Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 1640167, 15 pages
https://doi.org/10.1155/2018/1640167

Review Article

Lightweight Cryptographic Techniques for Automotive Cybersecurity

Ahmer Khan Jadoon[1], **Licheng Wang**[1], **Tong Li**[2] and **Muhammad Azam Zia**[3]

[1]*State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2]*School of Computer Science, Guangzhou University, China*
[3]*Department of Computer Science, University of Agriculture Faisalabad, Pakistan*

Correspondence should be addressed to Tong Li; litongziyi@mail.nankai.edu.cn

Received 10 March 2018; Accepted 24 May 2018; Published 26 June 2018

Academic Editor: Joseph Liu

A new integration of wireless communication technologies into the automobile industry has instigated a momentous research interest in the field of Vehicular Ad Hoc Network (VANET) security. Intelligent Transportation Systems (ITS) are set up, aiming to offer promising applications for efficient and safe communication for future automotive technology. Vehicular networks are unique in terms of characteristics, challenges, architecture, and applications. Consequently, security requirements related to vehicular networks are more complex as compared to mobile networks and conventional wireless networks. This article presents a survey about developments in vehicular networks from the perspective of lightweight cryptographic protocols and privacy preserving algorithms. Unique characteristics of vehicular networks are presented which make the embedded security applications computationally hard as well as memory constrained. The current study also deals with the fundamental security requirements, essential for vehicular communication. Furthermore, awareness of security threats and their cryptographic solutions in terms of future automotive industry are discussed. In addition, asymmetric, symmetric, and lightweight cryptographic solutions are summarized. These strategies can be enhanced or incorporated all in all to meet the security perquisites of future cars security.

1. Introduction

There has been a tremendous increase in the number of vehicles compared to the number of roads. This situation leads to many challenges like heavy traffic jams, economy, pollution, and many other issues related to efficiency and safety of transportation systems. Many initiatives have already been taken in response to these challenges in order to overcome the situation. For this scenario, utilization of wireless technology in vehicular networks makes a huge difference to overcome the traffic issues and reduce the chances of accidents or injuries. Intelligent transportation systems (ITS) [1] are developed, aiming to improve the efficiency and safety of transportation systems. This technology mainly relies on the information sharing and authentication of vehicles. Moreover, it makes them traceable to law enforcement authorities in case of overspeeding, crash or collection of tolls, etc. The authentication of vehicles can be performed through radio links, instead of conventional methods such as reading license plates. Vehicles also need to be authenticated by other vehicles and infrastructure for secure communication. Many service providing companies exchange information with vehicles to facilitate the use in terms of location services or other helpful applications. All these authentications are carried out by cryptographic algorithms to ensure the identity of sender and receiver.

A general vehicular network consists of three types of communications links, i.e., Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Infrastructure to Infrastructure (I2I) communication. All these links require being protected in order to insure the security of network. Vehicles are equipped with On-Board Units (OBUs) to communicate with each other and Road Side Units (RSUs). Validation and authentication of information exchange between the vehicles

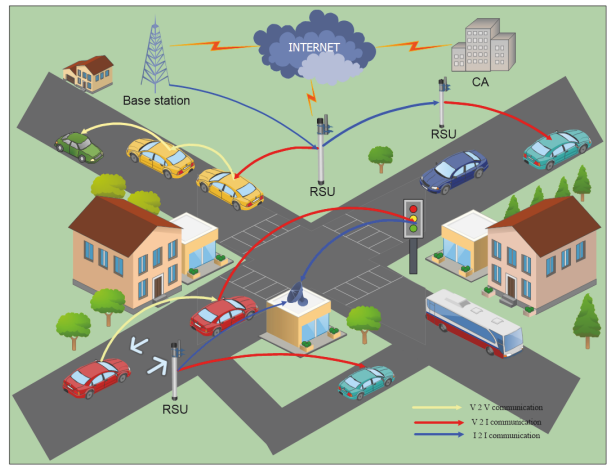

Figure 1: Vehicular network architecture.

are a key concern for the traffic safety. Furthermore, driver's privacy also needs to be considered (their details must be confidential from unauthorized entities) and their confidential information can only be accessed by a legitimate authority. The main goal is to achieve both anonymity and traceability at the same time [2]. Privacy in a vehicular network is more considerable as compared to mobile network, since a mobile phone can be switched off at any time but a license plate needs to be accessed by the law enforcement authorities all the time.

However, the protection against many malicious attacks like message suppression, denial of services, dropping down of packets from network, broadcast of false information, getting control over the network, and several other attacks is still unknown to manufacturers and suppliers. Conventional cryptographic algorithms such as public-key infrastructure (PKI), elliptic curve cryptography (ECC), HASH functions, and symmetric key cryptography may not be applied directly in vehicular networks due to their high mobility and dynamic network topology [3–5]. Vehicular networks require real-time response and cannot tolerate delay in communication. Therefore, the conventional protocols that are developed for traditional networks fail to provide high throughput performance, low latency, and reliability for vehicular networks. So, there is a need to implement secure lightweight cryptographic algorithms (as well as lightweight PKI [6]) on small embedded devices at acceptable execution time. Recently, scholars focus on developing the lightweight cryptographic algorithms and key generations schemes which may provide security for vehicular networks with high performance efficiently.

Primary target of this article is to give an overview on advancements of vehicular systems insight into the lightweight cryptographic conventions and security protecting calculations. The public acceptance for new technology in vehicular networks can only be ensured by optimizing the security and privacy of users. Moreover, awareness of security threats regarding the malicious attacks in future automotive industry should be known by the users and manufacturers. Security concerns for the future automotive industry are hurdle in the way of extensive deployment of vehicular networks commercially. Furthermore, we provide knowledge about resource constraints and challenges during the implementation of cryptographic algorithms for vehicular networks. We also present suggestions and lightweight cryptographic solutions to overcome the problems in future automotive industry.

The paper is organized as follows: In Section 2, we present the architecture of vehicular networks in sight of characteristics and security requirements. In Section 3, we discuss the security attacks on vehicular systems. Lightweight cryptographic protocols for vehicular networks are characterized in Section 4. Finally, Section 5 presents concluding remarks.

2. Architecture of Vehicular Ad Hoc Network

VANETs consist of the two basic wireless terminals, namely, On-Board Unit (OBU) and Road Side Unit (RSU) [1, 7–9]. The OBUs are embedded wireless devices installed in vehicles to communicate with RSUs and other OBUs. While RSUs are located at important points alongside the road or infrastructure and represent the wireless access points for communication. Each terminal acts like a node that can receive and relay messages within a wireless network. These nodes function as a router to other nodes in the network as shown in Figure 1. There is also interroadside communication of these access points with each other or with other devices. For instance, traffic lights may communicate with each other or RSU may communicate with cellular base stations etc. IEEE 802.11p Dedicated Short Range Communication (DSRC) has been selected as a standard for V2V and V2I communication in order to provide high data transfer with low latency [9]. It works in 5.9 GHz frequency band with 75 MHz bandwidth and has 300-1000 m range with several vehicle velocities in different environments [9, 10].

The existing Wireless Access in Vehicular Environments (WAVE) uses DSRC protocol to broadcast the services provided at RSUs [3]. Basically short messages contain vital

information about location, speed, and direction as well as emergency information with respect to airbag deployment, accident report, emergency brakes, etc. However, current approach of broadcast mechanism can result in network traffic congestion due to the insignificant usage of network resources. This issue can be resolved by tracking the addresses of OBUs and their connections with respective RSUs to perform efficient mobility management. There have been many suggestions related to mobility management in WAVE.

Chun et al. proposed two types of mobility management schemes, i.e., location estimation-based mobility management (LEMM) and basic mobility management (BMM) for WAVE services [11]. In LEMM scheme, positioning systems (e.g., GPS) are utilized to determine the location of OBUs in a fast moving vehicle, whereas, in BMM scheme, all RSUs are divided into different location areas which can determine the locations of OBUs by their MAC addresses. Torrent-Moreno et al. present a scheme for congestion mitigation based on distributed and fair transmit power-control [12]. Tielert et al. proposed a message-rate controller which uses disseminating congestion information over multiple hops to achieve global fairness [13]. Most of the schemes proposed a common feature for congestion control in the literary work and their goal was to attain unweighted fair sharing of the scarce channel resource to all vehicles [12–14]. Recently, Xu et al. proposed a lightweight scheme known as Dynamic Fully Homomorphic encryption-based Merkle Tree (FHMT) for lightweight streaming authenticated data structures which can be adopted in vehicular networks as a congestion mitigation technique. By leveraging the computing capability of fully homomorphic encryption, FHMT shifts almost all of the computation tasks to the server, reaching nearly no overhead for the client [15]. These schemes are significant to vehicular security requirements; however DSRC requires cryptographic protocols for authentication and authorization purposes which can result in network congestion. Therefore, lightweight cryptographic algorithms should be the first choice to ensure efficient security in automotive technology.

2.1. VANET Characteristics. VANETs use ad hoc approach to execute the wireless communication. The combination of properties of both wireless medium and ad hoc approach is generally defined as characteristics of VANET which makes it unique. We list some of the unique characteristics of VANETs as follows:

(1) **High mobility:** Mobility in VANETs is relatively higher as compared to MANETs. Generally, each node moves at higher speed in VANET. Therefore, network's communication time is reduced due to high mobility of the nodes [16, 17].

(2) **Time critical data exchange:** In VANET, the transfer of information to legitimate nodes should be reached within a specific time limit in order to execute rapid actions based on decisions made by the node.

(3) **Dynamic network topology:** The high mobility of vehicles makes the VANET topology irregular. Rapid changes in topology make the vehicular network vulnerable to attacks. Under such conditions, malicious vehicles are quite hard to detect.

(4) **Unbounded network density:** In VANETs, the density of network mainly relies on number of vehicles that may be high in traffic jams and low in suburban and rural areas. There is no bound to the number of vehicles joining the network.

(5) **Frequent disconnections:** Vehicles mostly use wireless medium to communicate in VANET, so frequent disconnection may occur due to high density of the vehicles or worse weather conditions.

(6) **Wireless medium:** Since only transmission medium that can be used in VANETs is wireless medium, therefore, the transmission of data should be anonymous. If the medium of transmission is not properly protected, then security of whole network can be jeopardized by using the same operating frequency [18].

(7) **Power constraints:** As compared to MANETs, the vehicular nodes do not experience power issues because of an uninterrupted power supply which can be arranged for OBUs by using long life battery.

(8) **Limited power transmission:** The architecture of wireless access of vehicles (WAVE) supports maximum range of 0 to 28.8 dBm for transmission power and associated coverage of distance range from 10 m to 1 km. So, coverage area distance is limited due to limitation of transmission power [9].

(9) **Wireless transmission limitations:** The factors like reflection, scattering diffraction, and refraction present in the urban areas makes the performance of DSRC wireless communication limited [19].

(10) **Computing capacity and energy storage:** The energy or storage breakdown problems are not present in VANETs. However, processing of very large amount of information is required due to huge scaling environment which becomes certainly a big challenge.

2.2. VANET Security Requirements. The main objective of VANET is to provide the comfort and safety to the driver as well as passengers. Communication between OBUs and RSUs can be employed to realize the active safety services like collision warnings, active navigation systems, real-time traffic information or weather information, etc. Facilities like multimedia or Internet connectivity are provided in the wireless coverage of a car. VANETs also include automatic parking payments and electronic toll collections. To ensure the efficient working of all these applications and services, a network needs to authenticate every message sent or received by the nodes. A small error or attack may result in a big damage for the safety and security of public. Certain security requirements for the V2V and V2I communication links in a basic vehicular network are listed as follows:

(1) **Message authentication and integrity:** Message authentication is the fundamental part of vehicular

Table 1: Attacks on VANET and their impact on security requirements.

Security Requirements	Attacks	Reference (Security Requirements/Attacks)
Message authentication and integrity	Sybil/Impersonation/Replay attacks	[20–23]/[46, 47, 53]
Availability	DoS/Sybil/Bogus information/Routing attacks	[24–26]/[46, 49, 50]
Confidentiality	Sybil/Impersonation attacks	[20]/[46–48]
Non-Repudiation	Impersonation attacks	[24, 25]/[48]
Privacy	Impersonation/Location Trailing/Eavesdropping attacks	[28, 29]/[41–45]

security. It ensures that each received message arrives in the same condition as it was sent out by the sender. Moreover, ID, location, and property of a sender must be authenticated and it is made sure that legitimate sender transmits reliable information [20]. Integrity check allows the receiver to verify if there has been any kind of fabrication or modification within the duration in which message was sent and received. We can find related work on message authentication and data integrity in literature [21–23].

(2) **Availability:** Availability of information is directly related to the efficiency of vehicular network. It ensures that network resources such as session key and applications must be available to legitimate nodes in a certain period of time without affecting operation of the network even in the presence of faults or malicious nodes [24, 25]. A number of multipath algorithms have been proposed to transfer information via multiple disjointed paths in order to reduce the chances of transmission breaks as an effect of a path failure. Ad hoc On-demand Distance Vector Multipath (AODVM) [26] and Ad hoc On-demand Multipath Distance Vector (AOMDV) [27] are extensions to the general Ad hoc On-demand Distance Vector (AODV) routing protocol.

(3) **Confidentiality:** All drivers private information has to be confined. This security prerequisite is to ensure that confidential information will only be read by permitted users. Requirement of confidentiality is needed in group communications, where only authorized group members are allowed to read such data. Confidentiality is considered a security issue when some message contains sensitive information like session key or toll payment data, etc. [20].

(4) **Access Control:** The security mechanism must guarantee that only authorized users can access the ad hoc network resources and information provided by the certificate authority. Access control provides protection against malicious vehicle to access unauthorized services and sensitive information of certificate authority. These messages must be encrypted using cryptographic encryption techniques.

(5) **Nonrepudiation:** Nonrepudiation is a service that requires a vehicle sending a safety message to other vehicles which cannot deny having sent message [24, 25]. This requirement is important as in case of any dispute a user of the vehicle shall not deny its fault.

(6) **Privacy:** Unauthorized node should not be able to access personal information of a driver. While the information in a vehicular network is broadcast publicly, there is a big threat to privacy. An adversary can collect and analyze this information to harm the users. An eavesdropper should not have the ability to distinguish two distinct information messages which came from same node [5, 20]. The fundamental concept of privacy preservation schemes in VANET is to periodically change the pseudonyms. There exists many schemes that have been proposed by researchers in which the concept of changing pseudonym is used to preserve the privacy of user [28–36]. Data owners often suppress their data for an untrusted trainer to train a classifier due to privacy concerns. Li et al. proposed a privacy preserving solution for learning algorithms based on differentially private naive Bayes learning, allowing a trainer to build a classifier over the data from a single owner [37]. Data privacy also becomes a central consideration in vehicular networks, where outsourcing data to the cloud server is done [38]. L-EncDB is a lightweight framework for privacy preserving scheme for efficient data outsourcing [39]. Recently HybridORAM [40] scheme is proposed which provides a better solution to securely outsource data to the cloud.

3. Cyberattacks in Automotive Technology

In this section, we present a summary of various attacks on vehicular networks, which can be found in the literature [41–53]. Some of these attacks are performed by the member nodes already registered with the network and called insider attacks. When a nonregistered node carries out an attack, it is known as outsider attack. These attacks can also be categorized as active and passive attacks. In an active attack, the attacker may generate new packets to damage the network or falsify the legitimate information, while the passive attacker can only eavesdrop the channel and acquires sensitive information. We categorize these attacks according to the violation of security services provided by vehicular networks. However, some of the attacks may violate more than one security service as shown in Table 1. The following are the common types of attacks which can be harmful to the security of vehicular network.

3.1. Attacks Related to Authentication. Attacks related to authentication are performed by unauthorized nodes entering

into the network and gaining access to the network privileges or claiming illegal authority. The most frequent attacks related to authentication of vehicles are summarized as follows:

(1) **Sybil attack:** In Sybil attack a node asserts itself as several nodes by simulating multiple identities [46, 47]. An attacker sends several messages with multiple identities and announces its various positions at the same time. Multiple copies of a node create confusion in the network and hence claim all the fake and illegal authority. Sybil attacks are harmful to the network topology and cause bandwidth consumption [10].

(2) **Impersonation attack:** In this type of attack, an attacker characterizes itself as an authorized node [48]. Objective of these attacks is to either gain access to the network privileges or to disturb the network. These attacks are potentially possible through possession of false attributes or identity theft.

(3) **Bogus information:** Attackers may send fake or bogus information to the system for their own advantage. For instance, an attacker sends bogus information of a heavy traffic jam due to an accident on a certain road to make its route clear. These attacks compromise the authentication requirement of vehicular network [20].

(4) **Session hijacking:** The attacker targets unique Session Identifier (SID) allocated for each new session and may get control over that session. An attacker gets edge of the fact that authentication at the network layer is done only once. No authentication is done after generation and allocation of the SID; therefore attackers get advantage of this feature [17].

(5) **Replay attacks:** The attacker impersonates itself as a legitimate vehicle or RSU to capture information packets and then sends out the replica of the captured signal to another node for its own benefits [53]. Replay attacks are considered threat to confidentiality and authenticity of the system.

(6) **GPS spoofing:** The Global Positioning System (GPS) Satellite stores geographical locations of vehicles and their identities in form of a location table. The attacker may alter these location table readings to mislead the vehicle. Signal simulators can be used by the attacker to generate signals stronger than the actual signals generated by satellite.

3.2. Attacks Related to Network Efficiency. Attacker may try to jam the network or produces delays in communication of vehicles which severely affects the performance and efficiency of vehicular network. Time is very critical issue in a vehicular network as a small delay can result into accidents or severe traffic issues. There is a need to apply antijamming techniques for better network efficiency [54]. Some of the common attacks related to efficiency and performance of vehicular network are described as follows:

(1) **Denial of service attacks:** DoS attacks can have severe effect on the efficiency and performance of vehicular network. The attack is performed by sending dummy messages to the network and making a victim node unavailable to other legitimate users by SYN flooding, jamming, or distributed DoS attack [49].

(2) **Routing attacks:** Routing attacks generally exploit the loopholes and vulnerability in routing protocols of a network. These attacks can be categorized as follows:

(i) **Black hole attack:** In this attack, malicious node first sends false route with lower hop count to attract the source node to send packet through itself. After source node sends data packet to the route, attacking node silently drops these packets [50].

(ii) **Gray hole attacks:** Similar to black hole attack, the compromised node drops packet but this dropping is performed only on selective packets. Selection is done according to requirement and intensions of attacker [50].

(iii) **Wormhole attack:** Two or more nodes work together to make tunnels within a network. The malicious node receives the packets and routes it to the other end of the tunnel. Through this tunneling process, hop count of the route decreases and the compromised nodes attract packets. In this way attacker node gets strong position than other deserving nodes in the network and thus it can carry out DoS attacks, replay attacks, etc.

(3) **Timing attacks:** In timing attack, the attacker node creates a delay in communication by altering time slot of the received packet. Due to this alteration, the neighbors of malicious node might not receive sensitive messages on time. In vehicular network, information is time critical with respect to its sensitivity and hence a small delay can result in accidents or severe traffic issues.

(4) **Intruder attack:** An unregistered node or application tries to enter the network in order to disturb the efficiency of network or gain false attributes. Intrusion detection systems (IDSs) are widely deployed in various networks in order to identify cyberthreats and possible incidents [55]. Li et al. proposed a malware detection system based on permission usage analysis by significant permission identification technique. 3 levels of pruning by mining the permission data are developed to identify the most significant permissions [56]. These recently proposed techniques can be incorporated with vehicular networks to mitigate intruder attacks.

3.3. Attacks Related to User's Privacy. Unauthorized nodes may attempt to access sensitive data from network and target the privacy of a legitimate user. Some common attacks on the user's privacy and confidentiality requirement in a vehicular network are given as follows:

(1) **Eavesdropping:** This type of attack is a risk to confidentiality of a network. The core objective of this attack is to get sensitive and confidential data for which the attacker is not authorized [24]. It is a passive attack in which an attacker sniffs the data silently to get the confidential information and further use it for his own benefits. Vehicular networks consist of relays that may be corrupted by multiple cochannel interferers, and the information transmitted from the relays to the destination can be overheard by the eavesdropper. Fan et al. investigate the impact of cochannel interference on the security performance of multiple amplify-and-forward (AF) relaying networks [57, 58].

(2) **Location trailing attack:** Location attacks generally target the privacy of a user in vehicular network by continuously tracking the location of a user. In this attack, position of the vehicle at a given moment or path trace along certain period of time can be used to map out the user [52, 59].

(3) **Identity revealing:** Attacker may try to reveal identity of vehicle's owner. As identity of the owner represents the driver, it can be latter used by the attacker for its own illegal benefits.

4. Cryptographic Techniques for Automotive Security

Safety has a long practice in history of automotive industry. Cryptography has played a key role in securing vehicular systems. Cryptography in vehicles was introduced in Remote Key-less Entry (RKE) in the middle of 1990s, which was followed by electronic immobilizers. We have a lot of solutions in isolated systems, such as single car. Developments in automotive technology such as connected cars and vehicular networks set up new security challenges. Although security in these networks depends more than just on cryptographic algorithms, still cryptographic schemes are the basic building blocks of security solutions in automotive industry. The embedded security applications in vehicular networks tend to be computationally hard and memory constrained due to their unique characteristics as described in Section 2.2.

We present an overview of the existing cryptographic schemes with respect to their complexity. Firstly, asymmetric cryptography is mainly used for digital signatures and key distribution over unsecured channels in vehicular networks. secondly, the symmetric algorithms are used for data encryption and message integrity checks. Recently there have been researches done on the lightweight cryptographic algorithms and dynamic key generation schemes are developed to secure vehicular networks.

4.1. Asymmetric or Public-Key Algorithms. Public-key infrastructure (PKI) based algorithms involve complex mathematical computations with large numbers and hard theoretical problems (commonly in the range of 1024-4048 bits), depending on the security level of selective algorithm. However, they provide advanced functions for data encryption and integrity check. Digital signatures and key distribution schemes are used for privacy preservation in unsecured channels. Asymmetric cryptographic techniques are projected in order to protect transmitted messages and also support mutual authentication between network nodes [60]. Table 2 presents some of the common asymmetric cryptographic solutions with security requirements support and their limitations.

A security protocol based on PKI was introduced by Raya et al. in which every vehicle is equipped with several private keys and their corresponding certificates [43]. The above security scheme is inefficient and apparently cannot manage to facilitate large vehicle populations due to its computational hardness. Efficient Conditional Privacy Preservation (ECPP) protocol is proposed by Liu et al. [61]. Instead of storing many anonymous keys and certificates, ECPP protocol generates short-time anonymous keys and certificates to reduce storage requirement. However, this protocol involves complex processing to generate anonymous keys, which results in serious computational overhead. Lin et al., Studer et al., and Ying et al. proposed hash chains based authentication protocol to deal with the overhead issue [21, 62, 63].

ID-based signatures are proposed to hide real identities of vehicles [51, 64]. Biswas et al. proposed an ID-based proxy method by using signatures [64]. This authentication technique is effective but vulnerable to reveal private key. Lo et al. also proposed similar authentication protocol which is based on elliptic curve cryptography [51]. Privacy preservation schemes also use ID-based signatures to provide anonymity [62, 65, 66]. In above schemes, public keys are used as vehicles' identity, so there is no need to store certificates. However, the scheme is vulnerable to replay attack [67]. Zhang et al. showed that the above technique is also vulnerable to impersonation attacks [62]. In order to enhance the security, Zhang et al. presented a privacy preservation scheme by using improved ID-based authentication process which generates digital signatures for vehicles' anonymity. However this scheme is vulnerable to the modification attacks [68]. Moreover, the above ID-based signature techniques lead to computational overhead because of bilinear pairing calculations. Recently Qun et al. proposed linearly homomorphic signature schemes that allow performing linear computations on authenticated data [69]. Qun et al. also proposed a short homomorphic proxy signature scheme. Proxy signature schemes permit an original signer to hand over his/her signing authority to a proxy signer, so that the proxy signer can sign on behalf of the original signer [70].

Zhang et al. presented another asymmetric technique based group signature method which allows RSUs to authenticate messages from vehicles [41, 62]. Zhang et al. also proposed RSU-aided authentication method using Hash Message Authentication Codes for secure vehicular communication [71]. In the above scheme, RSU provides a symmetric key to each vehicle by a key agreement protocol. Jung et al. also presented an RSU-aided privacy preservation technique

Table 2: Asymmetric cryptographic solutions for VANET.

Asymmetric Cryptographic solutions	Security Requirements support	Limitations
Anonymous keys and certificates.	Authentication/Availability/Privacy Preservation	Computational hardness
ID-based proxy signatures	Authentication/Privacy Preservation/Non-Repudiation	Vulnerable to reveal private key
Elliptic Curve Cryptography	Authentication/Availability/Privacy Preservation	Vulnerable to replay attack
RSU-aided Authentication Methods	Authentication/Privacy Preservation	Compromise on an RSU can result in disclosure of information
Smart Cards for identification	Message authentication/privacy preserving	Storage

Table 3: Symmetric ciphers for vehicular network with respect to security requirements and attack mitigation.

Cryptographic Ciphers	Security Requirements support	Attack Mitigation
Blowfish	Authentication/Availability	Differential related-key attacks/Brute-force attack
PBAS	Authentication/Availability/Confidentiality	DoS attack, Impersonation attack
Camellia	Authentication/Availability/Privacy Preservation	Impersonation attack/DoS/Sybil attacks
CAST	Authentication/Availability/Confidentiality	Sybil/Impersonation attack/routing attacks

that assigns anonymous certificates to vehicles which helps to minimize system overhead [72]. RSU-aided schemes however become easy targets for the attackers because they are semitrusted authorities. Compromise on an RSU can result in disclosure of information.

Use of smart cards has also been suggested for authentication and identification of vehicle under active attack scenarios. Paruchuri et al. proposed smart cards in vehicular networks for message authentication [73]. Smart cards can store users private/public keys, real identity, and the related certificates. However there are limitations regarding the storage. Smart cards can only store small amount of data whereas the data required to store private/public keys, real identity, and the related certificates may exceed the capacity.

4.2. Symmetric Algorithms. Symmetric algorithms often require less memory resources and tend to run comparatively faster than asymmetric algorithms. A wealth of established symmetric algorithms exists; among those the most prominent representatives are the block ciphers: Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Other than block ciphers, there also exit several symmetric stream ciphers, which prove to be even more efficient as compared to block ciphers. Stream ciphers sometimes are preferred for embedded applications; however block ciphers are still more secure. We present the list of symmetric ciphers that are proposed to meet the security requirements of vehicular networks as shown in Table 3.

(1) **Blowfish:** Blowfish is a symmetric block cipher which was designed by Bruce Schneier in 1993 [87]. It provides an efficient encryption rate in software based embedded devices. It is equipped with variable length keys, which allows user to trade off between security and speed. A simple encryption algorithm makes it fast and efficient. Blowfish is a license-free and unpatented cipher that is available for free for almost all applications. However Blowfish cipher is vulnerable to attacks on a class of keys known to be weak [74]; therefore Blowfish users must select keys carefully. Although it suffers from weak keys attacks, there is no attack on S-boxes and subkeys generated by cipher itself. If the private key is large enough then brute-force key search is not possible. It is also secure against differential related-key attack.

(2) **PBAS:** Proxy-based Authentication Scheme (PBAS) allows proxy vehicles to authenticate multiple messages from other vehicles by using its computational capacity. This scheme helps to reduce the load on RSUs [75]. It also provides RSUs with an independent and systematic mechanism to authenticate messages from the proxy vehicle. In addition to this, PBAS is also able to negotiate session key with other vehicles to make the sensitive information confidential. PBAS scheme continues working properly, even if few proxy vehicles are compromised in the network, which makes it fault tolerant. It is an effective security scheme for efficient authentication in VANET.

(3) **Camellia:** Nippon Telegraph and Mitsubishi Electric Corporation in 2000 joined together to develop a symmetric cipher called Camellia [47, 76]. It has the same security level and processing capacity as compared to AES. It is compatible for both hardware and software implementations on common 8-bit processors as well as 32-bit processors, for instance, cryptographic hardware, smart cards, and embedded systems. Camellia provides high level security on multiple platforms for embedded systems.

(4) **CAST:** Carlisle Adams and Stafford Tavares in 1996 created a symmetric cipher which was named as CAST [77]. It is commonly a 64-bit block cipher which also allows key sizes up to 128 bits and 256 bits. CAST is used in applications of GPG and PGP as the default symmetric cipher [74]. Canadian government has approved it for the use of Secure Communication Establishment. CAST cipher has the ability to survive against linear and differential cryptanalysis attacks.

4.3. Lightweight Protocols. Based on asymmetric and symmetric cryptography, the following lightweight protocols have been designed to enhance future automotive security and meet the VANET security requirements as shown in Table 4:

(1) **ARAN:** Authenticated Routing for Ad hoc Network (ARAN) is based on Ad hoc On-demand Distance Vector (AODV) routing protocol in which the third-party CA presents signed certificate to vehicular nodes [78]. Every new node joining the network has to send request certificate to CA. All authorized nodes are provided with the public-key of CA. ARAN uses timestamps for route freshness and asymmetric cryptographic technique for secure route discovery authentication.

(2) **SEAD:** Secure and Efficient Ad hoc Distance (SEAD) vector protocol is based on dynamic destination-sequenced distance vector routing (DSDV) [79]. It

Table 4: Lightweight Protocols for vehicular network with respect to security requirements and attack mitigation.

Lightweight Protocols	Security Requirements	Attack Mitigation
ARAN	Message authentication/Integrity	Impersonation/Eavesdropping/Replay
SEAD	Authentication/Availability/Privacy Preservation	Routing/DoS/Impersonation Attacks
Ariadne	Availability/Privacy Preservation	DoS/Routing/Replay attacks
SAODV/A_SAODV	Authentication/Availability/Privacy Preservation	Impersonation/Bogus/information/Routing attack
OTC	Availability	Session hijacking
ECDSA	Authentication	Bogus information/Impersonation Attacks
RobSAD	Confidentiality/Authentication/Integrity	Sybil Attack
Holistic	Authentication/Confidentiality	Impersonation Attacks

works on one-way hash function for authentication purpose. This protocol shields against incorrect routing. Destination-sequence number is used to avoid long-lived route and ensure route freshness. The protocol applies intermediate node hashing to guarantee the authenticity of each route.

(3) **ARIADNE:** This protocol is based on Dynamic Source Routing (DSR) on-demand routing protocol [80]. Ariadne works very efficiently with symmetric cryptographic operations. It uses one-way hash function and MAC authentication for secure communication between nodes. Authorization is done by using shared key. TESLA broadcast authentication technology is source of Ariadne protocol that uses TESLA time interval for authentication and route discovery process.

(4) **SAODV:** This protocol was projected to embed security in AODV [81]. Hash functions are used to protect hop count and all messages are digitally signed to ensure authenticity of routes. However, this approach prevents the intermediate node to send any route reply even if it knows the fresh route. This problem can be solved by using Double Signature, but at the cost of system complexity increase.

(5) **A-SAODV:** An extension of secure ad hoc on-demand distance vector (SAODV) protocol was proposed that has features of adaptive reply decisions. Depending on the threshold conditions and queue length, each intermediate node can make decision to reply to source node [82].

(6) **OTC:** Generally, cookies are allotted per session for session management purpose. One time cookie (OTC) protocol is proposed to protect the system from theft of SID and session hijacking [83]. This protocol generates tokens for every request and attaches them to the request by using HMAC to avoid the reuse of token.

(7) **ECDSA:** As the name suggests Elliptical Curve Digital Signature (ECDS) Algorithm uses digital signature [84]. Asymmetric cryptographic operations with hash function provide security and authenticity to the system. The sender and receiver both require agreeing upon elliptical curve parameters.

(8) **RobSAD:** This protocol provides an efficient method for Sybil attack detection [85]. Sybil node is identified if two or more nodes have similar motion trajectories. Two different vehicles driven by different drivers cannot hold same motion patterns, because each person drives according to his own need and comfort.

(9) **Holistic protocol:** In this protocol, the authentication of every vehicle is done by RSU [86]. Vehicles are registered to RSU by sending a "Hello" message. In response, the RSU sets up a registration ID (consisting vehicle registration number and licence number) and sends it to the vehicle. Further authentication is made through certificate supplied by RSU. Data can only be shared if the node is authenticated by RSU or else the node is blocked.

4.4. Physical Layer Key Generation Schemes. There are certain attacks that may attempt to extract the private key from security devices. These types of attacks are known as side channel attacks [88]. They are performed by observing the electromagnetic radiations, power consumption, or the timing behavior of an embedded device. After collecting this information, the attacker attempts to extort the secret key by utilizing signal processing techniques. Side channel attacks approve being severe threat in the real world unless some extraordinary countermeasures are applied to generate dynamic secret keys based on physical layer. The basic advantage of generating dynamic key on physical layer is that there is no direct key distribution process involved. In the ideal condition, an eavesdropper cannot obtain any information related to the secret key [89]. Secret keys can be generated dynamically for two terminals by using random characteristics of the communication channel such as received signal strength (RSS), frequency phase information, or secrecy wiretap channel codes as shown in Figure 2. These random characteristics of channel are known as channel state information (CSI). Recently there has been focus on extracting similar feature from the channel which can be used to generate dynamic secret keys on physical layer.

The theoretical secrecy extraction characteristics from the correlation of random source were first considered in open literature in 1993 [90]. These schemes exploit random characteristics of the physical layer to share secret keys. It

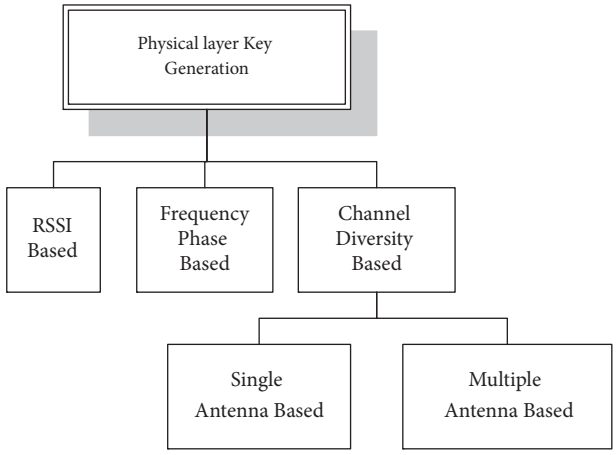

Figure 2: Physical layer key generation schemes for vehicular security.

is clearly shown that the correlated information of random sources can be used to extract secret keys by communicating over a shared channel, whereas the leaked information rate is arbitrarily low to the eavesdropper.

The best attainable secret key generation rate is defined as secret key capacity. Physical layer key generation scheme has gained significant attention in recent years due to its lightweight and information theoretic security features [88, 91–99].

The main challenge in physical layer key generation is to find a proper random source for high key generation rate. It is shown that there is a tradeoff between the public communication rate and secret key generation rate in the key agreement process [92, 93]. The random source is provided by an artificial signal and secret key is generated by the quasi-static fading channel [91]. Signals are sent if the channel state of legitimate node has better correlation than that of eavesdropper. However, the above approach contains certain assumptions that are difficult to realize in practice. Recently key generation in fast fading channels is a challenging issue and limits the application related to vehicular communications. Physical layer based key generation schemes are designed with the vehicle's maximum speed up to 50 mph but their key generation rates are limited to 5 bit/s [100, 101]. Much attention is needed in this area to develop certain schemes to improve the key generation rates. Moreover new random characteristics of the fading channel need to be explored in order to achieve higher key generation rates with more security.

4.5. Comparison. In Table 5, we present a summary of asymmetric, symmetric, and lightweight cryptographic techniques for attack mitigation and security requirements support. We also present the related references for the reader to understand these security protocols that are a foundation towards future automotive security. All protocols have their own advantages and disadvantages. A designer may select these protocols according to their own preferences. For instance some protocols provide good authentication but they are vulnerable to location based attacks; on the other hand, some protocols provide strong privacy but they are computationally complex. So there is a need to trade off for the choice of best suitable algorithms for securing the network. New standards can be developed by combining the existing protocols or use in parallel with the techniques presented in Table 5 to enhance the vehicular security.

5. Conclusion

Information technology has achieved vital significance for many new applications and services for automotive industry. The majority of innovations in cars are mainly based on software and electronic technology. Intelligent transportation systems are developed, aiming to improve the efficiency and safety of transportation systems. Security of these systems is a pivotal concern for next generation automotive technology. Conventional cryptographic algorithms such as public-key infrastructure, elliptic curve cryptography, HASH functions, and symmetric key cryptography may not be applied directly in vehicular networks due to their high mobility and dynamic network topology. Vehicular networks require real-time response and cannot tolerate delay in communication. Therefore, the conventional protocols that are developed for traditional networks fail to provide high throughput performance, low latency, and reliability for vehicular networks. So, there is a need to implement secure lightweight cryptographic algorithms on small embedded devices at acceptable execution time.

We argue that lightweight cryptographic protocols play a vital role in order to tackle the upcoming security challenges in future automotive technology, especially regarding vehicular safety and traffic efficiency. Security concerns for the future automotive industry act as a barrier in the way of extensive deployment of vehicular networks commercially. There is a need for understanding security threats and finding a solution to secure automotive technology by either building new lightweight cryptographic protocols or even using already existing algorithms in an efficient way. The public acceptance for new technology in vehicular networks can only be ensured by optimizing the security and privacy of users.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key Research and Development Program (no. 2016YFB0800602), the National Natural Science Foundation of China (NSFC) (no. 61502048), and Shandong provincial Key Research and Development Program of China (2018CXGC0701, 2018GGX106005).

Table 5: Summary of cryptographic techniques for attack mitigation and security requirements support.

	Cryptographic Solutions	Security Requirements	Attack Mitigation	References
Asymmetric Algo	Anonymous keys and certificates.	Authentication/Availability/Privacy Preservation	Eavesdropping/Replay/Impersonation attacks	[21, 63, 66, 68]
	ID-based proxy signatures	Authentication/Privacy Preservation/Non-Repudiation	Routing/DoS/Impersonation attacks	[46, 51, 62, 64]
	Elliptic Curve Cryptography	Authentication/Availability/Privacy Preservation	DoS/Routing/Replay attacks	[51]
	RSU-aided authentication method	Privacy Preservation/Authentication	Impersonation/Bogus/information Routing attack	[66, 72]
	Smart cards for identification	Message authentication/integrant/privacy preserving	Impersonation/Sybil attack	[71, 73]
Symmetric Algo	Blowfish	Authentication/Availability	Differential related-key attacks/broot force attack	[74]
	PBAS	Authentication/Availability/Confidentiality	DoS attack, Impersonation attack	[75]
	Camellia	Authentication/Availability/Privacy Preservation	Impersonation attack/DoS/Sybil attacks	[76]
	CAST	Authentication/Availability/Confidentiality	Sybil/Impersonation attack/routing attacks	[77]
Lightweight Protocols	ARAN	Message authentication/Integrity	Impersonation/Eavesdropping/Replay	[78]
	SEAD	Authentication/Availability	Routing/DoS	[79]
	Ariadne	Availability/Privacy Preservation	DoS/Routing/Replay attacks	[80]
	SAODV/A_SAODV	Authentication/Availability/Privacy Preservation	Impersonation/Bogus/information/Routing attack	[81, 82]
	One Time Cookie	Availability	Session hijacking	[83]
	ECDSA	Authentication	Bogus information/Impersonation Attacks	[84]
	RobSAD	Confidentiality/Authentication/Integrity	Sybil Attack	[85]
	Holistic	Authentication/Confidentiality	Impersonation Attacks	[86]

References

[1] T. Vaa, M. Penttinen, and I. Spyropoulou, "Intelligent transport systems and effects on road traffic accidents: state of the art," *IET Intelligent Transport Systems*, vol. 1, no. 2, pp. 81–88, 2007.

[2] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 912–925, 2018.

[3] R. Stanica, E. Chaput, and A.-L. Beylot, "Properties of the MAC layer in safety vehicular ad hoc networks," *IEEE Communications Magazine*, vol. 50, no. 5, pp. 192–200, 2012.

[4] B. Jarupan and E. Ekici, "A survey of cross-layer design for VANETs," *Ad Hoc Networks*, vol. 9, no. 5, pp. 966–983, 2011.

[5] H. Trivedi, P. Veeraraghavan, S. Loke, A. Desai, and J. Singh, "Routing mechanisms and cross-layer design for vehicular ad hoc networks: a survey," in *Proceedings of the IEEE Symposium on Computers and Informatics*, pp. 243–248, March 2011.

[6] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *Journal of Network and Computer Applications*, vol. 106, pp. 117–123, 2018.

[7] K. N. Qureshi and A. H. Abdullah, "A survey on intelligent transportation systems," *Middle East Journal of Scientific Research*, vol. 15, no. 5, pp. 629–642, 2013.

[8] S. Ahmed and S. S. Kanere, "SKVR: Scalable knowledge-based routing architecture for public transport networks," in *Proceedings of the Third ACM International Workshop on Vehicular Ad Hoc Networks (VANET '06)*, pp. 92-93, September 2006.

[9] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: its architecture, design, and characteristics," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 4, pp. 504–518, 2010.

[10] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: applications and related technical issues," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 3, 2008.

[11] C.-C. Huang-Fu, Y.-B. Lin, and N. Alrajeh, "Mobility management of unicast services for wireless access in vehicular environments," *IEEE Wireless Communications Magazine*, vol. 19, no. 2, pp. 88–95, 2012.

[12] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-vehicle communication: fair transmit power control for safety-critical information," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3684–3703, 2009.

[13] T. Tielert, D. Jiang, Q. Chen, L. Delgrossi, and H. Hartenstein, "Design methodology and evaluation of rate adaptation based congestion control for vehicle safety communications," in *Proceedings of the IEEE Vehicular Networking Conference (VNC '11)*, pp. 116–123, November 2011.

[14] G. Bansal, J. B. Kenney, and C. E. Rohrs, "LIMERIC: a linear adaptive message rate algorithm for DSRC congestion control," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 9, pp. 4182–4197, 2013.

[15] J. Xu, L. Wei, Y. Zhang, A. Wang, F. Zhou, and C. Gao, "Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures," *Journal of Network and Computer Applications*, vol. 107, pp. 113–124, 2018.

[16] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET 1," *International Journal of Computer Science and Network*, vol. 2, no. 1, pp. 88–96, 2013.

[17] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[18] J. Blum and A. Eskandarian, "The Threat of Intelligent Collisions," *IT Professional*, vol. 6, no. 1, pp. 24–29, 2004.

[19] T. S. Rappaport, *Wireless Communications: Principles and Practice*, vol. 2, Prentice Hall PTR, New Jersey, NJ, USA, 1996.

[20] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Computer Communications*, vol. 44, pp. 1–13, 2014.

[21] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 574–588, 2009.

[22] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3339–3348, 2013.

[23] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "The TESLA broadcast authentication protocol," *Rsa Cryptobytes*, vol. 5, no. 2, pp. 2–13, 2005.

[24] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[25] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 6, pp. 2985–2996, 2015.

[26] Z. Ye, S. Krishnamurthy, and S. Tripathi, "A framework for reliable routing in mobile ad hoc networks," in *Proceedings of the Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM '03)*, pp. 270–280, San Francisco, Calif, USA, 2003.

[27] M. K. Marina and S. R. Das, "On-demand multipath distance vector routing in ad hoc networks," in *Proceedings of the 9th International Conference on Network Protocols (ICNP '01)*, pp. 14–23, November 2001.

[28] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: why simple pseudonym change is not enough," in *Proceedings of the IEEE/IFIP International Conference on Wireless On-Demand Network Systems and Services (WONS '10)*, pp. 176–183, February 2010.

[29] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: robust location privacy scheme for VANET," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 8, pp. 1569–1589, 2007.

[30] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: a practical pseudonym changing scheme for location privacy in VANETs," in *Proceedings of the IEEE Vehicular Networking Conference (VNC '09)*, pp. 1–8, IEEE, Tokyo, Japan, October 2009.

[31] Z. Huang, S. Liu, X. Mao, K. Chen, and J. Li, "Insight of the protection for data security under selective opening attacks," *Information Sciences*, vol. 412-413, pp. 223–241, 2017.

[32] Y. Wei and Y. Chen, "Safe distance based location privacy in vehicular networks," in *Proceedings of the 71st Vehicular Technology Conference*, pp. 1–5, Taipei, Taiwan, May 2010.

[33] B. Palanisamy and L. Liu, "Attack-resilient mix-zones over road networks: architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 14, no. 3, pp. 495–508, 2015.

[34] R. Yu, J. Kang, X. Huang, S. Xie, Y. Zhang, and S. Gjessing, "MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 1, pp. 93–105, 2016.

[35] X. Zhang, Y. Tan, C. Liang, Y. Li, and J. Li, "A covert channel over VoLTE via adjusting silence periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.

[36] H. Li, H. Zhu, and D. Ma, "Demographic information inference through meta-data analysis of wi-fi traffic," *IEEE Transactions on Mobile Computing*, vol. 17, no. 5, pp. 1033–1047, 2018.

[37] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private Naive Bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89–104, 2018.

[38] X. F. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2386–2396, 2014.

[39] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: a lightweight framework for privacy-preserving data queries in cloud computing," *Knowledge-Based Systems*, vol. 79, pp. 18–26, 2015.

[40] B. Li, Y. Huang, Z. Liu, J. Li, Z. Tian, and S. Yiu, "HybridORAM: practical oblivious cloud storage with constant bandwidth," *Information Sciences*, 2018.

[41] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*, vol. 2429 of *Lecture Notes in Computer Science*, pp. 251–260, Springer, Berlin, Germany, 2002.

[42] G. Guette and B. Ducourthial, "On the Sybil attack detection in VANET," in *Proceedings of the Internatonal Conference on Mobile Adhoc and Sensor Systems (MASS '07)*, pp. 1–6, October 2007.

[43] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[44] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS '12)*, pp. 1–9, Queensland, Australia, December 2012.

[45] S. Sharma, "A review: analysis of various attacks in VANET," *International Journal of Advanced Research in Computer Science*, vol. 7, no. 3, pp. 249–253, 2006.

[46] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—(CRYPTO 2001)*, vol. 2139 of *Lecture Notes in Computer Science*, pp. 213–229, Springer, 2001.

[47] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support," *Security and Communication Networks*, vol. 6, no. 4, pp. 523–538, 2013.

[48] T. W. Chim, S. M. Yiu, L. C. Hui, and V. O. Li, "Security and privacy issues for inter-vehicle communications in VANETs," in *Proceedings of the 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops (SECON Workshops' 09)*, pp. 1–3, Rome, Italy, June 2009.

[49] Y. Kim, I. Kim, and C. Y. Shim, "A taxonomy for DOS attacks in VANET," in *Proceedings of the 14th International Symposium on Communications and Information Technologies (ISCIT '14)*, pp. 26-27, September 2014.

[50] A. Rathod and S. Patel, "A survey on black hole & gray hole attacks detection scheme for vehicular ad-hoc network," *International Research Journal of Engineering and Technology*, vol. 04, no. 11, pp. 1508–1511, 2017.

[51] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2016.

[52] A. Prado, S. Ruj, and A. Nayak, "Enhanced privacy and reliability for secure geocasting in VANET," in *Proceedings of the 2013 IEEE International Conference on Communications (ICC '13)*, pp. 1599–1603, June 2013.

[53] Q. G. Fan, L. Wang, Y. N. Cai et al., "VANET routing replay attack detection research based on SVM," *Matec Web of Conferences*, vol. 63, p. 05020, 2016, EDP Sciences.

[54] H. Zhu, C. Fang, Y. Liu, C. Chen, M. Li, and X. S. Shen, "You can jam but you cannot hide: defending against jamming attacks for geo-location database driven spectrum sharing," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 10, pp. 2723–2737, 2016.

[55] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: a review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[56] J. Li, L. Sun, Q. Yan, Z. Li, W. Srisa-an, and H. Ye, "Significant permission identification for machine learning based android malware detection," *IEEE Transactions on Industrial Informatics*, no. 99, 2018.

[57] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1494–1505, 2016.

[58] X. Lai, W. Zou, D. Xie, X. Li, and L. Fan, "DF relaying networks with randomly distributed interferers," *IEEE Access*, vol. 5, pp. 18909–18917, 2017.

[59] H. Li, H. Zhu, S. Du, X. Liang, and X. Shen, "Privacy leakage of location sharing in mobile social networks: attacks and defense," *IEEE Transactions on Dependable and Secure Computing*, no. 99, 2016.

[60] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 49–55, 2004.

[61] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 1229–1237, April 2008.

[62] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 246–250, April 2008.

[63] B. Ying, D. Makrakis, and H. T. Mouftah, "Privacy preserving broadcast message authentication protocol for VANETs," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1352–1364, 2013.

[64] S. Biswas and J. Misic, "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2182–2192, 2013.

[65] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[66] X. Lin, X. Sun, X. Wang, C. Zhang, P.-H. Ho, and X. Shen, "TSVC: timed efficient and secure vehicular communications

with privacy preserving," *IEEE Transactions on Wireless Communications*, vol. 7, no. 12, pp. 4987–4998, 2008.

[67] C.-C. Lee and Y.-M. Lai, "Toward a secure batch verification with group testing for VANET," *Wireless Networks*, vol. 19, no. 6, pp. 1441–1449, 2013.

[68] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Expert Systems with Applications*, vol. 41, no. 5, pp. 2559–2564, 2014.

[69] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[70] Q. Lin, J. Li, Z. Huang, W. Chen, and J. Shen, "A short linearly homomorphic proxy signature scheme," *IEEE Access*, vol. 6, pp. 12966–12972, 2018.

[71] C. Zhang, X. Lin, R. Lu, and P.-H. Ho, "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 1451–1457, May 2008.

[72] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: a robust signature scheme for vehicular networks using Binary Authentication Tree," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974–1983, 2009.

[73] V. Paruchuri and A. Durresi, "PAAVE: protocol for anonymous authentication in vehicular networks using smart cards," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, pp. 1–5, December 2010.

[74] M. Alimohammadi and A. Pouyan, "Performance analysis of cryptography methods for secure message exchanging in VANET," *International Journal of Scientific &Engineering Research*, vol. 5, no. 2, pp. 911–917, 2014.

[75] W. Huang, Y. Xiong, and D. Chen, "DAAODV: a secure ad-hoc routing protocol based on direct anonymous attestation," in *Proceedings of the 7th IEEE/IFIP International Conference on Computational Science and Engineering (CSE '09)*, pp. 809–816, August 2009.

[76] S. Chang, Y. Qi, H. Zhu, J. Zhao, and X. Shen, "Footprint: detecting Sybil attacks in urban vehicular networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 1103–1114, 2012.

[77] C. Adams, "The CAST-128 encryption algorithm," 1997, https://dl.acm.org/citation.cfm?id=RFC2144.

[78] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A secure routing protocol for ad hoc networks," in *Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP '02)*, pp. 78–87, IEEE, Paris, France, November 2002.

[79] P. Mutalik, S. Nagaraj, J. Vedavyas, R. V. Biradar, and V. G. C. Patil, "A comparative study on AODV, DSR and DSDV routing protocols for Intelligent Transportation System (ITS) in metro cities for road traffic safety using VANET route traffic analysis (VRTA)," in *Proceedings of the 2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT '16)*, pp. 383–386, December 2016.

[80] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, no. 1-2, pp. 21–38, 2005.

[81] M. G. Zapata and N. Asokan, "Securing ad hoc routing protocols," in *Proceedings of the 1st ACM Workshop on Wireless Security*, pp. 1–10, Atlanta, GA, USA, September 2002.

[82] D. Cerri and A. Ghioni, "Securing AODV: the A-SAODV secure routing prototype," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 120–125, 2008.

[83] I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, "One-time cookies: preventing session hijacking attacks with stateless authentication tokens," *ACM Transactions on Internet Technology*, vol. 12, no. 1, pp. 1–24, 2012.

[84] S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, "Message authentication in vehicular ad hoc networks: ECDSA based approach," in *Proceedings of the International Conference on Future Computer and Communication (ICFCC '09)*, pp. 16–20, April 2009.

[85] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban VANETs," in *Proceedings of the 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS Workshops '09)*, pp. 270–276, Montreal, Quebec, Canada, June 2009.

[86] K. S. TamilSelvan and R. Rajendiran, "A holistic protocol for secure data transmission in VANET," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 6, pp. 2278-1021, 2013.

[87] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," in *Fast Software Encryption*, vol. 809 of *Lecture Notes in Computer Science*, pp. 191–204, Springer, Berlin, Germany, 1994.

[88] S. Watanabe and Y. Oohama, "Secret key agreement from correlated gaussian sources by rate limited public communication," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 93, no. 11, pp. 1976–1983, 2010.

[89] B. Yang and J. Zhang, "Physical layer secret-key generation scheme for transportation security sensor network," *Sensors*, vol. 17, no. 7, p. 1524, 2017.

[90] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[91] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[92] T.-H. Chou, S. C. Draper, and A. M. Sayeed, "Key generation using external source excitation: capacity, reliability, and secrecy exponent," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 58, no. 4, pp. 2455–2474, 2012.

[93] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited public communication," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 541–550, 2011.

[94] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 58, no. 6, pp. 3373–3391, 2012.

[95] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 650–660, 2011.

[96] H. Zhou, L. M. Huie, and L. Lai, "Secret key generation in the two-way relay channel with active attackers," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 476–488, 2014.

[97] T.-H. Chou, S. C. Draper, and A. M. Sayeed, "Secret key generation from sparse wireless channels: ergodic capacity and secrecy outage," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1751–1764, 2013.

[98] M. Wilhelm, I. Martinovic, and J. B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1779–1790, 2013.

[99] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 58, no. 11, pp. 6747–6765, 2012.

[100] J. Wan, A. B. Lopez, and M. A. Al Faruque, "Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security," in *Proceedings of the ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS '16)*, pp. 1–10, Vienna, Austria, April 2016.

[101] X. Zhu, F. Xu, E. Novak, C. C. Tan, Q. Li, and G. Chen, "Using wireless link dynamics to extract a secret key in vehicular scenarios," *IEEE Transactions on Mobile Computing*, vol. 16, no. 7, pp. 2065–2078, 2017.