Bima Journal of Science and Technology, Vol. 6 (3) Dec, 2022 ISSN: 2536-6041

DOI: 10.56892/bima.v6i03.61

A REVIEW ON AUTHENTICATION AND PRIVACY PROTECTION SCHEMES IN VEHICULAR AD HOC NETWORKS (VANETS)

[1]*IDRIS LAWAL BAGIWA, [2]ABUBAKAR AMINU MU'AZU and [3]MUSA AHMED ZAYYAD

[1]Department of Computer and Information Technology, Alqalam University, Katsina P.M.B. 2137, Katsina State, Nigeria

[2]Department of Computer Science, Umar Musa Yar'adua University P.M.B, 2218, Katsina State, Nigeria.

[3]Department of Computer Studies, Hassan Usman Katsina Polytechnic P.M.B. 2052, Katsina State, Nigeria.

Corresponding Author: lawal.idris.bagiwa@hukpoly.edu.ng

ABSTRACT

Vehicular ad hoc networks (VANETs) is a sort of mobile ad hoc network (MANET) that is designed based on moving vehicles, which are referred to as nodes. The nodes communicate with one another wirelessly, without the need for a network infrastructure that physically connects them. Once the network design has changed, nodes are free to migrate in whatever direction they want as long as the nodes are available to move in that direction. As a result, each node acts as a router, sending traffic to the nodes to which it has been directed. VANET' popularity however brings with it a variety of issues, including security, routing, and data dissemination. Many solutions have already been presented by different researchers to address these issues, but due to the constant emergence of new threats and attacks, privacy of users must be prioritized above all in VANET. Consequently, a review of authentication, privacy and security solutions presented in different researches have been discussed in this paper, as well as the security services they have studied which were centered towards Authentication, Confidentiality, Availability, and Integrity. In this paper, 10 most relevant schemes were analysed and the result shows that privacy challenges and high computation overhead which causes transmission delays and adds a difficult verification process to VANET communications was the major challenge affecting the VANETs.

Keywords: Ad hoc, MANET, Privacy, Protection and Vehicular.

INTRODUCTION

Considering how things are moving so fast nowadays, transportation systems are becoming more advanced and intelligent than ever before. The Vehicular Ad Hoc Network (VANET) is one of the most promising Intelligent Transportation System candidates (ITS). VANET are a new type of mobile ad hoc network in which vehicles serve as mobile nodes. It is gaining popularity as a result of several distinctive features it possesses(Afzal and Kumar, 2020). VANET enable communication between moving vehicles in order to disseminate information about traffic, road conditions, weather conditions, accident information, and other related information in order to offer support to the vehicle or the driver of the vehicle. It can assist vehicles in reducing the likelihood of accidents and other disturbances. There are other domains in VANET that require additional investigation, including routing protocols, security, architecture, difficulties, and standardization (Ahmad, 2021).

Bima Journal of Science and Technology, Vol. 6 (3) Dec, 2022 ISSN: 2536-6041

DOI: 10.56892/bima.v6i03.61

TECHNOLOGIES IN VANET

Vehicular Ad hoc Networks encompass a number of technologies, particularly as facilitators of Intelligent Transportation Systems (ITS). GSM Network, UMTS, Wi-MAX/Wi-Fi, and a unique and specific technology designed for VANET, Wireless Access in Vehicular Environments (WAVE), also known as IEEE 802.11p (Klapež et al., 2021), are basic examples. This implies that a vehicle should have many radio interfaces (and/or a network card) on board. WAVE is a member of the IEEE 802.11 family, which implies that this solution is adopted from IEEE 802.11 and tailored for the VANET environment (Sepulcre et al., 2021).

Communication in Vanet

The two major communication modes in VANET are vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication (V2I). V2V communication refers to the ability to exchange transmissions between different cars, whereas V2I communication refers to communication between vehicles and the road-side framework. As indicated in Figure 1, the main communication module comprises of a Road-Side Unit (RSU), an on-board unit (OBU), and a trusted authority (TA). The RSU unit is fixed and consists of a transceiver that sends and receives information from the OBU and TA (Balu et al., 2019).

In previous designs, a vehicle and a roadside unit (RSU) would use the well-known Diffie-Hellman (DH) protocol to generate a secret key for one another and then exchange it. This procedure adds additional computational burden to each node in the system, which impacts the amount of time necessary to complete the registration phase. In this thesis, the confidential key is effectively distributed without the utilization of the Diffie-Hellman protocol. This strategy shortens the amount of time necessary to finish the registration phase by cutting down on the amount of extra processing that is required at each node.

Vehicle-to-Vehicle (V2V) Communication

Vehicle-to-Vehicle (V2V) communication allows cars to electronically broadcast speed, location, and direction. By sending and receiving Omni-directional messages as indicated in Figure 6 (up to 10 times per second), V2V technology give vehicles a 360-degree "knowledge" of their surroundings. With the right software (or safety applications), vehicles can leverage communications from other vehicles to identify potential crash hazards(Al-Heety et al., 2020). The technology can deliver visual, tactile, and audible alerts, or a combination of them. These signals enable drivers to avoid crashes. These V2V communication messages can detect threats hidden by traffic, topography, or weather. V2V communication enhances existing collision avoidance systems that use radars and cameras to detect danger. Figure 1 shows a typical V2V communication.

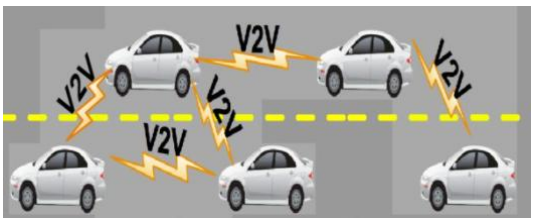

Figure 1: Vehicle-to-Vehicle (V2V) Communication(Ullah, 2016)

Vehicle-to-Infrastructure (V2I) Communication

Vehicle-to-infrastructure (V2I or v2i) communication is a communication model that allows vehicles to exchange data with the components that support a country's transportation system; Figure 3 shows how the communication process works. Overhead RFID readers and cameras, traffic signals, lane markers, lighting, signage, and parking meters are examples of such components.

Bima Journal of Science and Technology, Vol. 6 (3) Dec, 2022 ISSN: 2536-6041

DOI: 10.56892/bima.v6i03.61

V2I communication is often bi-directional and wireless: data from infrastructure components can be sent to the vehicle through an ad hoc network, and vice versa. V2I, like vehicle-to-vehicle (V2V) communication, transfers data via dedicated short range communication (DSRC) frequencies. V2I sensors in an intelligent transportation system (ITS) can collect infrastructure data and give travellers with real-time alerts regarding road conditions, traffic congestion, accidents, construction zones, and parking availability. Similarly, traffic management monitoring systems can use infrastructure and vehicle data to set variable speed limits and change traffic signal phase and timing (SPaT) to improve fuel economy and traffic flow.

The hardware, software, and firmware that allow vehicles to communicate with roadside infrastructure is a critical component of all driverless car initiatives(Hasan et al., 2020). Figure 2 presents a typical V2V communication.

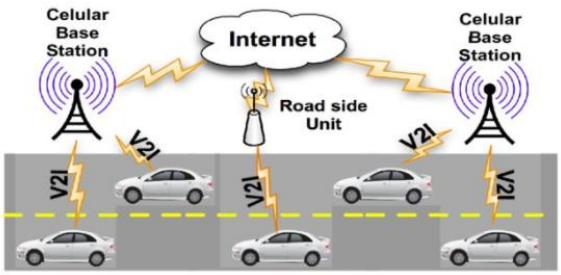

Figure 2: Vehicle-to-Infrastructure (V2I) Communication(Ullah, 2016)

Vehicle-to-Everything (V2X) Communication

Vehicle to Everything (V2X) is a vehicle-to-vehicle communication technology. Vehicle-to-everything (V2X) technology aims to improve traffic flow on the road. The NHTSA claims that V2X technology will cut road accidents nationally. To communicate with other vehicles and infrastructure such as parking spots, traffic lights, and cell phones, V2X systems use high-bandwidth and high-reliability networks to send data such as speed. The technology improves driver awareness, lowering injuries, fatalities, and car-to-car collisions. The technology suggests different routes and discovers empty parking places. V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) lets vehicles to interact with other vehicles, traffic lights, parking areas, bikers, and pedestrians.

These devices benefit drivers and other road users including bicycles and pedestrians. Conventional vehicles' V2X systems can provide vital information on weather, local accidents, road conditions, roadwork alerts and other drivers' activity. The V2X technology may augment existing navigation systems. This allows vehicles to examine their surroundings and make speedy decisions(Hasan et al., 2020). Figure 3 depicts basic V2X communication system.

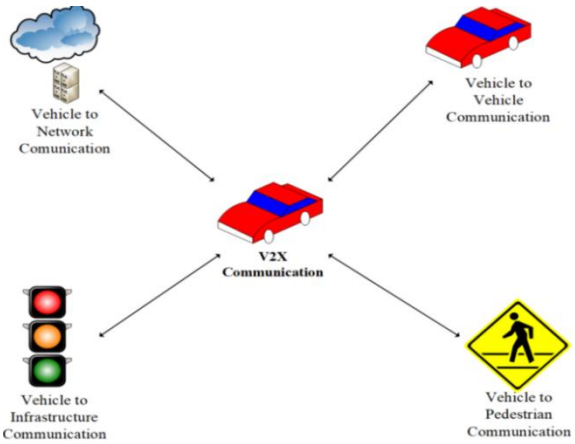

Figure 3: Vehicle-to-Everything (V2X) Communication(Hasan et al., 2020)

IEEE 802.11p Technology

IEEE 802.11p is an accepted modification to the IEEE 802.11 standard that adds wireless access in vehicle environments (WAVE), a vehicular communication system. It specifies the modifications to 802.11 (the foundation of Wi-Fi products) that are required to support

Bima Journal of Science and Technology, Vol. 6 (3) Dec, 2022 ISSN: 2536-6041

DOI: 10.56892/bima.v6i03.61

Intelligent Transportation Systems (ITS) applications.

This comprises data interchange between high-speed vehicles and between vehicles and roadside infrastructure; known as V2X communication, in the 5.9 GHz (5.85–5.925 GHz) licensed ITS frequency. IEEE 1609 is a higher layer standard that is built on the IEEE 802.11p standard. It is also the foundation of the ETSI ITS-G5 European standard for vehicular communication (Arena et al., 2020). Figure 4 depicts the system level structure of an IEEE 802.11p network with V2V and V2I communications.

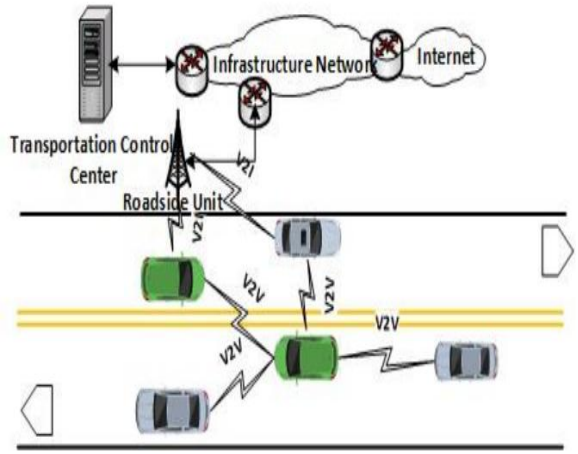

Figure 4: 802.11p Technology in VANET (Roy et al., 2018)

GSM Network

GSM (Global System for Mobile Communication) Network is an ETSI (European Telecommunication Standard Institute) standard that refers to the digital cellular network protocol in 2G. It was initially based on a circuit switched network, but it was later developed for complete optimal telephony transformation utilizing a packet switched network(Ashraf et al., 2016). As shown in Fig. 5, vehicular network architecture that uses GSM Network consists primarily of three components: smart vehicles, Road Side Units (RSUs), and vehicular communication.

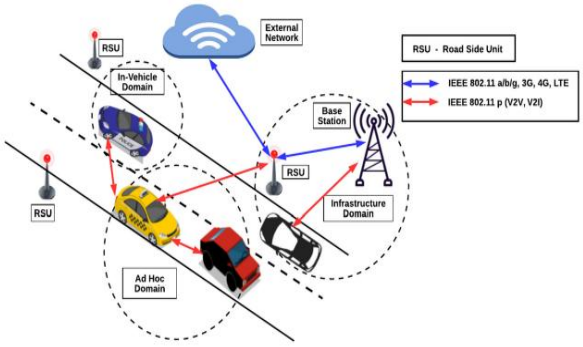

Figure 5: GSM Network based VANET(Sultana et al., 2021)

Universal Mobile Telecommunications Technology (UMTS)

The Universal Mobile Telecommunications System (UMTS) is a third-generation GSM mobile cellular system. UMTS is a component of the International Telecommunication Union's IMT-2000 standard set, developed and managed by the 3GPP (3rd Generation Partnership Project), and is similar to the CDMA2000 standard set for networks based on competitive CDMA One technology.

To provide mobile network operators with greater spectrum efficiency and bandwidth, UMTS leverages wideband code-division multiple access (W-CDMA) radio access technology. UMTS refers to a complete network system that includes the radio access network (UMTS Terrestrial Radio Access Network, or UTRAN) as shown in figure 3, the core network (Mobile Application Part, or MAP), and user authentication via SIM (subscriber identification module) cards. UMTS technology is also known as Freedom of Mobile Multimedia Access (FOMA) or 3GSM (Auvinen et al., 2019).

Bima Journal of Science and Technology, Vol. 6 (3) Dec, 2022 ISSN: 2536-6041

DOI: 10.56892/bima.v6i03.61

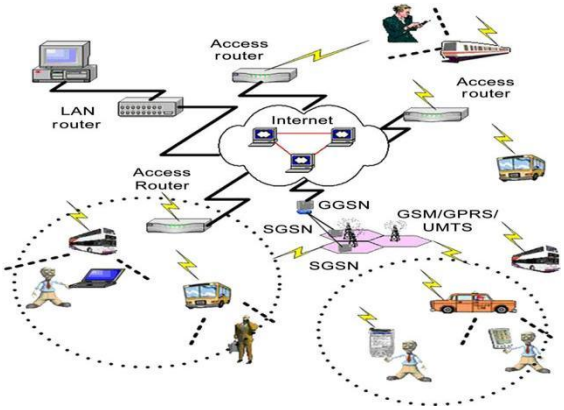

Figure 6: (UMTS) Universal Mobile Telecommunications Technology for VANET(Hamza et al., 2010)

Wi-MAX/Wi-Fi

Wi-Fi and WiMax are two technologies that are used to establish wireless network connections. When creating small networks, Wi-Fi is utilized to connect printers, computers, and gaming consoles to a centralized network. WiMax is a wireless technology that employs airwaves to give connection to a network. Internet services such as Mobile Data and hotspots are made possible through the deployment of WiMax technology (Sura and Reddy, 2020). A multi-vehicle-to-infrastructure (V2V2I) VANET that uses Wi-Fi for vehicle-to-vehicle communication and WiMAX for vehicle-to-infrastructure (V2I) connectivity is shown in Figure 7.

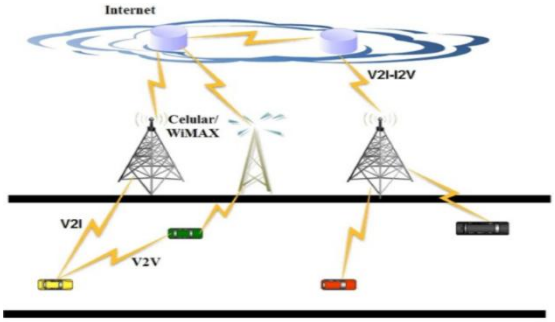

Figure 7: Wi-MAX/Wi-Fi for VANET Communication(Mojela and Booysen, 2013)

VANET ARCHITECTURE

Devices in VANET architecture can move in any direction independently, changing their links to other devices frequently (Al-Heety et al., 2020). As illustrated in Figure 5 below, the architecture of VANET is primarily composed of three types of domains(Panjrath and Poriye, 2017). According on the source and destination of information being communicated, these domains are subdivided into three categories; these three domains are as follows: the mobile domain, the infrastructure domain, and the generic domain

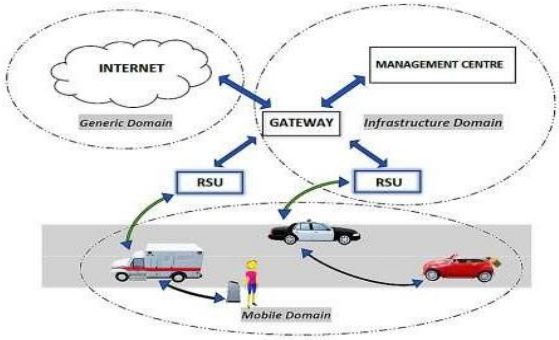

Figure 8: VANET Architecture (Balu et al., 2019)

Mobile Domain

The mobile domain is divided into two components: the vehicle domain and the mobile device domain. The vehicle domain includes all types of vehicles, such as automobiles and buses. The mobile device domain includes all types of portable devices, such as personal navigation devices and smartphones.(Balu et al., 2019).

Infrastructure Domain

There are two domains within the infrastructure domain: the roadside infrastructure domain and the central infrastructure domain. The roadside infrastructure domain is responsible for the infrastructure on the roadside. The roadside

DOI: 10.56892/bima.v6i03.61

infrastructure domain contains roadside unit entities such as traffic lights, which are located along the roadside. In the central infrastructure domain, there are infrastructure management centers, such as traffic management centers (TMCs) and vehicle management centers (VMCs) (Balu et al., 2019).

Generic Domain

Domains that are generic in nature are those that deal with cloud and internet services. In order to disseminates and maintain up-to-date information. Generally speaking, a generic domain is made up of two components: a private network and the Internet. A private network can be used to broadcast local information such as traffic flow and accident information, for example. The internet can be used to store data on the cloud for the purposes of data analytics(Balu et al., 2019). The evolution of VANET architecture, on the other hand, differs from one region to another. The reference design for the Vehicle to Vehicle (V2V) communication system, which is being pursued by the V2V communication consortium, differs from that of the V2V communication system. Its "manifesto" was released in 2007. The V2V communication consortium (V2V-CC) is the key driving force behind vehicular communication in Europe, and it is the most recent member of the V2V communication consortium. The in-vehicle domain, the ad hoc domain, and the infrastructure domain are all included in the system design.

VANET SECURITY CHALLENGES

The issue of security is critical in VANETs since it assures the safety of both drivers and passengers. This is required in order to create critical systems that ensure safety and security. According to Rahim et al. (2021), A considerable amount of previous research indicates that VANET faces several problems; and for these reasons, it is necessary to point out and emphasize these challenges due to the increasing number of connected devices in the system. According to Hezam et al. (2018)

- Availability
- Authentication
- Integrity
- Confidentiality
- Nonrepudiation
- Pseudonymity
- Privacy
- Mobility
- Data and location verification
- Access control
- Key management difficulties

These are among the security challenges faced by VANETs. The technologies of VANET have been extensively explored because of their several uses, such as enhancing traffic efficiency, assisting with passenger safety, and enhancing information. The deployment and management of VANET are becoming difficult due to the increase in vehicle technology and rapid expansion in the number of smart vehicles(Shrestha et al., 2018).

REVIEW OF AUTHENTICATION SCHEMES

Source authentication and message integrity of traffic-related data are critical security requirement in VANET. By easily safeguarding moving cars, RSUs, Application Servers, and roadside sensors, compliance with these security criteria ensures the confidence and proper performance of all flexible technologies that come with a VANET system(Vallent et al., 2021). A lot of progress has been made towards VANET, but security challenges still require more research attention (Afzal and Kumar, 2020).

(Perrig et al., 2005) Have suggested an authentication system that requires less transmission, processing time, scalability issues and is resistant to packet loss. During

DOI: 10.56892/bima.v6i03.61

loose time synchronization between the sender and receivers, they used the one-way function and the message authentication code (MAC) keys produced from it. Asymmetric cryptography is made more secure with Timed Efficient Stream Loss-tolerant Authentication (TESLA). However, the scheme uses anonymous authentication and require one-to-one communication between vehicles and the trusted authority (TA) which leads to privacy breach, routing challenge and computational overhead (delay in response time).

Due to the critical nature of authentication for safe operation in VANET, several researches were conducted previously such as those conducted by (Horng et al., 2013; Li et al., 2014; Studer et al., 2009) in order to address the challenges presented above.

On the recent efforts, Lin and Hsu (2018) Using a group key and MAC code, presented a conditional privacy approach. In this approach, each vehicle employs a group key for mutual authentication, and the produced group key is used to verify messages. The method uses an algorithm in conjunction with a key.

The algorithm is only as strong as the key's complexity and the output's size. It uses either 128 or 160 bits. However, Offline password guessing, stolen-verifier, and reflection attacks are all possible. Hubaux in (Al-ani et al., 2018) to cover users' true identity, the authors employ anonymous certificates (also known as pseudonyms). Despite the fact that anonymous certificates have no publicly known relationship to the genuine identities of the key holders, privacy can still be violated by logging messages containing a specific key and monitoring the sender until identity is determined. To prevent this attack, the way anonymous certificates are used should be changed so that the owner of the keys cannot be traced (Babaghayou et al., 2020).

Technique based on anonymous certificates by Wang et al. (2020) proposes storing a number of anonymous certificates (together with the appropriate private/public key pairs) in a vehicle so that it can employ different key pairs and avoid tracing. However, based on the frequency of key changes, which varies depending on the vehicle's current speed, vehicles will need to store a huge number of pairs. As a result, safe key distribution, key management, and storage become extremely difficult; as such, this type of scheme should be avoided for the sake of practical reason.

To provide an alternative solution to the problem of pre-storing large number of anonymous certificates while maintaining conditional privacy, Erskine (2020), believe that automobiles and RSUs can actively collaborate. When a vehicle passes by a RSU, it sends a request for a short-term anonymous certificate, and the RSU responds with an anonymous certificate following a two-round procedure.

Because a vehicle's anonymous certificate must be changed regularly to avoid message linkability, it must interface with RSUs constantly. The VANET's efficiency may be affected as a result of such frequent interactions. This temporary anonymous certificate must be sent and passed to verifiers in order for messages from the anonymous originator to be validated.

The systems presented in (Fotohi et al., 2020; Hussain et al., 2020) which similarly rely on RSUs, are also worth highlighting. The method of mixzones is utilized to improve vehicle anonymity. However, this system still relies on each vehicle pre-loading a huge number of anonymous certificates. In (Bouchelaghem and Omar, 2020), a technique for securing vehicle communications is

DOI: 10.56892/bima.v6i03.61

suggested that uses a keyed hash message authentication code (HMAC) with low communication overhead.

This approach necessitates a vehicle employing a key agreement protocol to receive a symmetric key from a RSU. To safeguard its privacy, the vehicle should communicate with the RSUs using different public keys. As a result, the vehicle must still pre-load a set of anonymous certificates. However, the systems totally rely on RSUs in terms of robustness. These methods will no longer work if an RSU fails.

Another effort towards solution to Authentication challenges in VANET by (Khan et al., 2021) suggested the Trust-text End Authentication Mechanism (TEAM), an authentication technique that permits participants to be co-located, in which cars are dispersed into smaller groups and a group leader is assigned to each group. Every participant authenticates with the chief, who authenticates with the trusted authority (TA) through the Road Side Unit (RSU).

At junction, group leaders may shift. After taking turns, a new group is established. Any approved public transportation vehicle could serve as the leader. Communication will swap between groups when a single vehicle goes down or leaves the party, similar to how a cell phone will switch between base stations. On the other hand, if a malicious vehicle is a member of a certain group, the privacy of each group member may be breached for a limited amount of time.

According to Thorncharoensri et al. (2020), certificateless signature authentication is the best technique for meeting privacy requirements since it has a less message overhead and a greater success rate than earlier solutions for message verification and authentication.

Al-Riyami and Paterson (2003), Were the first to propose certificateless public key cryptography. Certificateless public key cryptography, in contrast to standard public key cryptography, the technique does not require the use of a certificate to confirm the legitimacy of the public keys. Au et al. in (Elhabob et al., 2019; Tan et al., 2018; Thorncharoensri et al., 2020; Yulei et al., 2018) have all studied the formal security definitions of certificateless signature (CLS) systems extensively.

The lightweight certificateless signature proposed by Karati et al. (2018) can be used on limited devices. However, subsequent research conducted by (Zhang et al., 2018) shows that it is insecure technique in the case of a public key replacement attack.

According to Elhabob et al. (2020) Certificateless cryptography technique was introduced to alleviate the inherent key escrow problem of ID-based cryptography. In a certificateless signature technique, a user's private key is computed by two parties rather than simply the key generation center (KGC). To begin, the user receives a KGC-generated partial private key.

The user then chooses a secret value on their own and generates their private key for signature creation using the secret value and the partial private key. Due to this, in certificateless cryptography, the KGC does not have access to all of the users' private keys, removing the key escrow problem that exists in ID-based encryption. In certificateless based cryptography, no certificate is required to authenticate a user's public key, similar to ID-based encryption. Therefore, the complex certificate administration problem is avoided.

Cui et al. (2018) showed the usage of certificateless aggregate signature in a VANET application. They also presented a

DOI: 10.56892/bima.v6i03.61

VANET-specific certificateless aggregate signature approach that does not require bilinear pairing. Recently, due to the popularity of the IoT topics, the compact and lightweight certificateless aggregate signature schemes were proposed in (Deng et al., 2019).

It is efficient in the signing and verifying process where requires only two pairing operations in the verification, and the size of the signature is only one point on the elliptic curve and some state of information. However, the state of information must be shared among signers (devices) before each signer can sign on a message. Another problem arises as a result of the securely constructed shared state of information.

Liu et al. (2020) introduced a compact and unrestricted certificateless aggregate signature which the signature's size is constant. Their scheme shares the similarity to Deng *et al.*'s scheme; however, the former scheme is much flexible. It does not need to share a state of information for every time the signer generates a signature.

The most efficient certificateless aggregate signature approach was recently suggested by (Mei et al., 2020). The technique eliminates the need for bilinear pairing and allows for offline computation of scalar multiplication over device and storage of results for later use. As a result, it is well-suited to IoT devices with low computing power. However, the technique prove to require high computation overhead and transmission costs by (Xu et al., 2020).

Aggregated signature for CL-PKC is presented by Asari et al. (2021) to further reduce computation overhead and transmission costs, which is critical in resource-constrained scenarios. Signature aggregation means that if you have a certain signatures on a certain different messages from certain different node/device, they can be combined together into a single short signature (Tiwari and Gangadharan, 2021).

The majority of aggregated signature schemes necessitate sophisticated bilinear pairing processes, which are costly and unsuitable for lightweight devices like the OBU. (Asari et al., 2021) Proposed a certificateless aggregate signature system that only requires a minimal constant number of pairing operations to lessen the burden of bilinear pairing computations. It is, however, proven by Tiwari and Gangadharan (2021) that the privacy breach, computation overhead and transmission cost is still on the high side. Table 1.summarizes review of 10 articles for message Authentication Schemes conducted by different authors in the area of VANET.

CONCLUSION

VANET are becoming increasingly popular in traffic management systems, with the goal of ensuring the safety of human lives on the road and providing comfort to users by broadcasting safety warnings among vehicles. Because these safety messages are broadcast in an open-access environment, which makes VANET more vulnerable to attacks, a robust security algorithm must be created to combat security threats and attacks and maintain secure communication in VANET. In this review, the paper first provides a fundamental overview of VANET and their technologies, as well as VANET security challenges. The potential applications that are affected by risks and attacks are then thoroughly outlined; several authentication and privacy schemes with their strengths and weaknesses, security needs, threats, and performance aspects have been reviewed.

DOI: 10.56892/bima.v6i03.61

Table 1: Summary of Review on Message Authentication Schemes

S/No	Reference	Research Title	Targeted Security Service(s)	Proposed Technique/ Model	Methodology/ Approach Applied	Limitation
1	(Perrig et al., 2005)	Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction	Confidentiality and Authentication	Timed efficient stream loss-tolerant authentication (TESLA)	Asymmetric cryptography	Privacy breach, routing challenge and computational overhead (delay in response time).
2	(Lin and Hsu, 2018)	A Practical Certificateless Conditional Privacy Preserving Authentication Scheme for Vehicular Ad Hoc Networks	Authentication, Privacy and Integrity	practical certificateless conditional privacy preserving authentication (PCPA)	Chaotic Hash Function (CHF)	Offline password guessing, stolen-verifier, and reflection attacks are all possible.
3	(Wang et al., 2020)	Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANET	Authentication, Confidentiality and Availability	Identity-Based Anonymous Authentication Scheme	Signature Verification Algorithm Scheme	Vehicles will need to store a huge number of pairs of keys. As a result, safe key distribution, key management, and storage become extremely difficult
4	(Erskine, 2020)	Secure Intelligent Vehicular Network Including Real-Time Detection of DoS Attacks in IEEE 802.11p Using Fog Computing University of Bridgeport	Confidentiality and Availability	Anonymous Certificate Authentication Scheme	Software-defined networking (SDN) based on Fog Computing	Systems totally rely on RSUs in terms of robustness, therefore, the method will no longer work if an RSU fails.
5	(Fotohi et al., 2020)	Using a group key and MAC code, presented a conditional privacy approach. In this approach, each vehicle employs a group key for mutual authentication, and the produced group key is used to verify messages. The method uses an algorithm in conjunction with a key. The algorithm is only as strong as the	Confidentiality, Integrity, Availability	Keyed hash message authentication code (HMAC)	Mixzones Approach	Systems totally rely on RSUs in terms of robustness, therefore, the method will no longer work if an RSU fails.

DOI: 10.56892/bima.v6i03.61

S/No	Reference	Research Title	Targeted Security Service(s)	Proposed Technique/ Model	Methodology/ Approach Applied	Limitation
		key's complexity and the output's size. It uses either 128 or 160 bits				
6	(Xiong et al., 2020)	Energy-Saving Data Aggregation for Multi-UAV System.	Integrity, Confidentiality	PKI-based Authentication Approach	message aggregation Technique	unable to provide a generic mechanism for validating semantically aggregated data
7	(Khan et al., 2021)	Security Challenges of Location Privacy in VANET and State-of-The Art Solutions: A Survey	Availability	Trust-text End Authentication Mechanism (TEAM)	Location privacy schemes	Data management inefficient and privacy breach has been identified in the technique
8	(Mei et al., 2020)	Efficient certificateless aggregate signature with conditional privacy preservation in IoV	Confidentiality and Integrity	Certificateless aggregate signature approach	Aggregation Technique	The technique prove to require high computation overhead and transmission costs
9	(Thumbur et al., 2020)	Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks	Authentication	certificateless aggregate signature-based authentication scheme	aggregation and batch verification techniques	It incurs higher computational overhead in the signature generation and verification processes
10	(Asari et al., 2021)	A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems	Confidentiality	Certificateless aggregate signature Technique	Full Aggregation Technique	The privacy breach, computation overhead and transmission cost is still on the high side

Many solutions have already been presented by different researchers to address these issues, but due to the constant emergence of new threats and attacks, privacy of users must be prioritized above all in VANET. Consequently, a review of authentication, privacy and security solutions presented in different researches have been discussed in this paper, as well as the security services they have studied which were centered towards Authentication, Confidentiality, Availability, and Integrity. In this paper, 10 most relevant schemes were analysed and the result shows that privacy challenges and high computation overhead which causes transmission delays and adds a difficult

DOI: 10.56892/bima.v6i03.61

verification process to VANET communications was the major challenge affecting the VANETs.

REFERENCES

Afzal, Z., and Kumar, M. (2020). Security of vehicular Ad-hoc networks (VANET): A survey. Journal of Physics: Conference Series.

Ahmad, F. (2021). *A Trust Evaluation Framework in Vehicular Ad-Hoc Networks*. University of Derby (United Kingdom).

Al-ani, R., Zhou, B., Shi, Q., and Sagheer, A. (2018). A survey on secure safety applications in vanet. 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS).

Al-Heety, O. S., Zakaria, Z., Ismail, M., Shakir, M. M., Alani, S., and Alsariera, H. (2020). A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for sdn-vanet. *IEEE Access*, *8*, 91028-91047.

Al-Riyami, S. S., and Paterson, K. G. (2003). Certificateless public key cryptography. International conference on the theory and application of cryptology and information security.

Arena, F., Pau, G., and Severino, A. (2020). A review on IEEE 802.11 p for intelligent transportation systems. *Journal of Sensor and Actuator Networks*, *9*(2), 22.

Asari, A., Alagheband, M. R., Bayat, M., and Asaar, M. R. (2021). A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems. *Computer Networks*, *185*, 107599.

Ashraf, M., Bilal, H., Khan, I. A., and Ahmad, F. (2016). Vanet challenges of availability and scalability. *VFAST Transactions on Software Engineering*, *4*(1), 46-53.

Auvinen, A., Feychting, M., Ahlbom, A., Hillert, L., Elliott, P., Schüz, J., . . . Poulsen, A. H. (2019). Headache, tinnitus and hearing loss in the international Cohort Study of Mobile Phone Use and Health (COSMOS) in Sweden and Finland. *International journal of epidemiology*, *48*(5), 1567-1579.

Babaghayou, M., Labraoui, N., Ari, A. A. A., Lagraa, N., and Ferrag, M. A. (2020). Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications*, *55*, 102618.

Balu, M., Kumar, G., and Lim, S.-J. (2019). A review on security techniques in vanets. *International Journal of Control and Automation*, *12*(4), 1-14.

Bouchelaghem, S., and Omar, M. (2020). Secure and efficient pseudonymization for privacy-preserving vehicular communications in smart cities. *Computers and Electrical Engineering*, *82*, 106557.

Cui, J., Zhang, J., Zhong, H., Shi, R., and Xu, Y. (2018). An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks. *Information Sciences*, *451*, 1-15.

Deng, L., Yang, Y., and Chen, Y. (2019). Certificateless short aggregate signature scheme for mobile devices. *IEEE Access*, *7*, 87162-87168.

Elhabob, R., Zhao, Y., Sella, I., and Xiong, H. (2019). Efficient certificateless public key cryptography with equality test for internet of vehicles. *IEEE Access*, *7*, 68957-68969.

Elhabob, R., Zhao, Y., Sella, I., and Xiong, H. (2020). An efficient certificateless

DOI: 10.56892/bima.v6i03.61

public key cryptography with authorized equality test in IIoT. *Journal of Ambient Intelligence and Humanized Computing*, *11*(3), 1065-1083.

Erskine, S. K. (2020). *Secure Intelligent Vehicular Network Including Real-Time Detection of DoS Attacks in Ieee 802.11 p Using Fog Computing* University of Bridgeport].

Fotohi, R., Ebazadeh, Y., and Geshlag, M. S. (2020). A new approach for improvement security against DoS attacks in vehicular ad-hoc network. *arXiv preprint arXiv:2002.10333*.

Hamza, J. B., Ng, C. K., Noordin, N., Rasid, M., and Ismail, A. (2010). Review of minimizing a vertical handover in a heterogeneous wireless network. *IETE technical review*, *27*(2), 97-106.

Hasan, M., Mohan, S., Shimizu, T., and Lu, H. (2020). Securing Vehicle-to-Everything (V2X) communication platforms. *IEEE Transactions on Intelligent Vehicles*, *5*(4), 693-713.

Hezam, M. A., Junaid, A., Syed, A., Nazri, M., Warip, M., Fazira, K. N., . . . Nurul Hidayah, R. (2018). Classification of security attacks in VANET: A review of requirements and perspectives.

Horng, S.-J., Tzeng, S.-F., Pan, Y., Fan, P., Wang, X., Li, T., and 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.

Hussain, R., Lee, J., and Zeadally, S. (2020). Trust in VANET: A survey of current solutions and future research opportunities. *IEEE transactions on intelligent transportation systems*, *22*(5), 2553-2571.

Karati, A., Islam, S. H., and Karuppiah, M. (2018). Provably secure and lightweight certificateless signature scheme for IIoT environments. *IEEE Transactions on Industrial Informatics*, *14*(8), 3701-3711.

Khan, S., Sharma, I., Aslam, M., Khan, M. Z., and Khan, S. (2021). Security Challenges of Location Privacy in VANETs and State-of-The Art Solutions: A Survey. *Future Internet*, *13*(4), 96.

Klapež, M., Grazia, C. A., and Casoni, M. (2021). Experimental Evaluation of IEEE 802.11 p in High-Speed Trials for Safety-Related Applications. *IEEE Transactions on Vehicular Technology*, *70*(11), 11538-11553.

Li, J., Lu, H., and Guizani, M. (2014). ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. *IEEE Transactions on Parallel and Distributed Systems*, *26*(4), 938-948.

Lin, T.-W., and Hsu, C.-L. (2018). Anonymous group key agreement protocol for multi-server and mobile environments based on Chebyshev chaotic maps. *The Journal of Supercomputing*, *74*(9), 4521-4541.

Liu, J., Wang, L., and Yu, Y. (2020). Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks. *IEEE internet of things Journal*, *7*(6), 5256-5266.

Mei, Q., Xiong, H., Chen, J., Yang, M., Kumari, S., and Khan, M. K. (2020). Efficient certificateless aggregate signature with conditional privacy preservation in IoV. *IEEE Systems Journal*, *15*(1), 245-256.

Mojela, L. S., and Booysen, M. J. (2013). On the use of WiMAX and Wi-Fi to provide in-vehicle connectivity and media distribution. 2013 IEEE International Conference on Industrial Technology (ICIT).

DOI: 10.56892/bima.v6i03.61

Panjrath, N., and Poriye, M. (2017). A Comprehensive Survey of VANET Architectures and Design. *International Journal of Advanced Research in Computer Science*, *8*(5).

Perrig, A., Song, D., Canetti, R., Tygar, J., and Briscoe, B. (2005). Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction. *Request For Comments*, *4082*.

Rahim, M. A., Rahman, M. A., Rahman, M. M., Asyhari, A. T., Bhuiyan, M. Z. A., and Ramasamy, D. (2021). Evolution of IoT-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications*, *27*, 100285.

Roy, D., Chatterjee, M., and Pasiliao, E. (2018). Video quality assessment for inter-vehicular streaming with IEEE 802.11 p, LTE, and LTE Direct networks over fading channels. *Computer Communications*, *118*, 69-80.

Sepulcre, M., Gonzalez-Martin, M., Gozalvez, J., Molina-Masegosa, R., and Coll-Perales, B. (2021). Analytical models of the performance of IEEE 802.11 p vehicle to vehicle communications. *IEEE Transactions on Vehicular Technology*.

Shrestha, R., Bajracharya, R., and Nam, S. Y. (2018). Challenges of future VANET and cloud-based approaches. *Wireless Communications and Mobile Computing*, *2018*.

Studer, A., Bai, F., Bellur, B., and Perrig, A. (2009). Flexible, extensible, and efficient VANET authentication. *Journal of Communications and Networks*, *11*(6), 574-588.

Sultana, R., Grover, J., and Tripathi, M. (2021). Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges. *Vehicular Communications*, *27*, 100284.

Sura, P. R., and Reddy, S. N. (2020). Dual-band Bisected Psi Antenna for 3G, Wi-Fi, WLAN and Wi-MAX Applications. *Journal of Telecommunications and Information Technology*.

Tan, H., Choi, D., Kim, P., Pan, S., and Chung, I. (2018). Secure certificateless authentication and road message dissemination protocol in VANETs. *Wireless Communications and Mobile Computing*, *2018*.

Thorncharoensri, P., Susilo, W., and Baek, J. (2020). Aggregatable Certificateless Designated Verifier Signature. *IEEE Access*, *8*, 95019-95031.

Thumbur, G., Rao, G. S., Reddy, P. V., Gayathri, N., Reddy, D. K., and Padmavathamma, M. (2020). Efficient and Secure Certificateless Aggregate Signature-Based Authentication Scheme for Vehicular Ad Hoc Networks. *IEEE internet of things Journal*, *8*(3), 1908-1920.

Tiwari, D., and Gangadharan, G. (2021). SecAuth-SaaS: a hierarchical certificateless aggregate signature for secure collaborative SaaS authentication in cloud computing. *Journal of Ambient Intelligence and Humanized Computing*, 1-25.

Ullah, K. (2016). *On the use of opportunistic vehicular communication for roadside services advertisement and discovery* Universidade de São Paulo].

Vallent, T. F., Hanyurwimfura, D., and Mikeka, C. (2021). Efficient Certificate-Less Aggregate Signature Scheme with Conditional Privacy-Preservation for Vehicular Ad Hoc Networks Enhanced Smart Grid System. *Sensors*, *21*(9), 2900.

Wang, Y., Zhong, H., Xu, Y., Cui, J., and Wu, G. (2020). Enhanced security identity-

DOI: 10.56892/bima.v6i03.61

based privacy-preserving authentication scheme supporting revocation for VANETs. *IEEE Systems Journal*, *14*(4), 5373-5383.

Xiong, F., Zheng, H., Ruan, L., Wang, H., Tang, L., Dong, X., and Li, A. (2020). Energy-Saving Data Aggregation for Multi-UAV System. *IEEE Transactions on Vehicular Technology*, *69*(8), 9002-9016.

Xu, Z., He, D., Kumar, N., and Choo, K.-K. R. (2020). Efficient certificateless aggregate signature scheme for performing secure routing in VANETs. *Security and Communication Networks*, *2020*.

Yulei, Z., Huan, W., Yanli, M., Wenjing, L., and Caifen, W. (2018). Provable and secure traditional public key infrastructure-certificateless public key cryptography heterogeneous aggregate signcryption scheme. *40*(5), 1079-1086.

Zhang, B., Zhu, T., Hu, C., and Zhao, C. (2018). Cryptanalysis of a lightweight certificateless signature scheme for IIOT environments. *IEEE Access*, *6*, 73885-73894.