Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 32, S. 1121-1128, Aralık 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 32, pp. 1121-1128, December 2021

Research Article

Cyber Security of Connected Autonomous Vehicles

Kürşat Çakal[1*], İlker Kara[2], Murat Aydos[3]

[1*] Hacettepe University, Faculty of Engineering, Departmant of Computer Engineering, Ankara, Turkey, (ORCID: 0000-0002-9116-4910), kursatckl@gmail.com
[2]Dept. of Medical Services and Techniques, Eldivan Medical Services Vocational School Çankırı Karetekin University, Turkey (ORCID: 0000-0003-3700-4825), karaikab@gmail.com
[3]Hacettepe University, Faculty of Engineering, Departmant of Computer Engineering, Ankara, Turkey, (ORCID: 0000-0002-7570-9240), maydos@hacettepe.edu.tr

(International Conference on Design, Research and Development- 15 – 18 Aralık 2021)

(**DOI:** 10.31590/ejosat.1039449)

ATIF/REFERENCE: Çakal, K., Kara, İ. & Aydos, M. (2021). Cyber Security of Connected Autonomous Vehicles, *European Journal of Science and Technology*, (32), 1121-1128.

Abstract

Importance of communication security in vehicular network systems is a soaring issue with the evolving automotive industry day by day. The proposed study covers fundamental requirements to ensure automotive system security and some cryptography algorithms that can be beneficial for the security of connected cars from our point of view. Autonomous systems use lots of IoT sensors data. Connected vehicles have a data-sharing network and they are vulnerable to security attacks. So, ensuring the security of these data is an important challenge. The main purpose of this study is to draw attention to the basic security elements of communication between interconnected vehicles, to touch on its daily importance and usage points in human life, and to present the research on possible cryptography methods that can be used by giving information about the current studies. Our research focuses on ensuring both powerful securities infrastructure methods and considering hardware-based conditions. Different approaches, cryptography algorithms, protocols, and real-life companies that dive into autonomous system security challenges are tackled in this study. In addition, some of the important methods and applications are presented in a table from two different perspectives as attack mitigation and security requirements support that are thought to contribute to literature studies.

Keywords: VANET, MANET, Lightweight, RSU, OBU, CIA, GPS, ECU, TA, ARX, NSA

Bağlantılı Sürücüsüz Araçların Siber Güvenliği

Öz

Araç ağ sistemlerindeki haberleşme güvenliğinin önemi, gelişen otomotiv endüstrisi ile her geçen gün önemi artan bir konudur. Önerilen çalışma, otomotiv sistem güvenliğini sağlamak için temel gereksinimleri ve bizim açımızdan bağlantılı araçların güvenliği için faydalı olabilecek bazı kriptografi algoritmalarını kapsamaktadır. Otonom sistemler çok sayıda IoT sensör verisi kullanır. Bağlı araçlar bir veri paylaşım ağına sahiptir ve güvenlik saldırılarına karşı savunmasızdır. Dolayısıyla, bu verilerin güvenliğini sağlamak önemli bir zorluktur. Bu çalışmanın temel amacı, birbirine bağlı araçlar arasındaki iletişimin temel güvenlik unsurlarına dikkat çekmek, günlük önemine ve insan hayatındaki kullanım noktalarına değinmek ve kullanılabilecek olası kriptografi yöntemleri hakkında bilgi vererek araştırmayı sunmaktır. mevcut çalışmalar hakkında. Araştırmamız, hem güçlü menkul kıymetler altyapı yöntemlerinin sağlanmasına hem de donanıma dayalı koşulların dikkate alınmasına odaklanmaktadır. Bu çalışmada, otonom sistem güvenlik sorunlarına dalan farklı yaklaşımlar, kriptografi algoritmaları, protokoller ve gerçek hayattaki şirketler ele alınmaktadır. Ayrıca literatür çalışmalarına katkı sağlayacağı düşünülen bazı önemli yöntem ve uygulamalar saldırı azaltma ve güvenlik gereksinimleri desteği olarak iki farklı açıdan bir tablo halinde sunulmuştur.

Anahtar Kelimeler: VANET, MANET, Lightweight, RSU, OBU, CIA, GPS, ECU, TA, ARX, NSA

[*] Corresponding Author: kursatckl@gmail.com

1. Introduction

Over the last decade, the automobile industry has equipped with lots of IoT devices. Autonomous vehicles will be our life both as aerial and terrestrial and they will be vulnerable to data theft and hacking in the near future [1]. Ensuring security of data is critical issue for vehicular communication because of intelligent vehicles has data sharing networks [2]. There are two main point to ensure security for autonomous vehicles. Firstly, embedded electronic sensor systems such as steering angle, lidars, stereo cameras and brake mechanism have risks based on intrusion attacks by hackers. Secondly, communication systems, it is related such topics between the central coordination of vehicles, personal authentication, remote control call-back mechanism and location confidentiality. These developments cause cars to have a smart network. We have to look up VANET terminology to understand this smart network. This network exclusively means Vehicular Ad-Hoc Network that is a form of MANET. Fundamental elements of VANET are respectively On-Board Units (OBU) and Road-Side Units (RSU) that interact with sensors of the car. OBU is electronic device that consist different sub-systems such as GPS, Wi-Fi and Machine Interface. Vehicles has OBU to ensure communication with peripheral RSUs. RSU is a device that mounted at major places along the road. It ensures data sharing and channel assignment capability for communication between OBU in the scope. According to [3] VANET's main characteristics respectively are High mobility, Time Critical Data Exchange, Dynamic Network Topology, Computing Capacity and Energy Storage. Each unit or system object in the VANET performs both transmit and receive messages along communication network. The main process of the system operates in itself with Vehicles, OBUs, RSUs, and also other objects from life as shown in Figure 1. Breaking of the vehicle system, swarm driving that consist of the coordinated task of vehicles that shares acceleration and steering information between themselves, traffic information systems that provide real reports about accidents and jam, emergency services that provide road safety status information, warnings about infrastructure work around destination, rescue operations and sanitary transportation services are some of the important lifetime scenarios of VANET that affects humankind's daily life. It also affects lots of processes such as fast shopping, fuel intake, and restaurant needs that are human-centered. This is why the future of transportation will be information-driven and based on wireless interactive.

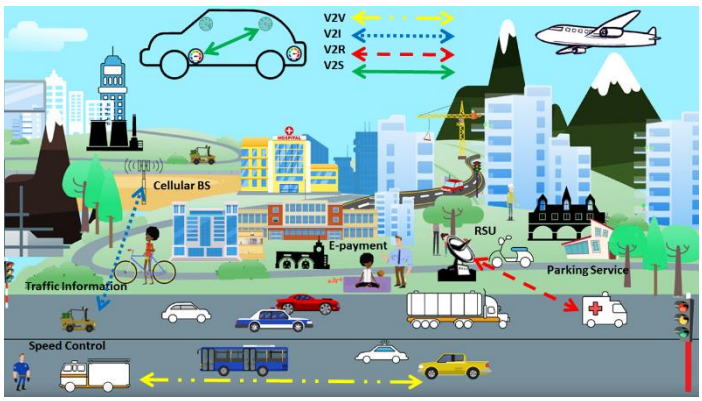

Figure 1. Nominal Estates of VANET [30]

Today's transportation technologies are mostly designed on intelligent systems. Main requirements of Intelligent Transportation Systems(ITS) are ensuring accessibility, efficiency, availability and confidentiality of relation between human life and automotive technology. There are too many competitions in both industrial consortiums and the academic communities to ensure effectiveness of the implementation plan of the relation between human life and automotive technology. It mainly relies on information sharing network of vehicles. This system ensures important advantages in such topic Safety Warnings, Dynamic Transportation Flow Services and Driving Boundaries. Safety Warning means accident reports and warning of road anomaly. Dynamic Transportation Flow Services means Emergency Vehicle Prioritization, Highway Information, interaction of multiple rescue team, urban surveillance, vehicle evacuation, route reservation and traffic light prioritization. For instance, traffic jams always can occur in daily life. Ambulances are also parts of the system, but the vehicle in front of an ambulance in this situation does not know that how it restricts the ambulance journey. Therefore, ITS can easily solve informing other vehicles by RSU. Driving boundaries means such topics Road Congestion, Government's Traffic Director Set Upper-Lower Limit for Speed by RSU, Identity-Based Traffic Controls, Traffic Flow Jams Reports by data stored in RSU, Weather information from base station services such secret icing temperature precipitation, Vehicular location and Path planning. As an important example, think that there is a identity-based control against a terrorism fact, it can be so easy to detect unexpected intrusion with the help of VANET because all of the cars in the traffic has an unique and real identity except from if there is a stolen-record belong to the car. As other soft example, there is a secret icing in the route of our destination but driver don't know whether exist, in this situation RSU can beacon by Weather Services or another driver that aware about the situation and it can make easier to understand by all other user with notifications. Although there are lots of advantages of this sophisticated vehicular network, there is a main concern about if all of the advantage use in malicious purpose such as malicious routing (reserving highways for its own purposes by infiltrating to RSU), the privacy of private life (obtaining specific people's location) and theft (breaking into remote keyless authentication). So, from now on, autonomous cars will become more like computers than mechanical structures. As you understand, with the help of these connected cars network architecture with their vulnerabilities. Information exchange process between the connected vehicles by ensuring CIA triad is the key concerns for traffic safety due to the availability of potential unauthorized access to the system. This exchange process includes mainly topics such as car's acceleration, steering, positional and identity-based privacy.

Vehicle industry has undergone a tremendous transformation in connectivity. Autonomous vehicles include many sensors information share between vehicle-vehicle, vehicle-satellite and vehicle-people such as software updates, accidental, traffic jam, speed, coordinate and authentication-based key information. All these communication channels needs to be protected against intruder to ensure the security of system. ITS have both OBU and RSU connectivity to ensure communication between vehicles. This connectivity opens up vehicles to the Network Security and Information Technology disciplines where the cyber dangers are constantly growing and complicated. Cyber Security Attacks are a prominent challenge to be focused on for Self-Driving Connected Vehicles [31-32]. In a nutshell, providing adequate cyber security features is very important. According to [2], vehicular networks have high topology. In vehicular network channel transmission delays can not tolerate because of their

topology has quick operating structure based on real time. That's why conventional security approaches for computing devices on traditional network isn't suitable to ensure such requirements reliability, high throughput and low latency. For this reason, lightweight methods have to implement our system and these methods have to be hardware-friendly to compensate execution time requirements. We focus lots of lightweight protocols, frameworks and algorithms in this research. Also, we compare these methods in terms of Security Requirements and Attack Mitigation.

2. Material and Method

2.1. Attacks On Data-Driven Vehicular Network

A general summary of the attacks on connected vehicle network presented under this heading. Actually, there are too many attack types in VANET as in normal network topology but we will emphasize the most important ones to understand the significance of future investment on this topic. However, lots of attack types can be derivable from current situation because of VANET directly affecting our life.

2.1.1. DoS Attacks

In DoS attack, intruders can create bottlenecks in the transmission medium and it causes to inability to serve network's to legitimate users. There are too many helping area of VANET for human in daily critical issues. So, operability of VANET is crucial factor for our daily life to obtain effective solutions of it. Malicious purposes can intrude our operating flow as connectivity. As you see in the Fig 2. Intruders can be involve and occupy of intelligent communication of transportation.

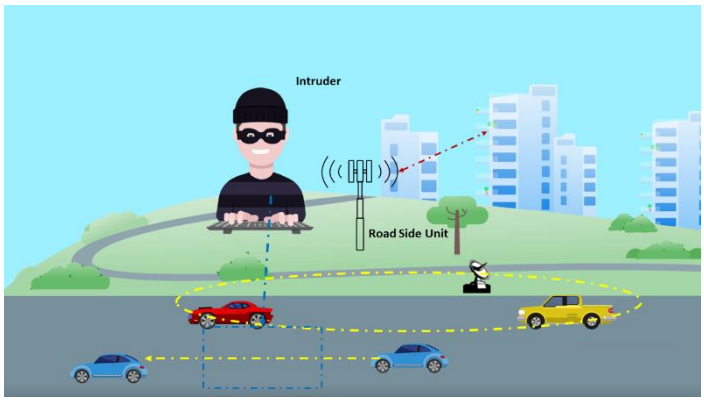

Figure 2. DDoS Attacks [29]

2.1.2. Node Impersonation Attacks

This type of attack based on imitating other one in traffic. It includes two form as invisible node attacks and stolen identity attacks. In invisible node attacks, intruder node X either act to A as if B or acts to B as if A while A-B communicating smoothly. So, intruders can access two sides of information and act as bridges between sides. In a Stolen Identity attack, intruder X acquires identity on any of the sides between A and B. The authorized node will be invalid if the intruder node can be surpassed the authorized node during the update of stolen credentials.

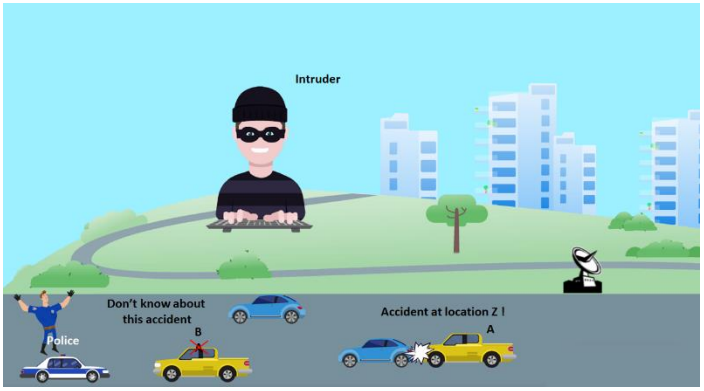

Figure 3. Node Impersonation Attacks [29]

2.1.3. Location Attacks

Other critical attack is location-based attacks because intruders can violate privacy of drivers and also can cause conspiratorial, theft and other similar purpose attempts. In fact it is a type of monitoring attack, tracking attacks target the coordinates of user at a given time. They trace user's path by taking coordinates constantly and mapping them.

2.1.4. Timing Attacks

Attackers do not interested in read or change data content or any feature of the data. Attacker only plans to create delay in original message. As you see in Fig 4. Attacker causes to delay in accidental report between vehicles and VANET get away from its main serving purposes.

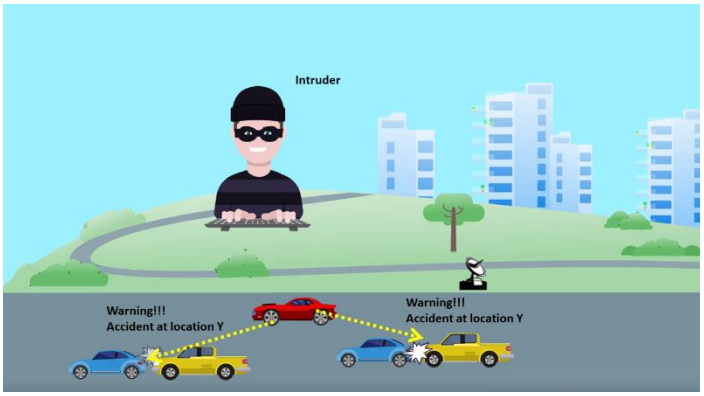

Figure 4. Timing Attacks [29]

2.1.5. Social Attacks

This type of attacks are opportune to creating hostility between drivers and disrupting traffic flow. Shown in Fig 5. it is based on effecting emotions and creating angry behaviours. There are too many areas that can be cause to confusion in traffic with the help these attacks.

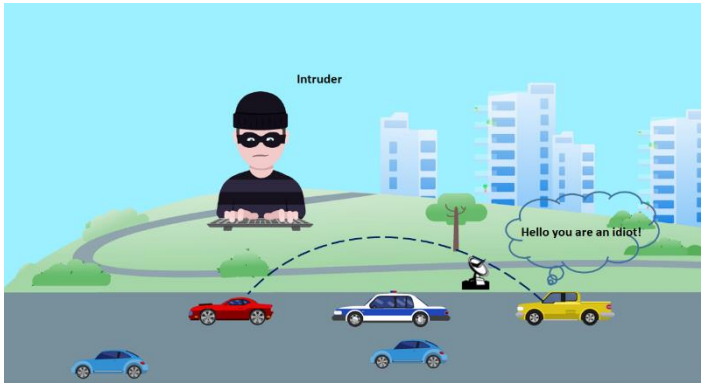

Figure 5. Social Attacks [29]

2.1.6. Application Attacks

VANET has lots of application as mentioned introduction such as safety warnings, public services and driving boundaries. This type of attacks directly target to change positive functionalities of VANET apart from DDoS that passivate functionalities. For example, there is an ambulance in highway it is an emergency situation VANET architecture can notify "clear path ambulance alert" to required driver this information but intruders can block this functionality by changing actual state to "no ambulance".

Figure 6. Application Attacks [29]

2.1.7. Sybil Attacks

Intruders mainly focus on misleading multiple vehicles in other directions and provoking their decisions to tend other routes for clearing out the way for their own purposes. As you see in Fig 7. Attacker creating imaginary car on the road for RSU and RSU send messages other RSU about the congestion. Then, vehicle changes their direction to another path by a misleading attackers.

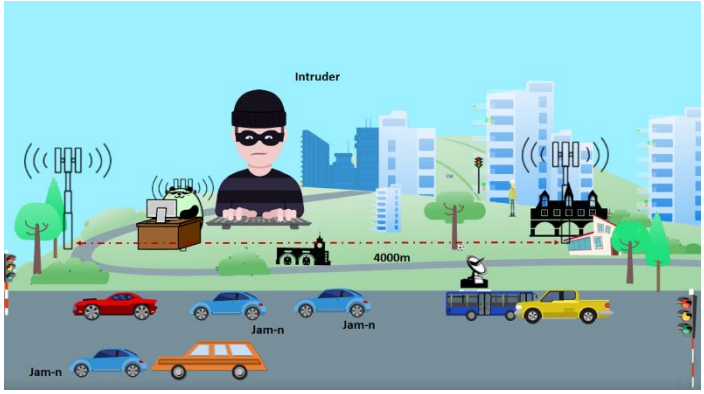

Figure 7. Sybil Attacks [29]

2.2. Lightweight Approaches for Ensuring Security of Vehicular Networks

Any of the proposed protocols or cryptographic approaches can not enough to ensure security in a vehicular network because of the existence of different demands in the vehicular network. In this section we present both proposed protocols for directly securing VANET and also algorithms that can be use in VANET protocol that will develop near feature.

2.2.1. Lightweight Protocols for VANET

The first one of the tackled point is AUTOSAR. It is a stack of standard that has important security opportunities to implement into the vehicle system these implementations are both hardware and software level. Actually, AUTOSAR is a de facto standard. Manufacturers can develop software-based solutions independently from hardware architecture to run their software on any ECU (Engine Control Unit) by adopting these standards as a base [7]. Secure On-Board Communication, Crypto Abstraction Library, and Service Manager are the main keystones and mechanisms of AUTOSAR. Crypto Service Manager allows different applications to access different cryptographic algorithms by using same services. The second crypto module Crypto Abstraction Layer provides the functionality of cryptographic operations directly on run-time. The Secure On-Board Communication module operates authentication mechanism for critical data.

A blockchain-based intelligent communication approach is proposed as a crypto IV-TP framework in [8]. The presented framework improves the privacy and secrecy of intelligent communication between vehicles by proving fast and secure infrastructure. In addition, IV-TP ensures detection of the detailed history of intercommunication by storing data will on the VC (Vehicular Cloud) if the user wants. IV-TP is a seven-layer conceptual model and it uses crypto-layer with hash algorithms, Merkle Tree to make secure blocks.

The CUBE [9] is tree-layer sophisticated technology platform that ensures data protection between connected cars on vehicular network. It has layers respectively Blockchain Layer, AI Deep Learning Layer and Quantum Hash Cryptography Layer to secure whole system of Autonomous Communication. CUBE use blockchain layer because of the problems in conventional security methods such centralization, privacy and safety issue. The main security mechanism in CUBE is based on blockchain now. However, designers of the proposed stack think that security is under an important risk if processing power and speed increase dramatically in the computer industry. So, designers include Quantum Hash Cryptography technology in CUBE with a visionary approach to improve security. Furthermore, deep learning based network security is another part of CUBE. This part of the security mechanism is a crucial and proactive point because it has prediction-based attack mitigation or detection against intruders rather than traditional approaches. CUBE puts Artificial Intelligence into its services in a way that allows learning from previous attacks and intrusions by predicting new possible cyber-crimes.

Another proposed study is the ARAN protocol. This protocol focuses to ensure routing security between connected vehicles and side units in VANET by using cryptographic certificates [10]. The main services of the protocol are authentication and non-repudiation for securing route operations by using predefined cryptographic certificates that have certainty for verifying end-to-

end identities. Thus, ARAN mitigates intrusion attacks that can affect other risky protocols at an important level.

Hop-by-hop protocol for verifying identities in ad hoc networks proposed as LHAP in [11]. The implementation point for LHAP starts after the data link layer and ends before the network layer. Thus, it provides layered protection against intruders as well as impersonation attacks from inside the system. LHAP uses a packet verification technique by using one-way hash chains. Also, LHAP has Timed Efficient Stream Loss-Tolerant Authentication. It reduces count of asymmetric key operations and maintains reliance between nodes. It is not dependent any of the routing protocols of network architecture. Performance and competence of LHAP has dominance over conventional packet authentication and trust management based protocols. Every node in this approach is authenticated with its own path. So, the packet authentication method is as expensive as possible in LHAP.

Chun Hu et al. presented a new protocol named SEAD in [12] as well as evaluation process and design details of it. Secure Efficient Ad Hoc Distance vector routing is tempered against multiple distributed attackers that forms inoperative routing state for any node. SEAD employs hash functions with one-way in efficient manner. It does not use public key cryptography operations to strengthen and make efficient the limited processing power of CPU. It also provides resistance against Denial of Service attacks that cause bandwidth or processing time to be exceeded.

Another proposed method by Hu et al. is ARIADNE. The proposed study covers the design details and performance metrics evaluation of a new trustworthy routing protocol for ad hoc networks. It primarily utilize Timed Efficient Stream Loss-Tolerant Authentication protocol with immensely effective private-key symmetric cryptography principles. ARIADNE ensures security against attackers or intruder hob from interference. Also, it eliminates Denial-of-Service attacks. It uses hash function with one-way to handle nodes whether it was omitted or not, and MAC authentication for safe data transmission between nodes.

Chen et al. [14] presented RobSAD. It is an effective and new mechanism to recognize Sybil Attacks within the limited topology of VANET. RobSAD ensures detection for each node independently against Sybil Attacks by using digital signature vector comparison operations between adjacent nodes. RobSAD algorithm is stronger than other methods that need to be establish collaboration between adjacent nodes in architecture with the help of these vector operations.

Other study related with connected car security is that Holistic protocol proposed by Selvan et al in [15]. Firstly, cars should be enroll to the nearest RSU by using personal identity and password. Then, RSU assigns Registration ID to people that consist vehicle registration and licence number. After that, RSU authenticate to the car via provided identity. Data transfer between parts is possible when the authentication is successful or not possible when it is fail. This case is blocked case for data and node. Holistic protocol means concerning with entire part of system versus specific parts.

One of the other proposed study is that Ad Hoc On Demand Vector (AODV) protocol for routing operations in [16]. This study proposed for ad-hoc and mobile networks that performs routing operations only between nodes which demands to data transfer. However, there are some security flows in AODV according to [15]. Two main mechanism attached in AODV to ensure security. First one is digital signatures to maintain authentication of the constant parts of the data. Second mechanism maintains security for node count information that uses hash chains. This Secure-AODV approaches constitute problem about intercepting the intermediate node events to transmit route response event if it aware about the live path. Issue can be solve by using multiple signature with causing expense of system increasing. In addition to SAODV, Cerri et al. [17] proposed a safe Ad-Hoc Distance Vector Extension based on adaptive reply decisions. In A-SAODV each node make own decision to replay source node depending queue status and threshold variable.

Tat Wing et al. proposed SPEC communication schemes in [18] that enhance security and privacy of data transmission for VANETs. SPEC handles ad-hoc and group messages for communication between connected cars. It is a software-based solution. SPEC makes possible signature verification process for RSU. Thrusted Authority in the system generates public parameters accessible among all RSUs and vehicles. SPEC includes six modules respectively handshaking for initial, signing for messages, batch verification, identity tracking and revocation in real manner, group message verification and signing. SPEC is first proposal as group communication protocol that empower known vehicles to create a community for safe data transmission. This approach gives at least more than 45% successful rate and lower message overhead than previous works in terms of effectiveness.

2.2.2. Lightweight Cryptography Techniques for VANET

Throughout the research lots of approaches seen that develop to ensure the security of VANET that are named “Lightweight” but based on traditional cryptography algorithms such as RSA, AES, SHA, MD5 and etc. So, the main focus of this study is to find new core pieces to be able to develop new Lightweight Vehicular Security approaches that are based on both effective security and also hardware friendly. Below we choose some of the suitable cryptographic algorithms considering some of the implementation properties such as their security level, throughput, and power consumption. Common features of these lightweight cryptographic algorithms are that they are intended to be efficient as well as ensure adequate security levels on limited hardware resources.

The PRESENT [19] is a block cipher method of under Lightweight Cryptography. PRESENT is Poschmann's PhD Thesis and it introduced in 2007 by Orange Labs. Prominent aspect of this method is its hardware efficiency in the design objective. PRESENT is a 31 rounded cryptographic network structure based substitution and permutation operations. It has 64 bits block length, 80-bit and 128-bit key support. Despite many SPN-based cipher similar to AES, PRESENT has explicit hardware implementation that use simple wiring transactions although bit-based permutation operations are not fine for software. It has 11.4/200(Kb/s @ 100kHz) throughput as well as 1.4/3.67 μW power consumption.

The PRINCE [20] is a Substitution Permutation Network based method. Low latency is the master point for design phase of PRINCE. It has a 128-bit master key that provides reproduction of three 64-bit keys and a real key schedule mechanism is not exist in PRINCE. Two of derived keys used intended to increase the security of an iterated block cipher keys and the third is simply applied xor during encryption. Each of the PRINCE has rounds key addition, S-Box layer, linear layer and round constant

addition. It has 529.9/533.3 (Kb/s @ 100kHz) throughput and 4.5/5.8 μW power consumption.

The SPARX proposed by Daniel et al. for the first time in [21]. It provides strength approach against differential and linear cryptanalysis with Addition/Rotation/XOR design strategy based private key. SPARX has 32-bit ARX-based(Addition-Rotation-XOR) S-boxes and has provable bounds against differential and linear cryptanalysis. The non-linearity is provided by both its key addition and also by SPECKEY. In addition, SPARX is very efficient on embedded platforms. Its optimized software implementation exists among the top best efficient ciphers such as LEA, RECTANGLE, Chaskey, Simon and Speck.

Ray et al. proposed the SIMON/SPECK twin [22]. National Security Agency designed these ciphers. SIMON/SPECK aims to fill the need for secure, flexible, and analyzable lightweight block ciphers despite many lightweight block ciphers is exist that operate data encryption/decryption processes fine with a single platform versus not providing good performance other devices. This twin aims to offer security on constrained devices where simplicity of design is crucial and very constrained environments where AES may not be suitable. Both of algorithms offer excellent performance on hardware and software platforms. They both Feistel networks with similar except the differences in their Feistel functions. Both of these twins are based Addition, Rotation and XOR processes but SIMON employs logical AND operations instead addition. This twin highly performs well in both hardware and software, although SIMON is better at hardware-oriented processes and SPECK more software-oriented.

Christof et al. proposed the SKINNY [23] that is a new tweakable block cipher family SKINNY. Tweakable means accepting a second input, named as tweak, that used in conjunction with the key to select the permutation computed by the cipher. One of the main aims of SKINNY is challenging with SIMON/SPECK designed by NSA in such areas directly relates to hardware/software performances. It has also aimed to provide a robust attack repelling mechanism with regards to differential/linear attacks. The main idea behind of the design is to provide minimum area in the hardware design without sacrificing speed and security. In the proposed method, thresholds are implemented for active S-Boxes in any differential trail for key settings different from NSA's SIMON according to [28]. It provides strong frontiers different from SIMON. SKINNY has resilient sizes for blocks, keys, and tweaks. It can also take advantage of very efficient applications against side-channel attacks. Furthermore, it has the smallest amount of operations for AND, OR, and XOR gates during the encryption and decryption process.

Table 1.Lightweight Approaches for Vehicular Network

Lightweight Approaches	**Security Requirement Support**	**Attack Mitigation**
ARAN	Authentication Integrity Non-Repudiation	Spoofing Attacks Impersonation Attacks Replay Attacks [10]
SEAD	Authentication Availability Privacy Preservation	DoS Attacks Impersonation Attacks [12]
Ariadne	Availability Privacy Preservation	Impersonation Attacks DoS Attacks Sybil Attacks [13]
RobSAD	Confidentiality Integrity Authentcation	Sybil Attacks [14]
SAODV/A *SAODV*	Authentication Availability Privacy Preservation	Impersonation Attacks Bogus Information Routing Attacks [16]
Holistic	Confidentiality Authentication	Impersonation Attacks [15]
PRESENT	N/A	Key-Schedule Attacks Linear Attacks Differential Attacks [19]
PRINCE	N/A	Linear Attacks Differential Attacks [20]

SPECS	Integrity, Authentcation Identity Privacy Preserving, Traceability, Revocability	Vehicle Attacks, RSU Attacks, Impersonation Attacks [17,28]
SPARX	Non-Linearity Diffusion	Single Trail Differential/Linear Attacks [21]
SIMON/SPECK	N/A	Side-Channel Attacks[22] Differential Attacks/Linear Attacks[24,25.26]
SKINNY	N/A	Meet in the Middle Attacks Impossible Differential Attacks Slide Attacks Subspace Cryptanalysis Algebraic Attakcs [23]

4. Conclusions

Vehicle industry has undergone a tremendous transformation in their hardware topology. This transformation brings new communication channels into vehicle network. People take lots of advantages of this sophisticated innovation into their life such as accessibility, efficiency, and availability with the help of Safety Warnings, Dynamic Transportation Flow Services and Driving Boundaries functions of VANET. All these functions of VANET require crucial security because of system has vital advantages and critical intervention to human life. Conventional security approaches or algorithms may not directly apply into vehicular networks due to their dynamic network topology. Dynamic topology means requirements for constantly real-time responses, high throughput and low delay. Therefore, a new deprivation arises related to security that can ensure dynamic topology and hardware-based requirements. We mentioned about approaches to ensure both light and secure safety requirements of VANET topology. All of the proposed protocols vary in terms of their purposes. This separation arises from VANET's large structure and sophisticated communication requirements. We review related protocols to ensure communication in VANET and also proposed some of the lightweight cryptographic approaches to give a lead to develop new security protocols for VANET. All of the proposed algorithms have advantages, disadvantages and difference relative to the each other in terms of their security level, throughput, energy consumption and latency factors. In addition, all of the approaches summarized in Table 1. in terms of attack mitigations and security supports. Summary, further enhancement of security take a vital role in upcoming challenges for the future of the automotive technology.

References

[1] Kara, I. The Spy Next Door: A Digital Computer Analysis Approach for Backdoor Trojan Attack. Avrupa Bilim ve Teknoloji Dergisi, (24), 125-129.

[2] Akca, A., Kara, I., & Aydos, M. Privacy, Security and Legal Aspects of Autonomous Vehicles.

[3] Jadoon, A. K., Wang, L., Li, T., & Zia, M. A. (2018). Lightweight cryptographic techniques for automotive cybersecurity. Wireless Communications and Mobile Computing, 2018.

[4] Sumra, I. A., Ahmad, I., & Hasbullah, H. (2011, October). Behavior of attacker and some new possible attacks in vehicular ad hoc network (VANET). In 2011 3rd international congress on ultra modern telecommunications and control systems and workshops (ICUMT) (pp. 1-8). IEEE.

[5] Rawat, A., Sharma, S., & Sushil, R. (2012). VANET: Security attacks and its possible solutions. Journal of Information and Operations Management, 3(1), 301.

[6] Zhang, Y., Liu, W., & Fang, Y. (2005, October). Secure localization in wireless sensor networks. In MILCOM 2005-2005 IEEE Military Communications Conference (pp. 3169-3175). IEEE.

[7] Karahasanovic, A. (2016). Automotive Cyber Security-Threat modeling of the AUTOSAR standard. Chalmers University of Technology.

[8] Singh, M., & Kim, S. (2017). Blockchain based intelligent vehicle data sharing framework. arXiv preprint arXiv:1708.09721.

[9] Kamble, N., Gala, R., Vijayaraghavan, R., Shukla, E., & Patel, D. (2021). Using Blockchain in Autonomous Vehicles. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 285-305). Springer, Cham.

[10] Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002, November). A secure routing protocol for ad hoc networks. In 10th IEEE International Conference on Network Protocols, 2002. Proceedings. (pp. 78-87). IEEE.

[11] Zhu, S., Xu, S., Setia, S., & Jajodia, S. (2006). LHAP: a lightweight network access control protocol for ad hoc networks. Ad Hoc Networks, 4(5), 567-585.

[12] Hu, Y. C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad hoc networks, 1(1), 175-192.

[13] Hu, Y. C., Perrig, A., & Johnson, D. B. (2005). Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless networks, 11(1), 21-38.

[14] Chen, C., Wang, X., Han, W., & Zang, B. (2009, June). A robust detection of the sybil attack in urban vanets. In 2009 29th IEEE International Conference on Distributed Computing Systems Workshops (pp. 270-276). IEEE.

[15] Zapata, M. G., & Asokan, N. (2002, September). Securing ad hoc routing protocols. In Proceedings of the 1st ACM workshop on Wireless security (pp. 1-10).

[16] Perkins, C. E., & Royer, E. M. (1999, February). Ad-hoc on-demand distance vector routing. In Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90-100). IEEE.

[17]Cerri, D., & Ghioni, A. (2008). Securing AODV: the A-SAODV secure routing prototype. IEEE Communications Magazine, 46(2), 120-125.

[18]Chim, T. W., Yiu, S. M., Hui, L. C., & Li, V. O. (2011). SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks, 9(2), 189-203.

[19]Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... & Vikkelsoe, C. (2007, September). PRESENT: An ultra-lightweight block cipher. In International workshop on cryptographic hardware and embedded systems (pp. 450-466). Springer, Berlin, Heidelberg.

[20]Mohammed, R. S., Jabbar, K. K., & Hilal, H. A. (2021). Image encryption under spatial domain based on modify 2D LSCM chaotic map via dynamic substitution-permutation network. International Journal of Electrical & Computer Engineering (2088-8708), 11(4).

[21]Dinu, D., Perrin, L., Udovenko, A., Velichkov, V., Großschädl, J., & Biryukov, A. (2016, December). Design strategies for ARX with provable bounds: Sparx and LAX. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 484-513). Springer, Berlin, Heidelberg.

[22]Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). The Simon and Speck families of lightweight block ciphers cryptology eprint archive.

[23]Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., ... & Sim, S. M. (2016, August). The SKINNY family of block ciphers and its low-latency variant MANTIS. In Annual International Cryptology Conference (pp. 123-153). Springer, Berlin, Heidelberg.

[24]Tupsamudre, H., Bisht, S., & Mukhopadhyay, D. (2014, September). Differential fault analysis on the families of SIMON and SPECK ciphers. In 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography (pp. 40-48). IEEE.

[25]Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2017). Notes on the design and analysis of SIMON and SPECK. IACR Cryptol. ePrint Arch., 2017, 560.

[26]AlKhzaimi, H., & Lauridsen, M. M. (2013). Cryptanalysis of the SIMON Family of Block Ciphers. IACR Cryptol. ePrint Arch., 2013, 543.

[27]Horng, S. J., Tzeng, S. F., Pan, Y., Fan, P., Wang, X., Li, T., & Khan, M. K. (2013). b-SPECS+: Batch verification for secure pseudonymous authentication in VANET. IEEE transactions on information forensics and security, 8(11), 1860-1875.

[28] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. Journal of cryptographic Engineering, 8(2), 141-184.

[29] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (2018). A review of lightweight block ciphers. Journal of cryptographic Engineering, 8(2), 141-184.

[30] Yang, K. Security and Privacy in Vehicular Ad Hoc Networks (VANETs). Broadband Communications Research (BBCR) Lab, (September 12, 2021). https://ece.uwaterloo.ca/~kan.yang/security_bbcr/vanet.html .

[31] Kara, İ.(2021) Web sitesi tabanlı oltalama saldırılarının adli analizi. Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi, 1-1.

[32] Kara, I., Aydos, M., & Bozkır, A. S. (2020). Characteristic Behavioral Analysis of Malware: A Case study of Cryptowall Ransomware. Avrupa Bilim ve Teknoloji Dergisi, 486-493.