN affects the security of VANET when it is used with standard VANET. SDN-based VANET security solutions are reviewed in this study, which also identifies future research areas for SDN-based VANETs. As far as we know, this is the first full assessment of the security aspects of SDN-based VANETs considering architecture and security services on various tiers of the network.

(Eftekhari et al., 2021) An entirely new concept has been established by the incorporation of fog-based computing paradigm into traditional vehicle networks. The goal of this integration is to provide a more fun and safe driving experience. Clearly, one of the most difficult aspects of achieving this aim is how to safeguard these massive communications. If developed and utilised correctly, shared secret key agreement protocols are an accepted solution for this purpose. There have been a large number of these strategies developed so far, but they have mostly failed to meet all of the needed security criteria outside a suitable performance. After the cryptanalysis of a state-of-the-art and distinguished protocol, we propose a security-enhanced three-party pairwise shared key agreement protocol for fog-based vehicular communications with a 23.65% computational cost reduction. Using a well-known "ProVerif" programme, in addition to informal reasons, the proposed protocol is formally validated as well.

Comparisons are made between security metrics and performance to show that the suggested protocol is superior when both security and efficiency are taken into account simultaneously.

(Nandy et al., 2021) Due to their small weight and lack of security, a large range of authentication methods are created to protect vehicular ad-hoc network (VANET) transmission from possible assaults. Trusted authorities and signatures are often used to authenticate communication in automotive networks; however this is not always sufficient. In these approaches, achieving speedy validation and correspondence is a challenge, and the execution demands from coming about overhead make it much more challenging. As a result, we've created ELSAP, a more secure and lightweight V2V authentication protocol for VANETs. A self-authentication method before communication, which increases network feasibilities, which in turn requires less message transmission during authentication and communication, indicating light characteristics. In addition, Burrow–Abadi–Needham (BAN) reasoning proves that two or more vehicles may safely undertake mutual authentication. According to Automated Validation of Internet Security Protocols and Applications (AVISA), the proposed protocol's ability to withstand current threats is shown by security analysis and comparison tools such as these (AVISPA). With the proposed protocol's security characteristics, the performance study demonstrates that communication and computation costs are lower than those of the previous authentication techniques.

(Sun et al., 2021) Due to their unique wireless characteristics, such as highly dynamic vehicles and unstable channels, vehicular ad hoc networks (VANETs) have high QoS and security requirements. QoS and security are difficult to maximise together since they are competing priorities for scarce network resources. Because of this, a trade-off is necessary. Each vehicle in the research competes for resources internally and externally in a two-period game that simulates each of these aspects. To optimise throughput in the initial external decision-making phase, each vehicle builds a cross-layer utility between the MAC and PHY layers. Aside from that, the optimum strategy for the vehicle's external decision-making is gained as an input for the following period, serving as an input for the optimal transmission power. An individual vehicle's QoS and security are regarded as two abstract actors competing for the vehicle's limited resources in the second stage of internal decision-making. The 'communication player,' which controls the quantity of data blocks, is modelled like a game, while the'security player,' which controls the hash length, is modelled after a game. Two players' optimum strategy composition is calculated and shown to equal the theoretical value of the Nash equilibrium of the internal game. Simulated findings show that a vehicle may achieve sufficient QoS and security levels by dynamically adapting its optimum tactics to the network and traffic conditions in which it is positioned.

(Amin et al., 2020) Vehicular Ad-Hoc Network (VANET) is a term used to describe the connectivity of automobiles for the purpose of sharing relevant information. Driving safety and comfort may be assessed using the information sent. It is also utilised in traffic analysis, road safety measures, vehicle performance statistics, and multimedia data sharing between cars through continuous Internet access. After obtaining critical information, adversaries might cause multiple system outages. As a result, establishing reliable communication requires a strong security protocol. The protocol developed by Bidi et al. is examined in this article and shown to have a number of serious security weaknesses. Once we've

established a high degree of security, we present a comprehensive protocol that defends against any and all connected threats. Using Scyther, we were able to verify that the creation of a shared key does not compromise the privacy of any data. In addition, the protocol's overall performance is better to that of competing methods.

(Al-Turjman & Lemayian, 2020) The future Intelligent Transportation Systems (ITS) must handle the essential issue of VSN security (ITS). Assailants have access to the personal information that users voluntarily provide. Malwares and Spams, Black Holes, Wormholes, and Physical/Electronic Outages are among the most common assaults. As a result of these VSN assaults, people may be killed in car accidents or have their privacy violated. VSNs in a smart city paradigm based on vehicle IoT are discussed in this study, emphasising on security aspects. VSN's resilience and dependability are also discussed in this section. We also address the security issues associated with various communication systems. This article focuses on the most pressing challenges in literature research and offers advice on how to overcome them. To create effective ITS, VSNs must play a vital part in this study's conclusion However, to provide a dependable and secure transportation system, present VSN security requirements must be upgraded.

(Malhi et al., 2020) Intelligent Transportation Systems (ITS) are concentrating their attention on cars that have extensive processing, communication, and sensor capabilities (often known as "smart" vehicles) (ITS). When it comes to vehicular ad hoc networks, the primary goal is to make driving more secure and efficient by giving real-time traffic information to drivers and any other parties that may be engaged. This article focuses on the security issues of VANETs and analyses some of the most popular safety solutions. VANET threats and security methods (a), a comparison of cryptography-based security schemes (b), and trust management strategies based on discrete features and intrusion detection systems (c) are the four main components of this study. (d) unresolved concerns that will need to be addressed in the future. On the basis of previous computer security research, we explore how this study represents the evolution of security assaults and its future predictions.

(Pu et al., 2020) Using edge stations or cloud service providers, vehicular social networks (VSNs) may deliver traffic or location services to cars. Furthermore, the exchange of information between cars may help prevent traffic accidents and ensure safe driving. When communicating between a car and an edge station, a cloud service provider or another vehicle over a VSN, it's simple for the privacy of the vehicle to be compromised. Some wicked users, on the other hand, may dishonestly provide information in order to deceive others for their own gain. Because of this, we provide a blockchain-based solution for VSNs that is fast, secure, and private. Using pseudonyms, we're able to protect the identities of individuals by obscuring the cars they're travelling in. An incentive-punishment scheme is also developed to encourage cars to submit reliable information. The message's dependability may be assessed using a combination of many variables and a single factor weighted assessment method. In addition, PBFT and blockchain are used to establish consensus and store data, respectively, to prevent malevolent actors from altering vehicle reward and credit ratings. As a last step, we examine the suggested scheme's security from several perspectives: external assaults, internal attacks, collusion

attacks, etc. According to the findings of the relevant experiments, our plan is both practicable and efficient.

(Ghaleb et al., 2019) Cooperativeness among network members is essential to the majority of VANET and FANET applications, protocols, and services. In order to enhance network performance and to offer safety, traffic efficiency, and entertainment, vehicles, including unmanned aerial vehicles (drones), communicate sensor data. VANET performance relies heavily on this data's precision and dependability. A vehicle's cooperativeness characteristic may be used by misbehaving (or defective) automobiles to pass on false information, resulting in the death or destruction of persons or property. Existing detection methods are unable to stop such assaults, which is a shame. Furthermore, they depend on predetermined and static security boundaries to distinguish between false and true information, which is a major oversight. Detection accuracy and false alarm rates may both be improved by using context-aware detection, as shown in this study. As a starting point, elements that accurately reflect the automobile setting have been culled out. An online unsupervised learning approach called the hierarchical clustering algorithm is utilised to identify the incoming messages as authentic or bogus. Finally, the classification's validity was confirmed using Bayesian-based hypothesis testing. The results demonstrate that the proposed detection method is promising in detecting false information attacks and enhancing application performance.

(Awais Javed et al., 2018) Transportation in smart cities will be safer and more dependable because to the potential of VSNs, or vehicular sensor networks. Various intelligent transportation applications may be accomplished by developing widespread communication between automobiles and road infrastructure. To successfully integrate VSNs, effective network security becomes a top priority. Strong security measures, on the other hand, come at a considerable cost in terms of security overhead and processing time, reducing QoS dramatically in heavy-traffic environments. The QoS of safety applications in VSNs may be improved by using a security adaption mechanism based on trust. Connectivity duration, security level, and centrality indicators of neighbouring cars are used to compute trust levels. Using simulation findings acquired from our proposed study, we have shown a 25–65% increase in safety awareness and a 33–53 improvement in packet inter-arrival time for safety applications in VSNs.

(Tyagi & Dembla, 2017) There are two types of ad-hoc networks in use today: those based on mobile nodes and those based on vehicle nodes. These two types of networks are known as MANETs and VANs, respectively (VANET). The goal of VANET is to keep drivers safe by allowing them to communicate with other cars autonomously. The ad hoc network's vehicles operate as intelligent mobile nodes, capable of forming dynamic networks and moving around rapidly. Due to the constant movement of the vehicles, the ad-hoc networks demand a high level of efficiency and security in their communication. Assaults such as denial of service and Black Hole attacks are more likely to occur on these networks. For the first time, this study attempts to explore and investigate the security characteristics of VANET's routing protocols and the applicability of the AODV (Ad-hoc On-Demand) protocol in order to identify and combat a specific kind of network assaults known as Black Hole Attacks. As part of a novel method

suggested to improve the security of the AODV protocol and to add a mechanism to identify and avoid Black Hole Attacks, a look-up table of all route answers is maintained by the source node and is used to keep track of the network's path. PUSH and POP operations are used to organise the reply sequences in ascending order in this table. Sequence number is used to determine priority, and RREPs with a very high destination sequence number are discarded. ITS security is improved, as is VANET security as a consequence of using the suggested technique to identify and prevent a Black Hole Attack on ITS nodes. In this study, NCTUNs simulator is used.

(Cherkaoui et al., 2017) Vehicular Ad-hoc Networks (VANs) are a new form of wireless ad-hoc network that may be used between automobiles. The creation of such a communication network is aimed at streamlining traffic and promoting driver safety by providing relevant information to its users. Prior to building up an actual network, we must protect the communication by forecasting certain security concerns and preparing for them. The Black Hole Attack is only one of the many crises that plague humanity. The black hole assault may be detected using a quality control chart proposed in this research. Real-time network activity monitoring utilising visual representations is used to identify any abnormalities that may occur during the course of communication using this technique in this manner. Conference Program Chairs responsible for peer review.

(Pan et al., 2017) It has emerged in recent years as a wireless ad-hoc network connecting automobiles, which is known as a Vehicular Ad-hoc Network (VAN). The creation of such a communication network is intended to help with traffic flow and to promote safe driving behaviour by providing users with relevant information. Consequently, we must foresee a number of security threats before implementing this network in the actual world. There are a number of difficulties that need to be addressed. Using a quality control chart, we offer a new approach for detecting black hole attacks. This approach monitors network traffic in real-time using graphical representations to identify any anomalous behaviour during communication. The Conference Program Chairs are in charge of peer review.

(Mokhtar & Azab, 2015) Unlike other ad hoc networks, vehicular Ad hoc Networks (VANs) are characterised by a lack of infrastructure as well as the fact that the communication entities move at varying speeds. As a result, dependable end-to-end connection and efficient data transmission are hindered. These network and security problems and difficulties influence the trust between mobile networking entities, which in turn affects the capacity of VANETs to provide ubiquitous connection, secure communications, and reputation management systems. To better understand the security aspects of VANETs, we conducted a study to categorise the assaults on VANETs based on the various network levels.

3. TYPES OF ATTACKS

Passive attacks and active assaults are the most typical types of attacks against ad-hoc routing methods:

Passive attack: In contrast to a Direct Attack, a Passive Attack aims to get valuable information through intercepting the protocol's communication. Sniffering the network is a key component of passive attacks. Defending against these types of assaults is tough since they are difficult to detect. If it is not feasible to pinpoint the precise position of a node, one may still be able to learn about the network's architecture by using this kind of attack.

Active attack: As the name implies, an Active Attack attempts to disrupt the protocol's normal functioning by injecting random packets in an attempt to restrict access, get authentication, or snoop on traffic heading to other nodes. Attraction of all packets for analysis or denial of service is the primary objective. Detection and identification of the nodes involved in such assaults is possible. Some of the threats to the routing layer and some of the routing protocols are outlined below.

- **Routing table overflow attack**

Proactive routing algorithms, which update route information on a regular basis, defend against this assault. Using this method, the attacker attempts to build routes from nonexistent nodes to the network's established and trusted nodes. The attacker may easily overwhelm the target system's routing database by sending out aggressive route announcements. Routing protocol implementation should be hindered or impossible because of the sheer volume of routes already in existence.

- **Routing cache poisoning attack**

The promiscuous way of updating the routing table is exploited in a routing cache poisoning attack. If the data in routing tables is updated, tampered with, or injected with incorrect information, this might happen. M, a malevolent node, is trying to poison the routes between X and Y. As a result, nearby nodes who overhear the packet and see the faked source route to X may add the route to their caches.

- **Attacks on particular routing protocols**

This survey's primary goal is to categorise VANET assaults by layer, hence we must include attacks that specifically target routing protocols. The fundamental issue with these proto-cols is that they don't pay enough attention to security. This issue is prevalent in most contemporary studies. Following that, we'll look at various typical routing protocols and the security risks, benefits, and drawbacks associated with each.

- **AODV**

AODV is a reactive technique for routing data over wire-less mesh networks using the Ad-hoc On-Demand Distance Vector (AODV) algorithm. Because it is simple, takes minimal memory, and doesn't produce more traffic for communication over existing networks, AODV is a good choice for routing. A malicious node may advertise a route that has a lower distance metric than the original distance or announce a routing update with a big sequence number that invalidates all other nodes' route updates. In order to improve the security of AODV's multihop authentication and integrity (using hash chains and signatures), a new version of the protocol known as "Secure AODV" was suggested.

- **DSR**

If you're looking for something similar to AODV, the Dynamic Source Routing (DSR) protocol could be a good fit for you. Source routing instead of depending on each intermediary node's routing table distinguishes them. In addition, a packet may be sent hop-by-hop using this feature. If an attacker wishes to change the source route mentioned in the RREQ or RREP packets, they may do so in DSR. It is possible to delete a node from the list, change the order, or add a new node to the list in DSR.

- **ARAN**

Malicious activity may be detected and prevented using the Authenticated Routing for Ad hoc Networks (ARAN) protocol, which is an on-demand routing system. To provide basic security, this protocol introduces authentication, integrity, and non-repudiation. When it comes to ad-hoc security measures, ARAN is meant to be resistant to the rushed assault detailed later.

- **ARIADNE**

Ariadne is an efficient and on-demand routing technology based on DSR that employs extremely effective symmetric cryptography. A message authentication code (MAC) and a common key between the two communicating parties are used to enable point-to-point authentication of a routing message. Cache poisoning and flood of RREQ packets aren't enough to keep ARIADNE safe from these attacks.

- **SEAD**

SEAD is based on the DSDV-SQ protocol, which is a subset of the DSDV standard. One-way hash chains instead of costly asymmetric cryptography operations are used to cope with attackers who modify routing information and replay attacks. To thwart the attackers, the system makes use of two separate methods for authenticating messages. SEAD, on the other hand, cannot handle wormhole assaults.

4. OTHER ADVANCED ATTACKS

VANET has recently been targeted by increasingly sophisticated and covert assaults. To counter the assaults, new routing protocols are being suggested and certain protocols have been improved. Even so, it's something that security personnel are interested in. Black holes (or sinkholes), Byzantine, wormholes, and rushing assaults are just a few of the most common instances.

- **Rushing attacks**

This is a new attack that results in denial of service when employed against all prior on demand ad hoc network routing prototypes. Routes longer than two hops cannot be discovered using DSR, AODV, or secure protocols based on these technologies, such as Ariadne and ARAN. An attacker who is able to fast send route requests might raise the likelihood that routes that involve the attacker will be identified

rather than other legal routes. A weakness of this assault is that it may be carried out by a very inexperienced attacker. Named Rushing Assault Prevention, it is an attempt to prevent this attack (RAP).

- **Wormhole attack**

The term "wormhole attack" refers to an attack in which two or more nodes work together to encrypt and tunnel data between them. This vulnerability allows a node or nodes to interrupt the regular flow of data, producing a virtual vertex cut in the network controlled by the two collaborating attackers.

- **Black hole attack**

There are two stages to the black hole assault. There are many ways that a malicious node might use the mobile ad-hoc routing protocol (such as AODV) in order to trick other nodes into believing that it has a legitimate route to the target node. No further action will be taken from this point forth. If the attacker is skilled, he or she may modify or silence packets emanating from certain nodes while leaving the rest of the data untouched. In this manner, the attacker tampered with the nearby nodes that keep track of the current packets.

- **Byzantine attack**

A single malicious node or a group of nodes working together may launch a byzantine assault. Compromises may be carried out either by a single compromised intermediate node or by a group of compromised intermediate nodes working together. Nodes that have been hacked may cause routing loops, send packets along a lengthy path rather than the best one, or even discard packets altogether. Routing services are disrupted and performance is degraded as a result of this attack.

An assault on the system's resources The MANET relies heavily on energy. In order to save battery power, battery-powered devices communicate with each other only when required. The goal of a resource consumption attack is to deplete the battery life of the victim node by sending requests for excessive route discovery or superfluous packets. As a result, the MANET's regular operation may be disrupted by an attacker or a compromised node. In VANETs, this assault has little impact since there are no significant restrictions on energy supplies.

- **Location disclosure attack**

Disclosed location attacks are part of an information disclosure assault. The rogue node discloses information about the network's location or structure, which it then utilises to further attack the system. It collects node location data, such as a route map, and determines which nodes are located along the intended path of travel. Detecting traffic patterns is one of the VANET security threats that has yet to be addressed.

5. CONCLUSION

There are several research possibilities in this area to stay up with technology advancements and the changing nature and demands of our society. As an example, balancing security, privacy, and function in certain vehicle circumstances may be a difficult task. Cyber-security in autonomous vehicle projects is heavily centred on V2X communications, which include vehicle-to-vehicle communication (V2V), as well as communication with infrastructure, network and cloud. V2D and V2P communications are also heavily emphasised in the paper, as is vehicle-to-pedestrian communication (V2P) (V2P).

REFERENCES

Al-Turjman, F., & Lemayian, J. P. (2020). Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview. *Computers and Electrical Engineering*, *87*, 106776. https://doi.org/10.1016/j.compeleceng.2020.106776

Amin, R., Lohani, P., Ekka, M., Chourasia, S., & Vollala, S. (2020). An enhanced anonymity resilience security protocol for vehicular ad-hoc network with Scyther simulation. *Computers and Electrical Engineering*, *82*. https://doi.org/10.1016/j.compeleceng.2020.106554

Awais Javed, M., Zeadally, S., & Hamid, Z. (2018). Trust-based security adaptation mechanism for Vehicular Sensor Networks. *Computer Networks*, *137*, 27–36. https://doi.org/10.1016/j.comnet.2018.03.010

Cherkaoui, B., Beni-Hssane, A., & Erritali, M. (2017). Quality Control Chart for Detecting the Black Hole Attack in Vehicular Ad-hoc Networks. *Procedia Computer Science*, *113*, 170–177. https://doi.org/10.1016/j.procs.2017.08.337

Eftekhari, S. A., Nikooghadam, M., & Rafighi, M. (2021). Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications. *Vehicular Communications*, *28*, 100306. https://doi.org/10.1016/j.vehcom.2020.100306

Ghaleb, F. A., Zainal, A., Maroof, M. A., Rassam, M. A., & Saeed, F. (2019). Detecting Bogus Information Attack in Vehicular Ad Hoc Network: A Context-Aware Approach. *Procedia Computer Science*, *163*, 180–189. https://doi.org/10.1016/j.procs.2019.12.099

Hidalgo, C., Vaca, M., Nowak, M. P., Frölich, P., Reed, M., Al-Naday, M., Mpatziakas, A., Protogerou, A., Drosou, A., & Tzovaras, D. (2021). Detection, control and mitigation system for secure vehicular communication. *Vehicular Communications*, *1*, 100425. https://doi.org/10.1016/j.vehcom.2021.100425

Kumar, A., Varadarajan, V., Kumar, A., Dadheech, P., Choudhary, S. S., Kumar, V. D. A., Panigrahi, B. K., & Veluvolu, K. C. (2021). Black hole attack detection in vehicular ad-hoc network using secure

AODV routing algorithm. *Microprocessors and Microsystems*, *80*(October), 103352. https://doi.org/10.1016/j.micpro.2020.103352

Malhi, A. K., Batra, S., & Pannu, H. S. (2020). Security of vehicular ad-hoc networks: A comprehensive survey. *Computers and Security*, *89*, 101664. https://doi.org/10.1016/j.cose.2019.101664

Mokhtar, B., & Azab, M. (2015). Survey on Security Issues in Vehicular Ad Hoc Networks. *Alexandria Engineering Journal*, *54*(4), 1115–1126. https://doi.org/10.1016/j.aej.2015.07.011

Nandy, T., Idris, M. Y. I., Noor, R. M., Das, A. K., Li, X., Ghani, N. A., & Bhattacharyya, S. (2021). An enhanced lightweight and secured authentication protocol for vehicular ad-hoc network. *Computer Communications*, *177*(June 2020), 57–76. https://doi.org/10.1016/j.comcom.2021.06.013

Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., & Batten, L. (2017). Cyber security attacks to modern vehicular systems. *Journal of Information Security and Applications*, *36*, 90–100. https://doi.org/10.1016/j.jisa.2017.08.005

Pu, Y., Xiang, T., Hu, C., Alrawais, A., & Yan, H. (2020). An efficient blockchain-based privacy preserving scheme for vehicular social networks. *Information Sciences*, *540*, 308–324. https://doi.org/10.1016/j.ins.2020.05.087

Sultana, R., Grover, J., & Tripathi, M. (2021). Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges. *Vehicular Communications*, *27*, 100284. https://doi.org/10.1016/j.vehcom.2020.100284

Sun, Z., Liu, Y., Wang, J., Yu, R., & Cao, D. (2021). Cross-layer tradeoff of QoS and security in Vehicular ad hoc Networks: A game theoretical approach. *Computer Networks*, *192*(2699), 108031. https://doi.org/10.1016/j.comnet.2021.108031

Tyagi, P., & Dembla, D. (2017). Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET). *Egyptian Informatics Journal*, *18*(2), 133–139. https://doi.org/10.1016/j.eij.2016.11.003

