Feasibility Analysis of Zero Knowledge Proof Authentication in Internet Of Vehicles

Student Name: Hanna Foerster
Supervisor Name: Dr. Gagangeet Aujla
Submitted as part of the degree of BSc Computer Science to the
Board of Examiners in the Department of Computer Sciences, Durham University

Abstract—Traditional anonymous authentication methods are currently not suitable for the Internet Of Vehicles (IoV) due to their computation or communication costs and problems with maintaining anonymity. So, this paper explores the practicality of a new anonymous mutual authentication protocol called "A ZKP-based Anonymous Mutual Authentication Scheme (ZAMA)", which is designed for the IoV using Zero-Knowledge Proof (ZKP) and Elliptic Curve Cryptography (ECC). ZAMA mitigates the problem of identity leakage and ensures robust user anonymity via the utilization of ZKP. An exhaustive computational and communication overhead analysis, along with a simulation, showcases ZAMA's efficiency. The security goals of mutual authentication, user anonymity, replay attack resistance, forward security, unlinkability, and traceability are met, as demonstrated through a comprehensive security analysis. The effectiveness of ZAMA highlights the potential for the application of ZKPs in other authentication systems including systems with any type of moving smart device such as drones or wearable technology devices.

Index Terms—Anonymous Authentication, Internet of Vehicles, Vehicle Security, Zero Knowledge Proof

1 Introduction

Internet started off with the use of Personal Computers (PCs) and has spread to smartphones. The trend is now moving to even more and smaller embedded devices. While Internet refers to a global network of interconnected computers and servers, now with the terminology of the Internet Of Things (IoT), Internet further encompasses networks of physical devices embedded with network connectivity. The IoT interconnects any smart device that can be uniquely identified with an Internet Protocol address (IP-address) to make data exchangeable and use big data computation to build more intelligent solutions [1]. Smart devices include sensors, processors, and actuators such as communication devices [2] which can be embedded in physical devices or systems. IoT and machine to machine (M2M) connections can be applied to create intelligent automation solutions in many different areas such as manufacturing, transportation, healthcare, energy management, smart homes, and cities, enabling data-driven decision-making, optimization of resources, and improved efficiency and productivity [1]. This paper will be focusing on the Internet of Vehicles (IoV). IoV refers to a broad spectrum of technologies and applications that establish a connection between vehicles and the Internet. This connection enables vehicles to interact with other vehicles, infrastructure, and the cloud, forming an interconnected network. Through the connection with nearby infrastructure and IoV data availability through the cloud, IoV can be the basis for traffic management systems and a backbone to the creation of smart cities.

Vehicular networks, specifically Vehicular Ad-hoc Networks (VANETs), are an older concept than IoV and focus on vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) communication using dedicated short-range communication (DSRC) technology [3]. VANETs are designed to exchange messages between vehicles and roadside infrastructure about traffic, road conditions, and other relevant data, enabling real-time traffic monitoring and accident prevention through traffic management [4]. Road accidents currently account for nearly 1.3 million deaths annually, with predictions suggesting that road accidents will become the fifth leading cause of death by 2030. The cost associated with traffic accidents accounts for about 3% of the world's GDP, equivalent to 1 trillion US dollars [5]. This is why VANETs with their primary focus on improving traffic safety and efficiency are of such utmost importance and have been a critical research focus. VANETs are typically comprised of a trusted authority (TA), a roadside unit (RSU) setup along the road, and an onboard unit (OBU) installed in vehicles [4].

In contrast, the newer concept of the IoV aims to create a comprehensive ecosystem of connected vehicles that can leverage the power of the Internet to enhance the driving experience, enable new services such as automatic communication with toll gates and communication servers located along the highway, and support a variety of applications in areas such as entertainment, navigation, and autonomous driving. The next generation of wireless networks, 5G, promises to deliver highly capable mobile networks with significant improvements in bandwidth (up to 10 Gbps), latency (around 1 ms), and operational costs [2]. This will have a profound impact on the quality of service and experience for users and applications. The premise of 5G would enable a future for autonomous and semi-autonomous driving, as well as entertainment in the car, and much more [2]. Useful V2V communications for example include beacons or basic safety messages that periodically exchange information on factors like velocity, steering wheel angle, and brake system status among nearby vehicles [6]. This kind of future will increase the need of secure networks that connect vehicles

and will demand ever higher efficiency while maintaining core security and privacy concepts. This is because interconnectivity is not only convenient for the average user, but also convenient for malicious actors.

What makes the IoV such a challenging environment is the short time span of communication between RSU and vehicles due to the high vehicle speed but short communication range [4]. Other characteristics that make the IoV environment so demanding include the large number of vehicles, the rapidly changing network topology, the unbounded network size, the frequent exchange of information and network congestion and collision, and the open medium nature of wireless communications [7]. Although compared to other IoT devices, embedded devices in IoV tend to have better energy capabilities and physical protection against tampering [7], compared to PCs for which most network security concepts were established in the past, they still are limited with lower power and are less secure due to not yet fully established security concepts.

Various attack vectors threaten the security of vehicular networks and the safety of the vehicles on the road. These attacks can target different aspects of the network, including availability, authentication/identification, confidentiality, privacy, non-repudiation, and data trust [7]. For example, attacks on availability can be carried out through spamming, broadcast tampering, and Denial of Service (DoS) attacks, while attacks on authentication can include replay/playback attacks, sybil attacks, masquerading, GPS spoofing, and node impersonation [7]. One critical security requirement in vehicular networks is message integrity and authentication, which ensure the legitimacy of the source and integrity of messages [5]. Without proper authentication, attackers can capture critical traffic-related messages, alter them, and disseminate false information, leading to dangerous situations such as traffic accidents [5]. Confidentiality can also be breached through eavesdropping or location tracking, while attacks on data trust can include manipulating sensor readings, sending false information, and affecting message calculations [7]. Moreover, to guarantee privacy, vehicular networks must protect the privacy-related information of users to prevent an observer from revealing their real identities, tracking their locations, and inferring sensitive data [8]. To mitigate these threats, security solutions that prioritize security requirements such as message integrity and authentication, anonymity, revocability, unlinkability, traceability, forward secrecy and replay attack resistance are necessary [9], [10].

As established through the attack vectors, authentication plays a crucial role as the first line of defense to establish a secure IoV environment, restricting communication to only non-malicious and trustworthy devices and people [11]. Authentication methods proposed for VANETs focus on latency due to its time critical nature, energy consumption and reliability, however, not enough focus was put on privacy and anonymity of vehicle drivers. Adding privacy as a requirement for authentication most authentication schemes can be classified in the four following approaches according to [5]: pseudonymous based authentication and privacy schemes (PAPS), group signature-based authentication and privacy schemes (GAPS), ID-Public Key Cryptography based authentication and privacy schemes (IAPS), and hybrid anonymous based authentication and privacy schemes (HAPS). However, these schemes have their weaknesses. PAPS may leak real user identity, require frequent pseudonym updates, and lack strong anonymity. GAPS may have accountability issues, be computationally expensive, and still allow tracking by malicious insiders. IAPS may have key escrow problems, non-repudiation issues, and be vulnerable to catastrophic TA compromise. HAPS may be complex, have performance overheads, security and privacy risks, and lack standardization.

Further, these authentication methods rely on cryptographic functions that are key to determine efficiency and possible anonymity already covered through the function. The most popular cryptographic techniques used in VANET authentication are public-key approaches and are based on bilinear pairings or Elliptic Curve Cryptography (ECC). Boneh and Franklin's identity-based encryption scheme [12] and Boneh, Lynn, and Shacham's short group signature scheme [13] are two significant applications of bilinear pairings used in authentication schemes [14] which utilize Zero Knowledge Proofs (ZKPs) as a primitive guaranteeing anonymity. Even though many schemes accelerate the verification process through batch verification of signatures [5], the cost in terms of computational overhead is significant and high processing power is required [6]. This is why ECC-based schemes have become the more accepted cryptographic method [4]. ECC provides strong security with shorter key lengths compared to other cryptographic techniques, a smaller memory footprint, low computational requirements and efficient computation, which is suitable for authentication of resource-limited devices [15]. It is important to note, however, that the selection of the elliptic curve parameters is crucial to ensuring security [15] and ECC must be combined with an additional anonymity scheme such as pseudonyms since it does not in itself guarantee anonymity.

This is where the concept of ZKPs comes into handy. This has previously not been explored much in the context of IoV authentication outside of pairing based cryptography, but the concept of Zero Knowledge guarantees anonymity. ZKPs are proof systems which allow a prover to prove that he knows some information without revealing its secret [16]. ZKPs have been gaining attention due to its practical applicability, for example in Blockchain. With traditional symmetric and asymmetric key encryption, the secure delivery of keys presents a problem. When the keys are compromised the cryptographic security will instantly be compromised. With ZKPs, this element can be eliminated since the proof is based on statistical verification of knowledge [17]. Further, they do not require complicated security algorithms which involve third parties and can be constructed to be more time efficient than pairing-based schemes and with higher privacy guarantee compared to pseudonym-based ECC schemes.

This paper analyzes a scheme called "ZAMA" from [10] that is an anonymous mutual authentication protocol for IoV that ensures users' anonymity using ZKP and ECC. It uses a lightweight Fujisaki-Okamoto Commitment and ECC as its cryptographic primitive and mechanisms to lighten computational overhead by precalculations are implemented. Our paper first discusses other authentication

protocols and their strengths and weaknesses in terms of anonymity and efficiency in the related works section. Then, in the methodology, the IoV model and threat model from [10] is introduced and the ZAMA protocol from [10] is described in detail. Further, our implementation of ZAMA in a simulation is discussed for the purpose of analysing the performance of the protocol at the end of the methodology section. The results section analyses the ZAMA from a security and efficiency perspective. The proofs of the security guarantees (anonymity, revocability, unlinkability, traceability, forward secrecy and replay attack resistance) that is found in [10] are explained to clarify how ZAMA achieves these security properties and to be able to later assess its suitability for IoV authentication in terms of security and privacy. The efficiency is tested by our simulation and an additional computational and communication overhead analysis which had not been discussed in [10]. Finally, in the evaluation section the results of our analysis are compared to the results obtained in the ZAMA paper and the overall efficiency and security guarantee of ZAMA is reevaluated by us. While the efficiency of the simulation that is presented in the ZAMA cannot be achieved in our simulation, the computational and communication overhead analysis reveals that ZAMA is superior to many of its peer authentication protocols. The aim through this is to show that ZKP authentication methods are efficient with a strong anonymity guarantee and therefore a more viable solution for authentication in IoV compared to other methods.

2 Related Work

Different authentication methods have been proposed to protect users from communication with malicious intent and identity disclosure. To accommodate the resource restrictions of OBUs lightweight protocols using symmetric or ultra-lightweight asymmetric key cryptography are preferred. Symmetric key cryptography uses a shared secret key for message encryption and decryption, ensuring confidentiality and integrity [18]. A popular symmetric key cryptography used in VANET authentication is the Advanced Encryption Standard (AES). Public key cryptography is the alternative to symmetric key cryptography and uses a public and private key pair. Bilinear pairings based cryptography and ECC are examples of public key cryptography. While public key cryptography requires more memory and computational power than shared key encryption, in symmetric key cryptography the key distribution can be a challenge, and the security of the system relies on the secure distribution of the key [19]. Hash functions, hash chains, and bitwise logical operators are also commonly used in combination to provide data integrity verification [20]. Although hash functions are efficient, they are vulnerable to collision attacks that can compromise system integrity.

Taking into account these properties of cryptographic functions as a starting point, we will proceed to assess previous research on IoV authentication, using the grouping categories proposed by [5]: pseudonymous based authentication and privacy schemes (PAPS), group signature-based authentication and privacy schemes (GAPS), ID-Public Key Cryptography based authentication and privacy schemes (IAPS), and hybrid anonymous based authentication and privacy schemes (HAPS) [5] and a last additional category, which are authentication schemes that use ZKPs.

2.1 Pseudonymous based authentication and privacy schemes (PAPS)

PAPS are schemes where anonymity is based on the concept of pseudonyms. Pseudonyms are false names that are used as an alternative to the real name and that should be made so that there is no linkability to information that would reveal the real identity [5]. To implement such a system each entity can only use one master secret/public key pair external to the pseudonym system [21]. The entity creates a pseudonym X that reveals their real identity (RID) and authenticates themselves as the valid owner with the TA, while the TA proves the validity by checking RID(X) = secret/public key pair [5]. The TA then issues a validity credential for X, which the entity transfers to other organizations to prove their authenticity. The PAPS system includes a certificate revocation list (CRL) containing revoked vehicle information, which is transmitted from vehicle to vehicle during message broadcasting. However, the increase in the size of the CRL can result in communication overhead. Additionally, some schemes do not preserve privacy between vehicles and RSUs [5]. PAPS based schemes cannot guarantee unlinkability of vehicle users because the pseudonyms used by the same user may be correlated over time. As a result, an adversary may link a user's activities over time using the same pseudonym. Additionally, frequent pseudonym updates are required to improve security, which puts an additional burden on vehicles [10].

In [9] the premise of bilinear pairing and dummy identities are used to enable anonymous V2V and V2I communication. They also use the popular concept of batch authentication. Nevertheless, in [10] it is shown that the latency due to the scheme's use of exponentiation, multiplication and pairing operations and communication overhead due to the frequent exchange of messages between vehicles and RSUs for certificate validation and revocation list updates is not competitive. Further, the scheme provides anonymity and unlinkability, but it does not offer strong traceability. This means that in case of a security breach or violation, it may be difficult to identify the culprit. Additionally, the scheme requires a large amount of storage for each vehicle to store its own and other vehicles' certificates and revocation lists. This may pose a challenge in resource-constrained environments.

Zhang et al. [4] propose a scheme that relies on solving the elliptic-curve discrete logarithm problem. The identity is kept hidden through pseudonyms that are changed after random time intervals and batch authentication functionality is also given. The main disadvantage of the scheme is that it relies on a TA to generate and distribute system parameters, which could be a point of vulnerability. Additionally, the scheme does not provide any protection against replay attacks or collusion attacks and the anonymity depends on the time interval in which pseudonyms are changed giving a tradeoff between overhead introduced through frequent pseudonym updates and anonymity. Finally, the revocation process requires frequent communication with the TA, which could result in increased network traffic and delay.

2.2 Group signature-based authentication and privacy schemes (GAPS)

In GAPS, anonymity is provided to the sending vehicle through the use of group signature (GS) based authentication. The group is comprised of members and a manager, where each member has a unique key pair consisting of a member private key and a group public key, based on PKI [5]. To sign a message, a group member uses its own secret key with respect to the group key. To verify a sent message, only the group public key is needed, and the sender identity is not revealed. If the scheme is made well there is also an additional algorithm that the group manager can run if a specific group member needs to be traced [5]. However, if this is not the case group signatures allow any member of the group to anonymously sign a message on behalf of the group, which may lead to accountability issues in case of misuse or illegal activities. GS ensure scalability and exculpability and possibly non-traceability. However, security against replay attacks or collusion attacks is not necessarily provided. Additionally, the verification process incurs computational overhead for key distribution and management (e.g. pairing operations), which increases with the message loss ratio [5]. Lastly, group signature-based schemes may not provide strong privacy guarantees since a malicious insider can still track the identity of the signer within the group.

The privacy-preserving authentication scheme proposed by Zhu et al [22] utilizes distributed management, Hash Message Authentication Code (HMAC), batch group signature, and cooperative authentication techniques. The precinct is divided into several domains, and RSUs manage vehicles and distribute group private keys in a localized manner. HMAC is used to ensure message integrity before batch group authentication and avoiding time-consuming CRL checking. Cooperative message authentication is also used to alleviate the authentication burden, with each vehicle verifying only a small number of messages. Disadvantages of this scheme are that the use of HMAC and cooperative message authentication could introduce additional computational overhead in message processing particularly for dense networks. Further, the scheme does not provide unconditional privacy, meaning that some information about the vehicle's identity or location may still be revealed to the RSUs or other authorized entities.

Similarly, Shao et al. [23] proposed a threshold anonymous authentication protocol for VANETs that combines a group signature with threshold cryptography. The protocol uses an RSU-assisted approach to distribute group keys to vehicles and threshold cryptography to achieve authentication and anonymity. The scheme allows a subset of RSUs to collaboratively sign messages on behalf of the group to reduce the computational burden on vehicles. The proposed protocol can withstand collusion attacks by up to t malicious RSUs, where t is a threshold value. A main disadvantage of the scheme are that the joint signing process may introduce some communication overhead and delay, especially when the threshold number of vehicles is large. This means that if efficiency is prioritized anonymity and security might not be upheld. Additionally, anonymity is conditional on the assumption that at least a certain threshold number of vehicles participate in the joint signing process.

2.3 ID-Public Key Cryptography based authentication and privacy schemes (IAPS)

IAPS use a cryptographic technique where the public key is derived directly from an entity's public known identity information, such as an email address or telephone number, thereby eliminating the need for certificate management as in traditional PKI [5]. This enhances the efficiency of VANETs by reducing the overhead produced from the messages containing certificates. However, this approach has some disadvantages related to key escrow problems, non-repudiation, and catastrophic compromising of TA [5]. Since the private key is generated by a trusted third party, such as a certificate authority, there is a risk that the third party may misuse or disclose the private key, which would compromise the security of the entire system. This issue called the key escrow problem is particularly concerning in situations where the third party is not trustworthy or is compromised. Another drawback is related to non-repudiation. Since the private key is generated by the third party, it is possible for the third party to forge a signature on behalf of the user. This can make it difficult to establish the authenticity of a message or transaction. Additionally, IAPS can be vulnerable to catastrophic compromising of the TA. If the TA's private key is compromised, an attacker can impersonate any user in the system, leading to a complete breakdown of the security of the system.

Zhang et al. [24] proposed an efficient scheme for secure and privacy-preserving vehicular communication authentication, which utilizes identity-based aggregate signatures and encryption techniques. The scheme enables hierarchical aggregation and batch verification, significantly reducing transmission and storage overhead. Vehicles generate signed messages which are received by nearby RSUs that aggregate and verify them in batches. The aggregated messages are further aggregated, verified, and analyzed by traffic management authorities. The scheme is designed for both periodic and non-periodic messages and allows for fast response times. The use of identity-based methods reduces the cost required for certificate management and verification. The scheme is based on bilinear pairing and enables conditional privacy-preserving; however, it is not collusion resistant and fulfills neither unlinkability nor unforgeability.

In [4], an efficient batch signature verification scheme for Vehicular Sensor Networks (VSNs) using bilinear pairing and identity-based cryptography is proposed. The scheme allows a RSU to verify a group of signatures at the same time, reducing the total verification time. The scheme also maps each message launched by a vehicle to a distinct pseudo identity, achieving conditional privacy preservation. A trust authority can retrieve the real identity of a vehicle from any pseudo identity in case of dispute from a vehicle site. Since certificates are not needed with identity-based cryptography, transmission overhead is significantly reduced. However, the scheme is susceptible to the key escrow problem in IAPS, meaning that if the trust authority is compromised, all communications between RSU and vehicles will be insecure.

2.4 Hybrid anonymous based authentication and privacy schemes (HAPS)

HAPS are authentication schemes that combine various mechanisms to achieve a balance between computational efficiency, communication efficiency, bandwidth utilization, and verification delay. These mechanisms include pseudonymous authentication protocols, group-based signature schemes, ID-based schemes, message authentication codes (MACs), and other authentication and privacy mechanisms [5]. The goal of HAPS is to overcome the limitations of individual schemes by leveraging the strengths of multiple mechanisms. However, there are several drawbacks to HAPS, including complexity, performance overhead, security risks, privacy risks, and lack of standardization. HAPS can be complex to implement and manage due to the use of multiple authentication and privacy mechanisms, and the use of multiple mechanisms can result in a higher performance overhead in terms of computation, communication, and verification. The combination of different mechanisms in HAPS can create security risks, as vulnerabilities in one mechanism can affect the overall security of the system. Additionally, HAPS can still have privacy risks, as the use of pseudonyms, group signatures, and other mechanisms can still allow for tracking and identification of users in certain scenarios [5]. Finally, the lack of standardization in HAPS can make interoperability between different systems difficult and can hinder the adoption of these schemes.

The scheme proposed in [25] is a hybrid scheme using pseudonyms and GS. Pseudonyms in this context can be used to provide an additional layer of anonymity by hiding the identity of the sender even within the group. Each vehicle generates their own pseudonyms and corresponding private keys on-the-fly using the GS on each pseudonym. Each valid vehicle can produce their own certificate which contains pseudonym and public key and attach this to each message. Adding to properties of unidentifiability of sender, a received certificate and pseudonym cannot be linked to prior pseudonyms. One of the key advantages of this scheme is its efficiency in terms of computation due to only requiring basic cryptographic operations such as hashing, encryption and decryption and communication overhead. However, it does not provide protection against certain types of attacks, such as collusion attacks, and it may be vulnerable to Sybil attacks in which a malicious vehicle generates multiple pseudonyms to gain influence in the network.

The Two-Factor Lightweight Privacy-preserving authentication scheme (2FLIP) proposed by Wang et al. [26] uses a decentralized TA and a biological-password-based two-factor authentication (2FA) to achieve its goals. Due to the TA decentralization, 2FLIP uses lightweight hashing processes and a fast MAC to sign and verify messages between vehicles. The scheme is equipped with a telematics device that uses biometric technology for multiple drivers' identities verification and tracing. 2FLIP provides strong privacy preservation and non-repudiation and is resilient to DoS attacks. It significantly reduces computation and communication overhead and does not require any CRL-related overhead on vehicles. The scheme has an outstanding performance of nearly 0-ms network delay and 0% packet-loss ratio, making it suitable for real-time emergency reporting applications. However, the use of biometric authentication raises privacy concerns, and the reliance on telematics devices can limit the widespread adoption of the scheme due to device availability and compatibility issues.

2.5 ZKP-based authentication schemes

ZKP-based authentication schemes can provide a high degree of privacy and security without requiring the exchange of sensitive information, such as private keys or passwords. Moreover, some ZKP-based authentication schemes can achieve high levels of efficiency by using techniques such as batch verification, pre-computation, and lightweight cryptography. This can help to reduce the overhead of authentication and enable real-time communication in VANETs.

In the context of VANETs, existing authentication technologies based on security policies and access control rules assume full trust on the RSU and authentication servers (AS) or TAs, leading to the disclosure of authentication parameters and violation of user privacy and anonymity. To address this, Rasheed et al. [3] proposed a novel, light-weight, adaptive group-based zero-knowledge proof-authentication protocol (AGZKP-AP) for VANETs. Their scheme offers various levels of user privacy settings based on the type of services available on the network and lets users make decisions on the tradeoff between resource utilization and privacy. The protocol is incorporated with a distributed privilege control and revoking mechanism that allows law enforcement to access user's private information in case of a traffic violation. However, in [10], this scheme is criticized for not guaranteeing user traceability in case of illegal uses. Nonetheless, the scheme appears to be very efficient, with the only drawback being the interactive nature of the ZKP protocol, leading to a higher communication cost and a possible higher message loss rate.

Chistousov et al. [27] propose an adaptive ZKP authentication protocol which eliminates the need for multiple authentication rounds and adapts parameters for efficiency while maintaining confidentiality. Session keys create an open communication channel after authentication, based on the complexity of solving the Diffie-Hellman problem. While the paper evaluates the protocol based on volume of information traffic, comparing it to authentication schemes analyzing authentication time by traffic intensity could be interesting. Additionally, Fuchsbauer et al. [28] proposed an anonymous credential system based on ZKPs that verifies ownership of user attributes and logical relationships between attributes. The scheme ensures constant proof size for a user's attributes and their proven logical relationships. However, it only supports logical AND and OR relationships between attributes, which may limit its applicability in some scenarios.

The literature exploration reveals that current authentication schemes for vehicular systems have weaknesses such as identity leakage, performance overheads, and key escrow problems. To address these limitations, ZAMA [10] proposes a novel anonymous authentication scheme that uses ECC cryptography and a ZKP approach. The ZAMA scheme achieves efficient mutual authentication while maintaining anonymity, unlinkability, traceability, forward security, and

resistance to replay attacks. Additionally, the scheme employs lightweight cryptography operations, which result in superior performance during the vehicle's registration, authentication, and reconnection. This approach overcomes the limitations of existing authentication schemes and offers a promising solution for secure and efficient authentication in vehicular systems.

3 Methodology

This section first discusses the IoV context in which the ZAMA protocol was proposed. This includes the model of the IoV and the threat model used in [10]. Then the ZAMA framework from [10] that was built on these models is explained in detail and finally our practical implementation of the protocol on a simulation software is described.

3.1 IoV Environment

3.1.1 IoV Model

The IoV environment comprises three main entities: the TA, AS/RSU, and Vehicular User (VU)/OBU. The VU wants to build a connection with an RSU in order to access various services such as broadcast on traffic situations. In order to prevent illegal access, the system requires vehicles to be authenticated before accessing these services [10]. The model of the IoV system is shown in Figure 1.

- **TA**: The TA works as a trusted third-party that initializes the entire system and is responsible for managing cryptographic parameters, private/public keys, and more. The TA not only assists in identifying unauthorized users in case of a violation during service execution, but also helps in reducing the computation overhead of vehicles by performing pre-calculations [10].
- **AS/ RSU**: The RSU is a base station that is deployed along the roadside and acts as an intermediate node between the TA and OBUs [5]. The AS is located inside a RSU and is responsible for verifying the identity of the VU who attempts to access cloud services and it stores the VU's credentials, including their user identity, for authentication purposes. To ensure privacy, all VU identities are stored in ciphertext mode. It is important to note that in our model, the AS is required to authenticate users without disclosing their real identities [10].
- **VU/OBU**: The VU serves as the end-user seeking to access a range of IoV services via the RSU. Due to its mobile nature, the VU may frequently establish or break connections with the cloud [10]. The OBU is installed on a vehicle to receive, process, and transmit traffic-related information to other vehicles and RSUs using DSRC protocols [5]. DSRC uses the IEEE 802.11p standard for wireless communication, allowing vehicles to disseminate traffic-related messages within a time interval of 100-300ms to other vehicles or RSUs [5].

The communication in IoV systems is classified as V2V and V2I, with V2V communication allowing vehicles to exchange messages about traffic conditions, weather, accidents, and more. V2I communication provides information

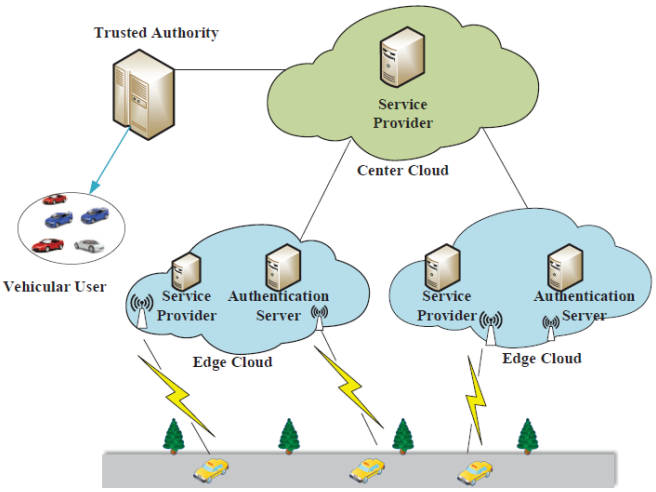


Fig. 1: Model of IoV from [10]

to vehicles about road safety and traffic management, and also provides value-added services like Internet access, navigation, and real-time multimedia streaming to drivers and passengers through RSUs [5]. In exceptional circumstances, drivers can make informed decisions or respond quickly based on the received information. The communication speed in VANETs ranges from 6 to 27 Mbps, and the maximum transmission coverage is up to 1,000m, with a typical range of 100 to 1000m using the 802.11p protocol [5].

To access IoV services, the VU connects to the RSU and the AS authenticates the VU who tries to access the services in the cloud. The Edge Cloud (EC) provides a few edge services with lighter memory and computation loads to legal users who passed authentication [10]. Edge computing is a solution that involves the cooperation of devices in the network to evaluate data locally, reducing communication costs and enhancing privacy and security [29]. Both the RSU and AS are located in the EC. The center cloud provides more powerful services to the VU, such as machine learning tasks. VU can access these services through the EC [10].

3.1.2 Threat Model

In the context of vehicular networks, there are various attack vectors that can threaten the security and safety of the vehicles on the road. These attacks can target different aspects of the network, including availability, authentication/identification, confidentiality, privacy, non-repudiation, and data trust [7]. Attacks on message integrity and authentication are critical, as they can lead to dangerous situations such as traffic accidents if attackers capture and alter critical traffic-related messages. The following is the threat model that was constructed in [10] that we will be following in this paper.

Our threat model posits that TA is a reliable third-party that is securely connected to AS via a wired channel. The setup process between TA and VU is performed offline when a new VU is registered in TA, and the communication channel between TA and VU is also deemed secure. However, AS in the EC is considered honest but curious, meaning it cannot be fully trusted. Although AS adheres

to our proposed scheme and responds to queries faithfully, it may aggressively collect sensitive information, such as identity-related data. Moreover, the wireless channels between the VU and AS are vulnerable, allowing an attacker to eavesdrop, intercept, replay, and fabricate any message. Our threat model takes into account two types of attacks: the *insider attack* and the *outsider attack*.

(i) The *insider attack* occurs when either EC or AS administrators or a compromised AS unlawfully collect and deduce the user's true identity.

(ii) The *outsider attack* on IoV involves an attacker disguising themselves as a legitimate VU or replaying messages, all while observing the messages to collect sensitive user information in an attempt to access EC's services.

ZAMA is a novel anonymous authentication scheme that addresses these threats during IoV authentication satisfying following security goals [10].

- **Mutual Authentication** Allows the identification of illegal VUs or fake ASs.
- **Anonymity** Ensures that VU's real identity is kept secret during the authentication process. Pseudonyms of VU's that may be obtained do not give any information as to the VU's real identity.
- **Unlinkability** Even if the wireless channel is under control of an adversary or AS is compromised, the VU cannot be identified or linked to their real identity by adversaries.
- **Traceability** Allows TA to trace the VU and hold them accountable if a violation occurs during the execution of IoV services.
- **Forward Security** Ensures that attackers cannot obtain any useful information about the previous session, even if they have all the information about the current session.
- **Replay Attack Resistance** The replay of past legitimate messages between VU and AS cannot pose a threat.

3.2 ZAMA framework

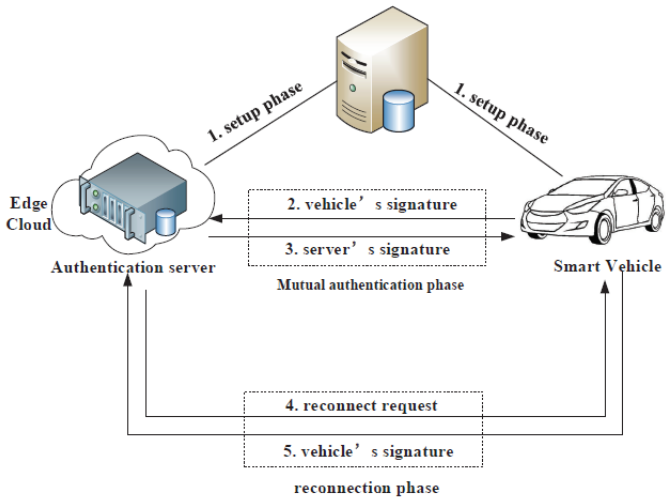


Fig. 2: ZAMA framework from [10]

The proposed scheme ZAMA [10] is according to the authors designed to establish mutual authentication between VU and AS in the EC, while preserving the anonymity of the VU. The ZAMA framework is depicted in Fig. 2 and comprises four distinct phases, namely registration, authentication, fast reconnection, and revocation [10].

In the registration phase, each vehicle is initialized by TA upon registration. When a smart vehicle seeks to access services in the EC or central cloud, the authentication between AS and VU is activated. During the authentication process, mutual authentication is achieved using ECC cryptography, while ZKP is employed to hide the user's identity from server administrators [10].

In case of a quick disconnection and reconnection of a VU, such as when switching RSUs, the fast reconnection process is initiated to simplify the authentication process based on the last authentication. This enhances the efficiency of the VU's access and ensures the quality of the IoV service [10].

3.2.1 Basic Cryptographic Operations

There are two cryptographic functions that the ZAMA scheme uses, which are ECC cryptography and the Fujisaki-Okamokoto (FO) Commitment Protocol [30], which makes up the zero knowledge part of the protocol. The following two definitions are taken from the ZAMA paper [10]:

Definition 1: **Elliptic Curve:** The elliptic curve E defined on the finite field Z_q is expressed as $E = q, q, b, G, n$. All points on the curve satisfy the equations:

$$y^2 = x^3 + ax + b \pmod{q} \tag{1}$$

$$\forall a, b \in Z_q, 4a^3 + 27b^2 \neq 0 \pmod{q} \tag{2}$$

Where G is a point on the curve E with order n, called the generation point [10].

Definition 2: **Fujisaki-Okamoto Commitent protocol:** t, l, s_1, and s_2 are four security parameters. Let n be a large composite number whose factorization is unknwon. g_1 is an element of large order in Z_n and g_2. h_1 and h_2 are elements of the group generated by g_1. Alice does not know $log_{g_1} h_1, log_{h_1} g_1, log_{g_2} h_2$ and $log_{h_2} g_2$. H is a hashfunction. Alice secretly holds $x \in [0, b]$. Let $E = e_1(x, r_1)$ and $F = E_2(x, r_2)$ be two commitments to x. In order to prove that Alice knows x, r_1 and r_2, Bob can verify Alice's commitment E, F, where E, F hide the same secret x.

1) Alice picks random $\omega \in [1, 2^{l+tb} - 1], \eta_1 \in [1, 2^{l+t+s_1} n - 1]$ and $\eta_2 \in [1, 2^{l+t+s_2} n - 1]$. Then she computes

$$W_1 = g_1^{\omega} h_1^{\eta_1} \pmod{n} \tag{3}$$

$$W_2 = g_2^{\omega} h_2^{\eta_2} \pmod{n} \tag{4}$$

2) Alice computes $c = H(W_1 \parallel W_2)$. Then she computes

$$D = \omega + cx \tag{5}$$

$$D_1 = \eta_1 + cr_1 \tag{6}$$

$$D_2 = \eta_2 \tag{7}$$

and sends c, D, D_1, D_2 to Bob.

3) Bob checks whether c satisfies

$$c = H(g_1^D h_1^{D_1} E^{-c} \parallel g_2^D h_2^{D_2} F^{-c}) \pmod{n} \quad (8)$$

When this protocol is executed without any error, Bob will be confident that E and F conceal identical secret numbers. The protocol can be considered statistically Zero-knowledge in the random-oracle model if $1/l$ is negligible [10].

In Table 1 all mathematical notation that is used throughout the mathematical description of the protocol in registration, authentication and revocation is summarised.

3.2.2 Registration Phase

The Registration process which is the preparation phase for the authentication scheme from [10] is described in this subsection. The main goal of this initial process is for the TA to generate public and private keys for the AS and to generate the aforementioned commitments and secret value for the VU. The commitments ensure the anonymity of the vehicle to the AS and EC. First, the security parameters are chosen. In the field of cryptography, a security parameter is used to determine how difficult it is for an attacker to break a cryptographic system [31]. The security of the FO protocol depends on the hardness of two problems: the decisional Diffie-Hellman (DDH) problem and the discrete logarithm problem (DLP). Therefore, the parameters must be selected such that solving these problems is computationally infeasible. It is important to note that the security of the protocol depends on the choice of parameters, and that these parameters must be kept secret. In the case of the DDH problem, the security parameter is usually measured in terms of the length of the prime modulus p used in the scheme. A typical security parameter for the DDH problem might be 2048 bits or higher. In the FO commitment protocol however, the modulus used is a composite number n whose decomposition is only known by the TA. To be able to sample a secure such n and secure parameters g_1, g_2, h_1, h_2 from the multiplicative group Z_n that does not allow for certain shortcuts to solving the DDH or DLP problem, distinct safe primes p and q must be sampled such that $(p-1)/2$ and $(q-1)/2$ are also prime. This is because for a random a in $[2, n-2]$, $g = a^2$ will then have order $(p-1)(q-1)/4 \approx n/4$ unless a, $a-1$ or $a+1$ is relatively prime to n. However, the probability of that is negligible with less than $3/p + 3/q$ [32]. h can be sampled in a similar way.

Similarly, in the case of the DLP, the security parameter is measured in terms of the length of the group elements used in the scheme. As a general rule, the larger the security parameter, the more secure the scheme is against attacks but the more the computation time is also increased. For example, a typical security parameter for the DLP might be in the range of 256 to 512 bits. Security parameters that influence the length of the group elements are s, b, t, l which determine the range of exponent size from which to sample. Further, the elliptic curve parameters for the AS must be generated along with the public key PK_H and private key k_h of the AS [10]. There are several elliptic curves that were deemed unsecure, so it is important that a secure curve is taken as a basis. Moreover, H is an ideal collision-resistant hash function. $n, g_1, g_2, h_1, h_2, PH_H$ and the hash function H are public and preloaded into VU and AS. After this preparation of parameters, the registration involves following five steps, which can also be seen in a digested graph in Fig. 3

TABLE 1: MATHEMATIC NOTATIONS from [10]

Notation	Description
S	server ID
VID	vehicle User ID
Z_n	multiplicative group
g_1, g_2, h_1, h_2	random numbers selected in cyclic group
a, b, t, l, s	the secret parameters generated by TA
r_1, r_2, x	users' secret parameters selected by TA
K_i	the i-th user's secret key selected by TA
E, F	the users' commitment computed by TA
w, q_1, q_2	random parameters generated by user
PK_U	the vehicle user's public key
N_d	a random number generated by server
E_H	the generator of a cyclic group
PK_H	the server's public key
k_H	the server's private key
α, β	random numbers selected by user
ξ_1, ξ_2	secret parameters selected by TA
u, v, h	public parameters generated by TA
DB	TA's database
RL	revoked list
P	the generate proof
AL	server's authenticated list
H	the collision-resistant hash function
K_s	the session key
K_n	the new session key

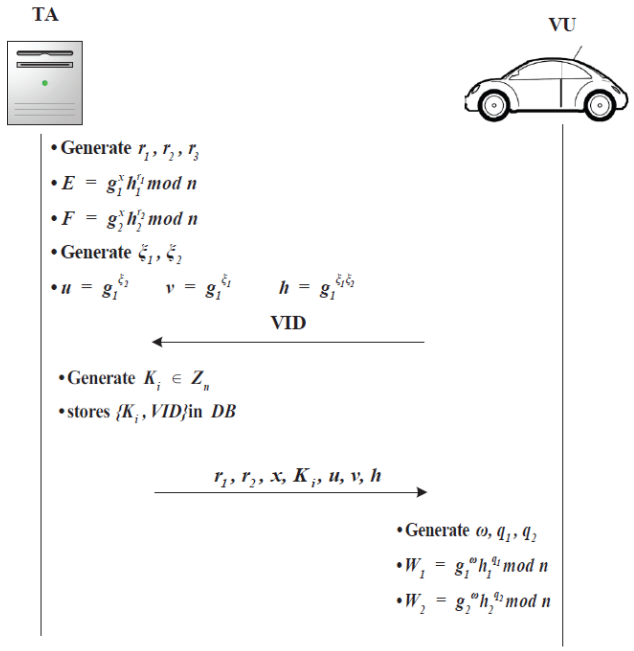


Fig. 3: Registration Phase from [10]

Step 1: Secret parameters r_1, r_2, x are selected randomly by the TA: $r_1 \in [-2^s n + 1, 2^s n - 1], r_2 \in [-2^s n + 1, 2^s n - 1], x \in [0, b]$. In the case that either r_1 or r_2 is in range $(0, 1)$ the inverse $\pmod{n}$ can be calculated with the Extended Euclidean Algorithm (EEA).

Step 2: Commitments E, F are computed by the TA using the secret parameters from Step 1:

$$E = g_1^x h_1^{r_1} \pmod n \tag{9}$$

$$F = g_2^x h_2^{r_2} \pmod n \tag{10}$$

Then, the TA randomly selects ξ_1 and $\xi_2 \in Z_n$ and computes u, v, h which make up the public key PK_U of VU:

$$u = g_1^{\xi_2} \tag{11}$$

$$v = g_1^{\xi_1} \tag{12}$$

$$h = g_1^{\xi_1 \xi_2} \tag{13}$$

The TA commits the commitments E, F to the AS while keeping r_1, r_2, x secret and initializes a revocation list RL and a database DB that is kept secret.

Step 3: After preparation is done on the TA side, the VU sends its Vehicular ID (VID) to the TA to start its registration.

Step 4: The TA generates a random secret key $K_i \in Z_n$ for the $i-$th user and assigns r_1, r_2, x, K_i, PK_U to the VU. Consequently, the secret key is stored alongside the VID in the DB as K_i, VID.

Step 5: The VU receives r_1, r_2, x, K_i and parameters $w \in [1, 2^{t+l}b - 1], q_1 \in [1, 2^{t+l+s_1}b - 1], q_2 \in [1, 2^{t+l+s_2}b - 1]$ are randomly generated. The following part of the ZKP proof can be then precalculated before authentication:

$$W_1 = g_1^w h_1^{q_1} \pmod n \tag{14}$$

$$W_2 = g_2^w h_2^{q_2} \pmod n \tag{15}$$

3.2.3 Authentication Phase

The authentication of the vehicle is based on the FO commitment protocol that provides a way of authentication without disclosing the VID through a ZKP [30]. The ZKP that the VU provides is enough for the AS to verify the VU's identity. Traceability options however are provided through the TA. The digested form of the authentication phase can be seen in Fig. 4

Step 1: The VU sends an authentication request. A nonce N_d which should be included in the proof is generated by the AS and sent to the VU. This nonce prevents replay attacks.

Step 2: VU receives N_d, generates a session key K_s and then starts generating the rest of the ZKP P:

$$P = C, D, D_1, D_2 \tag{16}$$

with C, D, D_1, D_2 calculated as:

$$\begin{aligned} C &= H(W_1 \parallel W_2 \parallel N_d) \\ D &= w + Cx \\ D_1 &= q_1 + Cr_1 \\ D_2 &= q_2 + Cr_2 \end{aligned} \tag{17}$$

Step 3: After the computation of the proof P, random numbers α, β are generated to calculate following parameters using K_i:

$$\begin{aligned} T_1 &= u^\alpha \\ T_2 &= v^\beta \\ T_3 &= K_i * h^{\alpha+\beta} \end{aligned} \tag{18}$$

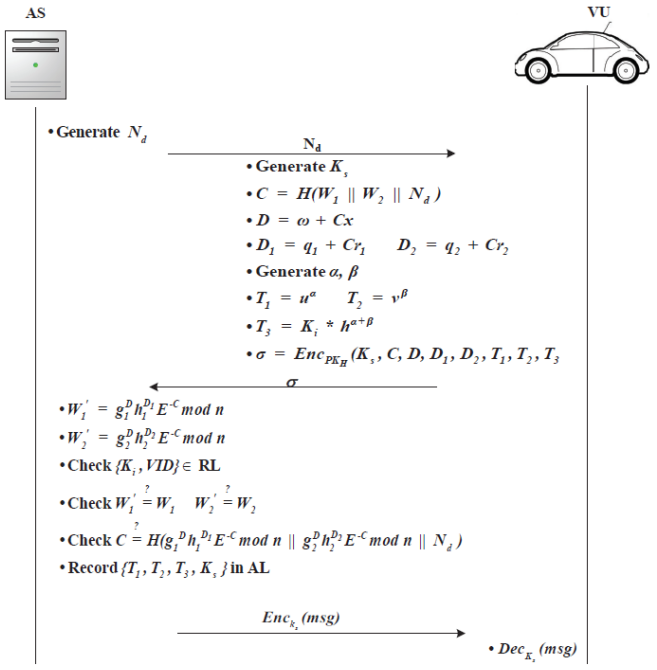


Fig. 4: Authentication Phase from [10]

This is a signature computed so that the TA can trace the VU in case of violations.

Step 4: To send the proof, signature and session key, the VU encrypts them with AS's public key PK_h:

$$\sigma = Enc_{PK_H}(K_s, C, D, D_1, D_2, T_1, T_2, T_3) \tag{19}$$

and sends this to AS.

Step 5: Upon receipt of the σ AS decrypts the message with its private key, to obtain the proof P and session key K_s and signature T_1, T_2, T_3. T_1, T_2, T_3 are directly sent on to the TA through a secure channel to check its identity against the RL. The VID can be obtained from T_1, T_2, T_3 by the TA, using ξ_1, ξ_2 in the following way:

$$\begin{aligned} \frac{T_1^{\xi_1} T_2^{\xi_2}}{T_3} &= \frac{(u^\alpha)^{\xi_1} (v^\beta)^{\xi_2}}{K_i * h^{\alpha+\beta}} \\ &= \frac{(u^{\xi_1})^\alpha (v^{\xi_2})^\beta}{K_i * h^{\alpha+\beta}} \\ &= \frac{((g_1^{\xi_2})^{\xi_1})^\alpha ((g_1^{\xi_1})^{\xi_2})^\beta}{K_i * (g_1^{\xi_1 \xi_2})^{\alpha+\beta}} \\ &= \frac{(g_1^{\xi_1 \xi_2})^{\alpha+\beta}}{K_i * (g_1^{\xi_1 \xi_2})^{\alpha+\beta}} \\ &= \frac{1}{K_i} \end{aligned} \tag{20}$$

Obtaining K_i from $1/K_i$, the TA can check whether there exists a record K_i, VID in RL and sends the results of this check to the AS. If this record exists, this means that the vehicle is potentially malicious and the AS sends authentication failed to the VU. Otherwise, the AS now continues on to validate the proof sent to them by the VU. For the VU to be valid $W_1' = W_1$ and $W_2' = W_2$ must hold, where

$$W_1' = g_1^D h_1^{D_1} E^{-C} \pmod n \tag{21}$$

$$W_2' = g_2^D h_2^{D_2} E^{-C} \pmod{n} \quad (22)$$

and consequently AS can verify VU by checking:

$$C = H(W_1' \parallel W_2' \parallel N_d) \quad (23)$$

Step 6: The verification succeeds if the proof is correct and the AS can conclude that the vehicle is legal. Then, the AS sends a message encrypted by the session key K_s signalling success to the VU. Additionally, the AS maintains a list of recently successfully authenticated VU called activation list (AL), where records of the form T_1, T_2, T_3, K_s are kept for each recently authenticated VU.

Step 7: Finally, if the decryption of the message sent to the VU by the AS is successful, the authentication process ends successfully.

3.2.4 Fast Reconnection Phase

Since vehicles are mobile, it is possible that the connection between the VU and the EC may get disrupted frequently. To address this in [10], a fast reconnection protocol was developed. In this protocol, the VU can use the previously established session key K_s to quickly resume the session with the EC, without having to go through the entire authentication procedure again. The steps involved in this fast reconnection procedure are illustrated in Fig. 5

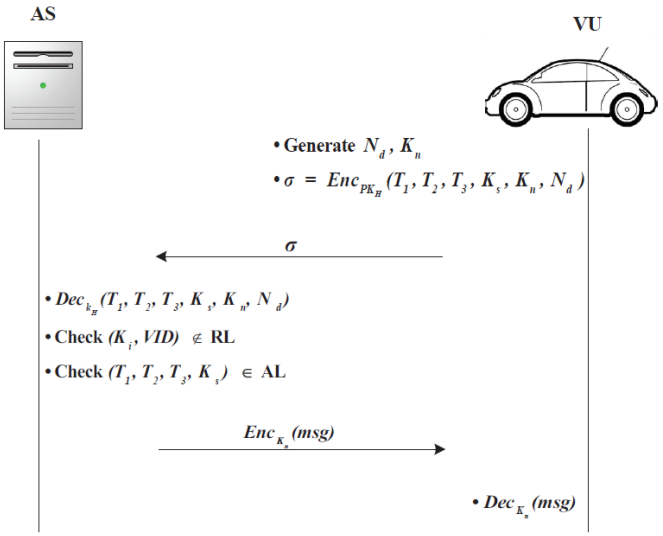


Fig. 5: Fast Reconnection Phase from [10]

Step 1: To reconnect the VU first generates a new session key K_n and a nonce N_d and encrypts a message M containing the signature, the old session key, the new session key and the nonce with public key PK_H of the AS.

$$\sigma = Enc_{PK_H}(T_1, T_2, T_3, K_s, K_n, N_d) \quad (24)$$

Step 2: As in the authentication process upon receival of σ, AS sends T_1, T_2, T_3 to TA for verification. If the vehicle is not in the RL, the AS checks the AL list, in which all recently authenticated vehicle pseudo identities are stored. If VU exists in AL, the vehicle is valid and the pseudo identity is updated to T_1, T_2, T_3, K_n, where K_n is the new session key. In this case an authentication success message is sent back to the VU encrypted by this new session key.

Step 3: Finally, if the VU successfully decrypts this message the VU is successfully re-authenticated.

3.2.5 Revocation Phase

In the IoV system, frequent connection and disconnection between VU and EC are common. Revocation of outdated VUs is necessary to maintain the system's security. ZAMA protocol considers the revocation procedure, which involves checking if the revoked identity Ki, VID is in the database DB. If it is not, the revocation process can be completed. However, if it exists, TA adds Ki, VID to the revocation list RL and the revoked VU's record must be deleted from DB. The AS must also delete the vehicle's records from the AL. If a vehicle must be identified because of criminal violations the TA can use the signature T_1, T_2, T_3 as described in 20 to obtain K_i and then the VID from DB.

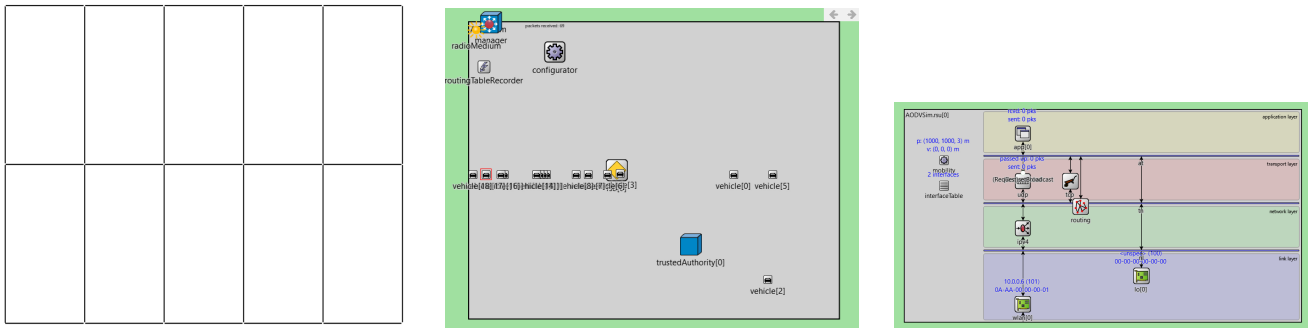
3.3 Practical implementation

We have implemented a simulation of this protocol to be able to understand better the practicality of the protocol for later analysis.

The simulation program used is called OMNET++ and specifically version 5.6.2 [33] was used. This was combined with VEINS version 5.2 [34], INET version 4.2.2 [35] and SUMO version 1.8.0 [36]. INET is a framework for modeling and analyzing communication networks, while VEINS is a framework for simulating vehicular communication networks. The two frameworks were combined to create INET-VEINS, a comprehensive simulation environment for vehicular communication networks. It supports multiple communication technologies, mobility models, and traffic generators, and is widely used in academia and industry. SUMO is an open-source traffic simulation framework used for modeling and simulating traffic networks.

The simple grid map (Fig. 6a) and a basic code base for a VANET was taken from [37] as a starting point. This is a different setup from the original paper, where a vehicular mobility dataset was taken from data collected around some roundabout in France. This setup could not be taken because this dataset was not available online. Furthermore, it is of greater interest to analyze the protocol from a different setup to see how this affects the performance of the protocol. Up to 100 vehicles are simulated to be on the grid map at the same time. As can be seen in Fig. 6b a radio medium, a network configurator, a routing table recorder, an RSU, a TA and multiple VUs are setup in the network. In OMNeT++ simulation, the radio medium simulates the wireless propagation and interference effects between nodes. The network configurator is a GUI tool used to create, configure, and manage network topologies. The routing table recorder module records routing tables of network nodes during simulation runs to analyze the performance of routing protocols. The recorded routing tables can be stored in a file for offline analysis.

The network topology (seen in Fig. 6c) follows the layered architecture of the OSI model, with each layer having a specific function. The physical layer deals with the physical transmission of data over the medium, while the data link layer is responsible for error detection and correction, as well as medium access control. The network layer provides



(a) Simple grid network (b) Omnet++ setup of TA, RSU, VUs (c) Network layer setup

Fig. 6: Simulation network

routing and addressing functionality, and the transport layer ensures reliable data transfer between applications. The application layer deals with the actual content of the data being transmitted. The layers work together to facilitate communication between network nodes and ensure efficient and reliable data transfer.

In the physical and link layer the wireless communication standard protocol in vehicular networks IEEE 802.11p was used. It is an amendment to the IEEE 802.11 standard that defines the physical and medium access control layers for wireless communication in the 5.9 GHz band. This band is allocated for use by intelligent transport systems (ITS) and is also known as the DSRC band. The IEEE 802.11p standard provides high-speed, low-latency, and reliable communication for V2V and V2I applications, such as collision avoidance, traffic management, and road safety.

Further, in the network layer the Ad hoc On-demand Distance Vector (AODV) routing protocol was used. It is a reactive protocol that establishes a route on-demand when a node wants to communicate with a destination node that is not within its direct transmission range. AODV uses sequence numbers to prevent routing loops and to ensure the freshness of the route information. When a node needs to send a packet to a destination for which it does not have a route, it broadcasts a route request (RREQ) message. Nodes receiving the RREQ message forward it to their neighbors unless they have a valid route to the destination. If the RREQ message reaches the destination or a node with a valid route to the destination, a route reply (RREP) message is sent back to the source node. The source node caches the route for future use and starts transmitting data packets to the destination.

In the transport layer User Datagram Protocol (UDP) was used. UDP is a transport layer protocol used for sending data over the network. It provides a connectionless communication service that does not guarantee the reliable delivery of packets, nor does it establish a connection before sending data. UDP is often used in situations where speed and low overhead are more important than reliability and error correction such as in the case of IoV.

Finally, ZAMA protocol was implemented in the application layer. Different application classes where made for RSU, TA and VUs and functions for initialization, receiving and sending packets where modified from basic UDP application templates that already existed in OMNET++.

4 Results

This protocol can be analysed in regards to security through a mathematical security analysis against the security goals formulated in [10]. Time measured when simulating the protocol and a computational and communication overhead analysis can be used to measure efficiency. This section provides insights on the results obtained on this regard. The security analysis only involves explanations of proofs for security guarantees obtained from the original ZAMA paper rather than new proofs obtained by us.

4.1 Security analysis

The goal of the authors in the paper [10] was to prove that the protocol fulfilled user anonymity, mutual authentication, user linkability, traceability, forward security and replay attack resistance. In the following we will explain the security proofs from [10] to understand the security guarantees of the protocol.

Mutual Authentication necessitates that legitimate parties are able to confirm each other's identities while preventing an attacker from successfully posing as an authorized AS/VU during authentication.

The proof for Mutual Authentication shows that in the ZAMA protocol, if the probability is negligibly low for legitimate parties to generate each other's private key, an attacker cannot successfully impersonate a legal party due to the infeasibility of computing certain parameters based on the Strong RSA Assumption and the Elliptic Curve Discrete Logarithm Problem (ECDLP). (The Strong RSA Assumption is an assumption that there is no efficient algorithm to find integers e and u that satisfy $z = u^e \pmod n$ for $z \in Z_n$. The ECDLP is a problem in which, given a point Q on an elliptic curve over a finite field and a generator point P, it is difficult to find the integer i such that $Q = iP$.) Specifically, the commitment scheme ensures that the VU cannot commit to two equal values x_1 and x_2 without having to reveal the value itself $E(x, r)$. This means that the secret parameters x, r_1, r_2 cannot be obtained by the attacker unless they can factor n or solve the logarithms in the commitment. Similarly, based on ECDLP it is infeasible for AS to generate the private key k_H based on any information they have.

User Anonymity refers to the property or condition of a protocol where the identity of a user or participant cannot be revealed or inferred, even by unauthorized access to information or compromise of the system.

The proof shows that in ZAMA, user anonymity is guaranteed because the commitments $E = g_1^x h_1^{r_1}$ and $F = g_2^x h_2^{r_2}$ generated by TA during the authentication phase reveal nothing to AS and the proof computed by VU during the mutual authentication phase can be authenticated by AS without revealing the real identity of VU, even if the wireless channel is observed or the AS is compromised.

Replay attack resistance is the property of a security scheme to prevent attackers from re-sending previously intercepted messages in an attempt to gain unauthorized access or privileges.

The proof involves two cases that must be satisfied for an attacker to replay a message: either the current random number and the replayed random number must be equal or the hash values of the current and replayed messages must be equal. However, since the random number selected by the AS is selected from a wide range of data, the probability of the current and replayed random number being equal can be neglected. Similarly, the hash function used in ZAMA is considered to be collision-resistant, making it impossible for the attacker to generate the same hash value without the current random number.

Forward security is a property that ensures that even if an attacker obtains the secret keys or other sensitive information used in the current communication session, they cannot use this information to compromise the security of previous sessions.

The proof mentions that ZAMA uses random numbers, such as N_d, r_1, and r_2, only once for each session and varied for each session, making it difficult for an attacker to obtain their previous values. As a result, an attacker cannot obtain any previous information, and ZAMA satisfies the forward security property.

Unlinkability is a property of a security protocol or system that ensures that the real identity of a user cannot be inferred or linked to their actions or transactions within the system.

ZAMA maintains unlinkability by using fresh and different anonymous identity credentials for each access such as the differing random values used in the calculation of the proof each time. This ensures that the anonymous identity credential for each access is unique and cannot be linked to a real user identity, even if an attacker intercepts messages over a long period of time.

Tracebability is the property that allows a trusted third party to reveal the real identity of a misbehaving or malicious user when necessary, while keeping the anonymity of the other users intact.

During the authentication phase, TA can use the secret key xi_1, xi_2 to calculate K_i, which can be used to query the database and reveal the true identity of VU. The xi_1, xi_2 used for revealing user identities are only known by TA, ensuring that VU can only be traced by TA. Since the attacker lacks xi_1, xi_2, even if they obtain T_1, T_2, T_3, K_n, they cannot correctly calculate K_i, making ZAMA traceable.

Overall, the security proofs from [10] are all stringent and therefore ZAMA fulfills all its security goals.

4.2 Computational and communication overhead analysis

The computation of the ZAMA protocol involves mostly modular exponentiations and other modular arithmetics, hashing, one ECC based encryption and decryption and one symmetric encryption decryption process.

For the registration process the biggest computational costs involve the generation of two big primes, the generation of elliptic curve parameters and modular exponentiations to generate the commitments. The generation of the two big primes involves a probabilistic primality test like the Miller-Rabin test for example, to generate a 256-bit prime using the Miller-Rabin test, it typically requires around 50 iterations. The time required for each iteration is relatively small compared to the cost of generating elliptic curve parameters or performing scalar multiplications on points on an elliptic curve, but the total time required can still be significant for very large primes. Further, generating the elliptic curve parameters is a time costly operation but it must only be done once, thus it does not have to be considered. The generation of a public and private key for each AS, takes about one scalar multiplication operation for each key pair. The modular exponentiations, some modular inverse calculations and other modular arithmetics are also involved in the registration process, however, in the literature, mostly only the ECC based arithmetic operations such as scalar multiplication and point addition, as well as hash function operations are considered for the computational overhead analysis because they are the most time consuming. A table of typical costs can be found in Table 2. These are execution times of cryptographic operations obtained using the MIRACL library on an Intel I7-4770 processor running on Windows 7 from [4].

In the authentication process the biggest computational cost is the ECC based encryption and decryption process and some hashing. Considering the Elliptic Curve Integrated Encryption Scheme (ECIES) for this, this would typically involve two scalar multiplications and one hashing process in the encryption process and one scalar multiplication and one hash operation in the decryption process. Adding this up, we have 3 scalar multiplications, 2 hashing operations, plus two other separate hashing operations in the authentication process. This makes the authentication process computational cost approximately:

$$\begin{aligned} &2T_h + 2T_{e,m} + T_h + T_{e,m} + T_h \\ &= 4T_h + 3T_{e,m} = 4 * 0.0001ms + 3 * 0.442ms \\ &= 1.33ms \end{aligned} \tag{25}$$

The fast reconnection costs are similar because it also involves ECC encryption and decryption, which is the most costly process. The only difference is that the proof does not have to be recomputed saving some time.

Further, the communication cost in bytes of the protocol can be considered in terms of n, since most integers in the protocol are calculated modular n. Considering n to be approximately of the size 2^{256}, we can assume all integers in the group Z_n to be approx. 32 bytes. Then, in the registration process the communication overhead is 16 bytes for the first transferal of VID from VU to TA, approx. $6 * 32 = 192$ bytes for communication back from TA to VU and approx.

TABLE 2: EXECUTION TIME OF CRYPTOGRAPHIC OPERATIONS

Symbol	Description	Time (ms)
$T_{e,m}$	Scalar multiplication operation $a*P$ in ECC, with $P \in G, a \in Z_q^*$	$0.442\ ms$
$T_{e,a}$	Point addition operation $P+Q$ in ECC, with $P, Q \in G$	$0.0018\ ms$
T_h	General hash function operation $h_k : 0,1^* \rightarrow 0,1^l$	$0.0001\ ms$

$2 * 32$ bytes from TA to AS. This makes the registration communication overhead approx. 272 bytes.

Moreover, the communication overhead in the authentication process involves the sending of the first nonce from AS to VU (approx. 32 bytes), the encrypted message containing the ZKP from VU to AS (approx. $8 * 32 = 256$ bytes), the message from AS to TA including T_1, T_2, T_3 (approx. 96 bytes), the success or failure message from TA to AS (approx. 4 bytes), and the final encrypted success or failure message from AS to VU (approx. 32 bytes). We could however, discount the communication from TA to AS, since this is described to be a wired secure channel that should not cause much overhead in practice. Then, the communication overhead of the authentication process is approximately 320 bytes.

Similarly adding up the communication bytes for the fast reconnection process, we get that its overhead is approximately 224 bytes. With one less communication step, since the first nonce does not need to be sent from the AS and a few less bytes to send from VU to AS because the ZKP does not need to be sent to the AS.

4.3 Practical analysis by simulation

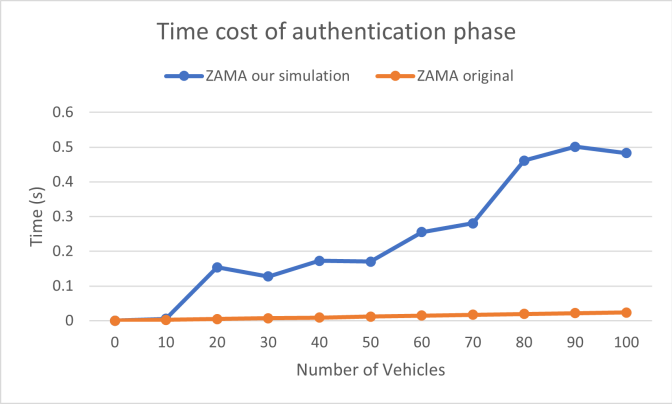


Fig. 7: Time cost of authentication by simulation

In our simulation the time cost of authentication for one vehicle was approximately 3.4 ms. For 10 VUs, in the original papar [10] the authentication time was approximately around 3 ms and in our simulation it was approximately 5 ms. For 10 vehicles the authentication time difference between the original paper and our simulation was still not that big as can be seen in Fig. 7, however, for simulations of more than 10 vehicles the authentication time jumps very high.

5 Evaluation

5.1 Comparison of analysis results to original ZAMA paper

As could be seen in the results section in Fig. 7, it is quite clear that the graph produced by our simulation is very different from the graph in the original paper. The following paragraphs discuss the reason for this difference and the validity of our results and consequence for the feasibility of the protocol.

In our simulation, we used a different map and different vehicular movements compared to the original paper. The original paper's setup was a smaller area around one roundabout, whereas we used a larger map size of 2500m*2500m to simulate 100 VUs wanting to authenticate at the same time. To account for this, we set the power of the radio transmitter to be strong enough to transmit signals across the entire map area, which caused a lot of interference. This is an important additional factor when evaluating the performance of an authentication protocol since many vehicles may want to communicate at the same time, leading to signal interference and blockage of each other's signal transmission. In our setup there were many outliers in the authentication time, where some VUs took over a minute for authentication which can be attributed to this interference phenomenon. These outliers were also the reason, why the average authentication time was so big for authenticating more than 20 VUs. However, since these do not have anything to do with the specific authentication protocol time, one could assume similar results for other authentication protocols. The only factor that would then make a big difference is the rounds of communication required until authentication. It is possible that the original paper did not account for this interference or mitigated its influence with a special setup. Additionally, the higher transmission power used in our simulation to be able to cover a larger area may have increased the interference factor. Although we set the minimum interference power to -80 dBM, the interference factor was still significant, affecting the performance of the authentication protocol.

Another factor that may have affected the performance of the authentication protocol is the time span for authentication used for the graph. The original paper did not specify the time span used for authentication, and it is unclear if they only considered compute time or accounted for other factors, such as the time taken for nodes to start communicating, pass messages in the network, communication interruptions, or incorrectly transmitted messages. Various routing protocols may also affect the time until communication can be started and the handling of transmission interruptions. These factors can significantly affect the authentication protocol's performance, and their impact should be considered when evaluating the protocol's efficiency and effectiveness.

Considering that typical RSUs have a communication area of around 500-1000m, a 2500m*2500m transmission area for a single RSU may seem relatively large. But, to realize the Internet of Vehicles (IoV), a network of RSUs must be built, and the cost of infrastructure is an important factor to consider. The number of RSUs required per kilometer of the road network significantly affects the infrastructure cost.

Furthermore, if the density of RSUs is too large in a network the number of times a VU must authenticate also increases, since authentication must happen before connecting to each RSU. Conversely, RSUs computing capacities are often limited including memory, processing power and storage capacity. However, with the fast development in computing capacity and the development of the EC, it seems feasible to suggest that the RSU will have higher capacity to handle complex computational tasks and a higher performance to deal with lots of processing requests in a small time interval.

Thus, the simulation's main result is that while the computational efficiency of the authentication protocol is important and should be under a certain threshold, there are many other factors that affect the protocol's performance, including RSU communication areas and resulting interference, interference from other IoT devices and infrastructure and routing protocols considering the whole new IoT infrastructure. This is why it is important to first figure out the whole network infrastructure before an authentication protocol is considered.

5.2 Overall evaluation of ZAMA

In terms of threshold of efficiency, the three most important factors are the computational overhead, the communication overhead in bytes and the communication overhead in terms of rounds required between nodes before successful authentication. For the computational overhead we have determined in the results section that the protocol costs approximately 1.33 ms authentication time and 2 rounds of communication are needed between VU and RSU during authentication. First, VU requests authentication, then AS sends a nonce, then VU sends the proof and AS sends either a success or failure message. Further, approximately 320 bytes must be sent during this process. Considering the categories in [5] this computational cost is considered very low. However, the communication cost of 320 bytes is considered very high. The fast reconnection method brings down the communication cost by 1/3 and the computation cost due to not having to compute another ZKP. Thus, considering that the protocol uses only a minimal number of communication rounds between AS and VU, overall the ZAMA protocol can be considered very efficient.

When it comes to authentication protocols, security promises are the most important consideration once a certain efficiency threshold has been met. In the case of ZAMA, our security analysis in the results section has shown that it fulfills all security and anonymity requirements that were set as goals in [10], including mutual authentication, user anonymity, replay attack resistance, forward security, unlinkability, and traceability.

Through these security properties ZAMA provides protection against a range of attacks. For example, attacks on authentication and identification, such as sybil attacks, can be prevented due to the protocol's unlinkability property. Sybil attacks involve an attacker impersonating multiple identities to increase their influence in the network. However, with unlinkability, even if an attacker's identity is revealed, it cannot be linked to their previous or future communication sessions.

Similarly, masquerading, which involves an attacker impersonating a legitimate vehicle, can be prevented by the traceability property of ZAMA. This property enables the protocol to trace the source of malicious actions, making it easier to identify and prevent future attacks. Node impersonation can also be prevented through unlinkability and traceability.

ZAMA also provides strong security against attacks on confidentiality, such as eavesdropping and location tracking. The protocol's user anonymity property ensures that the identity of the communicating parties is not revealed to third parties, thus preventing eavesdropping. Additionally, unlinkability ensures that even if the identity of one party is revealed, it cannot be linked to their previous or future communication sessions, thus preventing location tracking. Furthermore, attacks on privacy that reveal identity can also be mitigated through the user anonymity and unlinkability properties.

Non-repudiation, which refers to the ability to prevent a user from denying that they have sent or received a message, is achieved through the traceability provided by the TA. Finally, attacks on data trust, such as sending affected messages or manipulating sensors, can be traced in ZAMA to help identify the source of malicious actions, which can aid in preventing future attacks.

Nevertheless, some attacks such as on availability might not have been considered for, but could possibly be dealt with in the practical implementation. One example of an availability attack is spamming and DoS. To mitigate these attacks, practical implementations such as rate limiting, session limits, or IP blocking can be utilized. To implement these kind of schemes some pseudo identity is needed to determine how many times the same identity has requested authentication. However, in ZAMA due to unlinkability the AS cannot determine where requests come from and therefore to implement these schemes, check requests would have to be sent to the TA. Yet, due to the structure of the protocol, denial of authentication requests would only be able to be sent in the last authentication success/failure message. This is after most of the authentication process has already ended, thus not being a successful method for the prevention of attacks on access. However, an option would be to implement spam reducing methods in other layers of the OSI model.

Overall, ZAMA with its security properties is a strongly anonymous and secure protocol which only has some small weaknesses in the area of availability attacks.

6 Conclusion

This paper analyzes the feasibility of an efficient anonymous mutual authentication system called ZAMA. The protocol is evaluated through a security analysis, a computational and communication overhead analysis and a simulation. The results show that the protocol is efficient in terms of computational cost but has a high communication cost in bytes. Additionally, the proposed fast reconnection procedure, based on the security context from the last access, can reduce the computation overhead effectively. The protocol also offers security features such as mutual authentication, user anonymity, replay attack resistance, forward security, unlinkability, and traceability. It is found to be effective

in preventing attacks such as sybil attacks, masquerading, node impersonation, eavesdropping, location tracking, attacks on privacy, non-repudiation, and attacks on data trust due to these security features. However, attacks on availability such as spamming and DoS attacks are not explicitly considered. Overall, ZAMA is a strongly anonymous and secure protocol with minor weaknesses in availability attacks, thus becoming a very feasible option for VANET communication.

The issue of privacy in location-based information (LBI) has been a significant problem in the context of the IoV. Despite frequent pseudonym changes, route tracking could still be revealed through clever timing attacks [5]. This vulnerability has been addressed by ZAMA through the concept of unlinkability, which ensures that pseudonyms used at different points in time cannot be linked to the same vehicle. However, this feature also introduces the possibility of availability attacks, which could undermine the performance of the protocol. Therefore, there is a need for further research to find practical solutions that prevent these attacks while preserving the privacy of LBI. If successful, ZAMA could become a feasible protocol not just for the IoV, but for the broader Internet of Moving Things. Furthermore, it would be interesting to explore how ZAMA could be adapted for other types of networks, such as Vehicle to Everything (V2X) or the Internet of Drones. For instance, implementing ZAMA in a V2X network could provide secure and private communication between vehicles and other infrastructure, such as traffic lights or road signs, which would increase safety and efficiency in traffic management. Similarly, applying ZAMA to the Internet of Drones could improve the privacy and security of location-based information and enable more efficient drone traffic management.

As the IoV becomes more prominent, researchers have started to investigate the practical setup of this technology. One area that requires attention is the deployment of RSUs as part of the infrastructure. Research needs to be conducted to determine the optimal transmission range of these RSUs and the computing capabilities required to support them. This would involve studying the realistic infrastructure costs of deploying these units on a large scale. Furthermore, as more devices become connected to the IoV and more V2X connections are established, there is a need to reevaluate routing protocols. Previous routing protocols suffered from limitations in terms of routing overheads, computational complexity, and scalability [5]. With an ever-expanding network, scalability and routing overheads need to be carefully studied to ensure that the routing protocol can handle the increased traffic. In addition, interference issues need to be analyzed and practical solutions provided to ensure the timely delivery of critical information.

Tesla's vision-based approach to autonomous driving is an interesting development that could have a significant impact on the future of vehicular driving [38]. Computer vision has been a rapidly developing field, and the widespread adoption of these techniques in vehicles can be seen as a promising step towards fully autonomous vehicles. However, the question remains as to whether the benefits of vehicle connectivity are significant enough to justify the investment required for a large-scale infrastructure change project. Researchers could explore the advantages and disadvantages of a pure vision-based approach without interconnectivity of vehicles, and compare it to the benefits of added connectivity in terms of safety, traffic efficiency, and overall cost-effectiveness. A pure vision-based approach to autonomous driving may not be suitable for all driving scenarios, such as in adverse weather conditions, where V2V communication and data sharing could improve overall safety. Thus, there is a need for comprehensive research and analysis to determine the optimal level of connectivity required for different driving scenarios. Moreover, it is important to note that connectivity, while bringing benefits to traffic safety, can also be a cause for many attacks to the vehicular network that we have not seen in vehicles before. Therefore, further research must be conducted on other security features in vehicular connectivity to mitigate these risks.

REFERENCES

[1] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804517301455

[2] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for internet of things realization," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 2961–2991, 2018.

[3] A. A. Rasheed, R. N. Mahapatra, and F. G. Hamza-Lup, "Adaptive group-based zero knowledge proof-authentication protocol in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 2, pp. 867–881, 2020.

[4] J. Zhang, H. Zhong, J. Cui, Y. Xu, and L. Liu, "An extensible and effective anonymous batch authentication scheme for smart vehicular networks," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3462–3473, 2020.

[5] I. Ali, A. Hassan, and F. Li, "Authentication and privacy schemes for vehicular ad hoc networks (vanets): A survey," *Vehicular Communications*, vol. 16, pp. 45–61, 2019.

[6] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Edge computing in vanets-an efficient and privacy-preserving cooperative downloading scheme," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[7] A. Quyoom, A. Mir, and A. Sarwar, "Security attacks and challenges of vanets : A literature survey," *Journal of Multimedia Information System*, vol. 7, pp. 45–54, 03 2020.

[8] A. Wasef and X. Shen, "Efficient group signature scheme supporting batch verification for securing vehicular networks," in *2010 IEEE International Conference on Communications*, 2010, pp. 1–5.

[9] P. Vijayakumar, V. Chang, L. Jegatha Deborah, B. Balusamy, and P. Shynu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," *Future Gener. Comput. Syst.*, vol. 78, no. P3, p. 943–955, jan 2018. [Online]. Available: https://doi.org/10.1016/j.future.2016.11.024

[10] N. Xi, W. Li, L. Jing, and J. Ma, "Zama: A zkp-based anonymous mutual authentication scheme for the iov," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22 903–22 913, 2022.

[11] A. Albalawi, A. Almrshed, A. Badhib, and S. Alshehri, "A survey on authentication techniques for the internet of things," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, 2019, pp. 1–5.

[12] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology — CRYPTO 2001*, J. Kilian, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 213–229.

[13] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology – CRYPTO 2004*, M. Franklin, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 41–55.

[14] A. Menezes, "An introduction to pairing-based cryptography," 2005.

[15] A. Davenport and S. Shetty, "Comparative analysis of elliptic curve and lattice based cryptography," in *2021 Annual Modeling and Simulation Conference (ANNSIM)*, 2021, pp. 1–9.

[16] X. Salleras and V. Daza, "Zpie: Zero-knowledge proofs in embedded systems," *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 1382, 2021.

[17] "What are zk-snarks?" Jun 2022. [Online]. Available: https://z.cash/technology/zksnarks/

[18] A. K. Malhi, S. Batra, and H. S. Pannu, "Security of vehicular ad-hoc networks: A comprehensive survey," *Computers Security*, vol. 89, p. 101664, 2020.

[19] T. Shah and S. Venkatesan, "Authentication of iot device and iot server using secure vaults," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018, pp. 819–824.

[20] K. Lounis and M. Zulkernine, "Lessons learned: Analysis of puf-based authentication protocols for iot," *Digital Threats*, feb 2022, just Accepted. [Online]. Available: https://doi.org/10.1145/3487060

[21] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf, "Pseudonym systems," in *Selected Areas in Cryptography*, H. Heys and C. Adams, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 184–199.

[22] X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacy-preserving authentication based on group signature for vanets," in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 4609–4614.

[23] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for vanets," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 3, pp. 1711–1720, 2016.

[24] L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B. Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," *IEEE Transactions on Computers*, vol. 65, no. 8, pp. 2562–2574, 2016.

[25] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in vanet," in *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, ser. VANET '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 19–28. [Online]. Available: https://doi.org/10.1145/1287748.1287752

[26] F. Wang, Y. Xu, H. Zhang, Y. Zhang, and L. Zhu, "2flip: A two-factor lightweight privacy-preserving authentication scheme for vanet," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 2, pp. 896–911, 2016.

[27] N. K. Chistousov, I. A. Kalmykov, D. V. Dukhovnyj, M. I. Kalmykov, and A. A. Olenev, "Adaptive authentication protocol based on zero-knowledge proof," *Algorithms*, vol. 15, no. 2, p. 50, 2022.

[28] G. Fuchsbauer, C. Hanser, and D. Slamanig, "Structure-preserving signatures on equivalence classes and constant-size anonymous credentials," *J. Cryptol.*, vol. 32, no. 2, p. 498–546, apr 2019. [Online]. Available: https://doi.org/10.1007/s00145-018-9281-4

[29] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[30] E. Fujisaki and T. Okamoto, "Statistical zero knowledge protocols to prove modular polynomial relations," in *Advances in Cryptology — CRYPTO '97*, B. S. Kaliski, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 16–30.

[31] "Security parameter," Jun 2021. [Online]. Available: https://en.wikipedia.org/wiki/Security_parameter

[32] M. Carpenter and poncho, "Number generation for fujisaki-okamoto commitment scheme parameters," Sep 2015. [Online]. Available: https://crypto.stackexchange.com/questions/29370/number-generation-for-fujisaki-okamoto-commitment-scheme-parameters

[33] "Omnet++ 5.6 released," Jan 2020. [Online]. Available: https://omnetpp.org/software/2020/01/13/omnet-5-6-released

[34] C. Sommer. [Online]. Available: https://veins.car2x.org/

[35] "Inet framework." [Online]. Available: https://inet.omnetpp.org/

[36] P. A. Lopez, E. Wiessner, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flotterod, R. Hilbrich, L. Lucken, J. Rummel, P. Wagner, and et al., "Microscopic traffic simulation using sumo," *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018.

[37] J. Skiles, "Chaotictoejam/vanetproject: Solutions for vanet communication with omnet++," May 2020. [Online]. Available: https://github.com/chaotictoejam/VANETProject

[38] B. Dickson, "Tesla ai chief explains why self-driving cars don't need lidar," Jun 2021. [Online]. Available: https://bdtechtalks.com/2021/06/28/tesla-computer-vision-autonomous-driving/