IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

ROBUST KEY MANAGEMENT AND SECURE DATA TRANSFER SCHEME FOR VANET

KRISHNA KOMARAM[1], NAGARJUNA KARYEMSETTY[2]

[1]Reasearch Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, Andhra Pradesh, India.
[2]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, Andhra Pradesh, India.

ABSTRACT

Vehicular ad hoc network (VANET) networks play a vital role in vehicles control systems. VANET is commonly used network among the vehicles in a centralized way. The intricate web weaved within this network enables seamless communication with the vehicles it encompasses, yet unveils vulnerability to the lurking threats of cyber intrusions. Consequently, effective solutions are required to secure vehicles infrastructure as cyber-attacks on VANET systems can have severe financial and/or safety implications. In addition, the field devices in VANET possess microcontrollers dedicated to information processing, constrained by limited computational power and resources, posing challenges in implementing advanced security measures. Within the realm of this scholarly work, we present a pioneering stratagem encompassing a multi-tiered framework, ingeniously amalgamating symmetric and asymmetric key cryptographic methods. This innovative approach guarantees unparalleled attributes such as steadfast availability, unwavering integrity, impervious confidentiality, infallible authentication, and remarkable scalability. Additionally, we introduce an optimally streamlined session key management mechanism, skillfully blending the realms of random number generation with the efficacy of a hashed message authentication code. Furthermore, within the context of each session, we have innovatively incorporated three distinctive techniques of symmetric key cryptography, drawing inspiration from the timeless principles of the Vernam cipher. These techniques harmoniously coexist with a pre-shared session key, giving rise to an amalgamation of unparalleled security measures. One such technique involves the ingenious utilization of a random prime number generator, further enhancing the robustness of our cryptographic framework, prime counter, and hash chaining. The proposed scheme satisfies the Vehicular ad hoc network (VANET) has been considered as one of the most prominent technologies for improving the efficiency and safety of modern transportation systems. Nevertheless, the realm of VANET unravels a distinctive tapestry woven with a myriad of challenges and prospects that lie in wait for the domain of security. In particular, key management, requirements of real-time request response mechanism by supporting broadcast, multicast, and point to point communication.

1.INTRODUCTION

Enthralled by its captivating and auspicious capabilities such as vehicular safety, traffic congestion avoidance, and location-based services, the realm of Vehicular Ad Hoc Networks (VANET) has garnered immense popularity among networking enthusiasts. In this paper we mainly focus on overcoming the various problem defined in distributed key management framework and how to overcome the problems by adopting a separate management framework known as shared key management frame. The Road side unit measure road conditions at several position on the surface. At the core of VANET architecture, lies the noble pursuit of enhancing safety on the roads, evading traffic congestion, and providing location-based services. A crucial aspect involves vehicles generating warning messages, disseminated throughout a specific geographic zone, utilizing the potential of wireless multi-hop communication. The architecture encompasses an intricate interplay of sub-MTUs, diverse communication links (ranging from satellite, radio, and microwave links to cellular networks, switched or lease lines, and powerlines), as well as geographically dispersed field control devices, notably the ingenious Programmable Logic Controllers (PLCs) and remote entities. "An assemblage of RTUs, known as Terminal Units, coupled with IEDs (Intelligent Electronic Devices), form a powerful networked

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 2, 2024

infrastructure." The block diagram of a typical VANET system is depicted.

To ensure incessant supervision and regulation of the machinery present on the plant floor, an intricate system relies upon the utilization of sensors and actuators. These devices meticulously measure various attributes and relay the acquired information to field devices. Additionally, field control entities like PLCs, RTUs, and IEDs play a crucial role by providing digital status updates to the MTU, typically situated in a remote location, thereby enabling the determination of acceptable ranges as per predetermined criteria to parameters set in the server. This information will then be transmitted back to the field control device(s) where actions may be taken to optimize the performance of the system.Furthermore, the valuable status information finds its sanctuary within a meticulously curated database, seamlessly synchronized with a Human Machine Interface (HMI) stationed at the control center. This strategic placement empowers operators to engage in meaningful interactions with the intricacies of the plant's operations, navigating through a wealth of visualized data and real-time updates. floor machinery for centralized monitoring and system control. Large VANET networks such as those on a power plant require hundreds of field devices and dedicated subsystems to reduce the load on the centralized server.

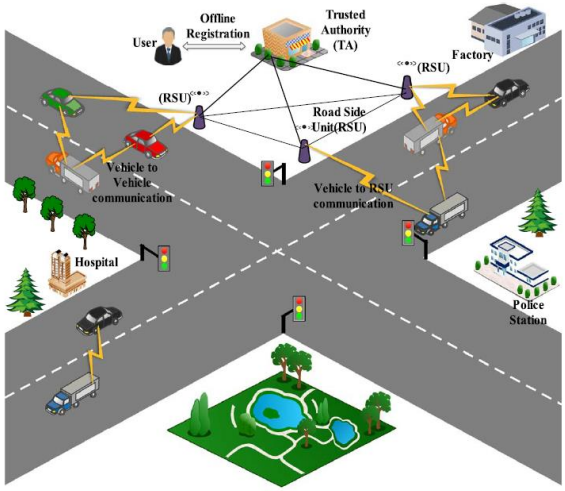

Fig. 1: Block diagram of a VANET system.

VANET communication messages have sensitive information as they are used to monitor and control the plant floor devices. For example, in water and sewage systems, the communication messages are used to raise and lower water tank levels or open and close the safety valves. Since these control devices are operated and monitored remotely, they can make them high-value targets for attackers to launch various cyber-attacks that can compromise the control systems, communication, and emergency services. Consequently, one of the critical aspects of the VANET systems is secure transmission of messages so that they cannot be tampered during the communication. Moreover, the VANET devices must be authenticated and maintain confidentiality of the information during the transmission so that no interceptor can misuse the system.

In the last few years, many key management techniques have been published to secure VANET communication, namely, VANET key establishment (SKE), VANET Key Management Architecture (SKMA), Advanced VANET Key Management Architecture (ASKMA), Hybrid Key Management Architecture (HKMA) and Advanced Hybrid VANET Key Management Architecture (AHSKMA), Limited Self-Healing key distribution (LiSH) [7], [8], [9], [10], [11], [12]. Within the realm of these techniques, they elegantly align themselves into two principal categories, encapsulating the essence of centralized key management and decentralized key management schemes. Furthermore, traversing the intricacies of each distinct category, we find an amalgamation of three distinct approaches employed for the generation and extraction of the session key. These approaches elegantly encompass the realms of symmetric cryptography, asymmetric cryptography, and a harmonious hybrid blending of the two. The drawback of the centralized scheme is that if the key distribution center (KDC) is down, the communication is cut off, which is not acceptable in VANET systems. In a decentralized approach, the keys are created using keying material and may only affect the single communication link in case of a breakdown. While the symmetric key based approach excels in terms of message integrity and high availability, it regrettably falls short in providing the crucial elements of authentication and confidentiality. On the other end, asymmetric key provides message integrity, authentication, and privacy, but may compromise availability. Hence, hybrid techniques are more suitable for VANET systems. The realm of key management has witnessed the emergence of several noteworthy techniques that venture beyond traditional boundaries, harnessing the power of hybrid methods. For example, Rezai et al. [10] Embarking on an innovative journey, we present a cutting-edge Hybrid Key Management Architecture (HSKMA) that builds upon and elevates the key management framework previously proposed by Choi et al. This advanced architecture promises to unlock new frontiers in efficient and secure key management, surpassing the boundaries of its predecessor[11]. However, Nevertheless, the mechanism at hand leverages the prowess of a

centralized Key Distribution Center (KDC) to proficiently disseminate the keys. Moreover, the communication between the MTU and the sub-MTU is established using Elliptic-Curve Cryptography (ECC) based asymmetric key cryptography while the sub-MTU and the RTU communicate using Rivest–Shamir–Adleman (RSA) asymmetric key cryptography. Employing a similar approach, we have augmented the scheme originally put forth by Rezai et al., infusing it with newfound enhancements and advancements. [13] using a decentralized system in [9]. Within this intricate scheme, a harmonious synergy unfolds as the master keys undergo refreshing through the utilization of Elliptic Curve Cryptography (ECC), while symmetric cryptography takes center stage for encryption, decryption, and the crucial task of session key updates. However, this scheme does not validate the message integrity and authentication. Furthermore, the intriguing facet lies in the absence of practical implementation evidence for any of the preceding methods, substantiating their capability to bestow immunity against the perils of quantum attacks[14]. Furthermore, it has been known that RSA does not guarantee perfect forward secrecy [11]. To encapsulate the essence, a comprehensive analysis reveals that none of the techniques encompass all the facets pertaining to security.

The forgoing discussion brings in the need for an effective cryptography solution that will prevent these systems from potential breaches. The objective of this paper is to propose a robust & low-cost security framework for automated industries to mitigate various security flaws and cyber-attacks. The proposed work aims to offer a multi-layered security framework for vehicles infrastructures by combining both symmetric and asymmetric key cryptography techniques. Reembracing an innovative paradigm, this groundbreaking approach unveils a meticulously crafted layered architecture. Within this framework, seamless communication thrives as the MTU and sub-MTU intricately engage in a hybrid technique, fostering uninterrupted exchanges throughout the entirety of a session. Simultaneously, the sub-MTU establishes a harmonious line of communication with the RTU, forging a cohesive and dynamic network fabric.using symmetric key cryptography once the session key is securely exchanged. Moreover, within the realm of our research, we have boldly put forth a groundbreaking proposition, introducing a unique methodology to generate symmetric keys by harnessing the unparalleled prowess of the Vernam cipher. Departing from conventional methods such as 3DES, AES, and others, this novel approach promises to unlock new dimensions in cryptographic endeavors. Furthermore, the proposed scheme satisfies VANET requirements of real-time request-response mechanism by supporting broadcast, multicast, and point-to-point communication.

A. Contributions of the Paper

1) We propose a secure session-key agreement scheme according to VANET protocol standards to ensure the security amongst MTU, sub-MTUs and RTUs. To achieve this objective, an ingenious approach is employed, utilizing a true random number generator that draws inspiration from both the current date and time (CDT) and a fractional representation of the square root of a prime number (FSRP) generate the session key. Moreover, these elements are shared by XORing them to enhance the privacy of the shared secrets.Furthermore, the dynamic HMAC undergoes derivation by harnessing the intrinsic value encapsulated within the Fraction Square Root of Prime (FSRP). Moreover, using these same elements, the HMAC is derived to validate the integrity of the message.The remarkable reusability of these elements serves as a catalyst, amplifying the computational speed for deriving the session key, symmetric key, and HMAC, igniting a profound acceleration in cryptographic operations. The inherent randomness exhibited by both the key and HMAC fortifies their resilience against a diverse range of attacks, including but not limited to correlation attacks and length extension attacks.,etc.

2)Innovatively, we put forth a pioneering approach to generate symmetric keys within the realm of the Vernam cipher, cleverly amalgamating the prime counter and hash chaining techniques. Our methodology draws upon the remarkable mathematical property of the Fraction Square Root of Prime (FSRP), a non-terminating, non-repeating irrational number. Building upon the recent work by Manjunatha et al. [15], who proposed the utilization of Vulgar fractions for the Vernam cipher, we enhance the process by enabling a secure seed exchange. This intricate fraction is derived through the division of a small number by a large prime number, yielding an extended sequence of digits [15]. For instance, the fraction frac(1/7) = 0.1428571428571 presents a remarkable pattern of repetitive digits, generating long and complex key strings. However, our proposed approach advances that method by generating completely random and non-repeating decimal numbers using the concept of FSRP. For example frac(sqrt (7)) = 0.64575131106459059050161 returns long strings without repetitive sequence of digits.

3) We propose a multi-layered framework by integrating the concept of symmetric and asymmetric key cryptography that ensures various security mechanisms, namely, authentication, confidentiality, message integrity, avail-ability, and scalability for VANET systems. The proposed method for symmetric key cryptography is based on the Vernam cipher, which provides protection against all the cryptographic attacks while the NTRU based post-quantum public-key algorithm resists quantum and data harvest attacks.

4) We identify an efficient cipher suite by comparing and analyzing various private and public key algorithms for the proposed framework by considering multiple fac-tors, namely, prevention mechanism against classical and quantum attacks, key storage cost, the random-ness of key and computational speed. The proposed cipher suite overcomes the weaknesses of the cipher suite offered by the American Gas Association (AGA) security standards [14], [16].

B. Outline of the Paper

The subsequent sections of this paper are structured in the following manner. Section II describes related research in the areas of key management and encryption schemes foe VANET systems. Section III, presents the reasoning of choice of the algorithms. The proposed multi-layered framework for secure VANET communication is introduced in Section IV, which covers secure key and information exchange. Section V presents the complete experimental setup which includes algorithm selection for cipher suites, computational speed of proposed framework, random-ness evaluation of symmetric key, and calculation of the cost of the keys. Section VI presents the comparative studies with the state-of-the-art techniques in terms of security analysis, storage cost, and execution speed. Section VII concludes the paper.

2. RELATED WORK

VANET networks are typically configured using proprietary protocols such as Modbus, IEC 61850, IEC 60870, DNP3, and Profinet, which do not support secure data communication. Furthermore, exemplifying the susceptibility that ensued, the Blaster worm [2] showcased the application of open link communication in the remote procedure call (RPC) context. Furthermore, many network sniffing tools are freely available to view and gather the network traffic [17]. Therefore, secure data trans-mission is one of the important requirements for VANET systems. Key management and encryption play a vital role in securing VANET communication. Typically, in a VANET communication, the MTU sends control signals to the RTUs to control the plant floor devices, which require three types of communication, namely, broadcast, multicast, and point to point. However, controller RTUs may need to operate other field RTUs.When confronted with an emergency shutdown scenario, MTUs employ a broadcasting mechanism to disseminate clock information or achieve synchronization across various control devices, including RTUs, IEDs, and PLCs.To operate a specific substation device, the MTU requires multicast communication, whereas monitoring and controlling the plant for machinery typically requires point-to-point communication. Therefore, while designing a secure framework for VANET networks, it is crucial to cover all three types of communication.

Over the past two decades, a multitude of key management schemes have been introduced, categorically divided into centralized key distribution schemes ([4], [7], [18], [19]) and decentralized key distribution schemes ([9], [20], [21], [22]).Within the centralized scheme, a pivotal role is assumed by the Key Distribution Center (KDC) in generating and disseminating secret keys, which in turn facilitate the establishment of secure communication among involved parties. Conversely, the decentralized scheme necessitates the utilization of pre-shared keying material to construct the session key.Once the session key is derived using keying essence, further communication takes place using that key.Moreover, certain key management schemes employ the technique of public key-based methodology to establish a secure mode of transmission. Despite being associated with significant time and power consumption, multiple research studies indicate that ECC (Elliptic Curve Cryptography) is a viable choice for a public-key cryptosystem, as evidenced by findings in [4], [9], and [11].

To satisfy the availability requirement, Hybrid Key Management Architecture (HKMA) and Advanced Hybrid VANET Key Management Architecture (AHSKMA) were proposed [10], but there is a chance that field devices will stop working during the replacement of field control devices. To solve this issue, Choi et al. propose a hybrid key management scheme [11]. A centralized key distribution (CKD) protocol is applied between the sub-MTU and MTU, and LKH protocol is applied between sub-MTU and RTU. Nevertheless, it falls short in terms of offering high availability.

Numerous authentication techniques are documented in the literature for VANETs, with Johnson et al. contributing to a selection of these existing methods. [12] propose Limited Self-Healing key distribution (LiSH), which offers revocation capabilities along with

collusion-resistance for group communication in VANET systems.

The hybrid Diffie-Key exchange, along with the authentication scheme, was proposed in [26]. This scheme uses RSA and AES for session key generation and encryption.Despite this, it lacks the capability to ensure high availability.

The literature offers numerous established techniques for authentication in VANETs, with Johnson et al. contributing to the array of available methods. [8] proposed an Elliptic Curve Digital Signature Algorithm (ECDSA), which is mathematically derived from the basic digital signature algorithm. ECDSA uses an asymmetric key pair which consists of a public key and a private key.For user authentication, this technique utilizes a public key derived from a random multiple of the base point, where the multiples are generated based on the private key. In this context, both the public and private keys are employed.This method incorporates two distinct attacking techniques: targeting the Elliptic Curve Discrete Logarithmic Problem (ECDLP) and exploiting vulnerabilities in the hash function. Wasef et al.Introducing the Efficient Certificate Management Scheme for Vehicular Ad Hoc Networks (ECMV), a novel approach was put forth for digital certificate management. The foundation of this approach lies in the utilization of a Public Key Infrastructure (PKI) system.This method is based on a Public Key Infrastructure (PKI). In this technique, each vehicle has a short lifetime certificate and this certificate can be updated from any RSU. To maintain privacy-preserving authentication, this certificate undergoes regular updates, leading to an accompanying increase in overhead. Shen et al. Proposing the Cooperative Message Authentication Protocol (CMAP), a comprehensive solution was presented to identify and mitigate the dissemination of malicious information originating from vehicles within the road transport system.. The cooperative message authentication is a promising technique to alleviate vehicle's computation over-head for message verification.Nonetheless, as the vehicle density rises, this approach experiences an escalation in communication overhead. Its primary limitation lies in the absence of a verifier to authenticate messages, thereby allowing malicious messages to potentially be accepted by vehicle users.

S. Biswas, J. Misic, and V. Misic [68]. Introducing a novel safety message authentication scheme tailored for vehicular ad hoc networks, we leverage an ID-based signature and verification mechanism. By employing an ID-based approach, we eliminate the need for certificates in public key verification, while the utilization of proxy signatures enhances the flexibility of message authentication and trust management. Within this scheme, we integrate an ID-based proxy signature framework with the standard ECDSA to authenticate safety application messages originating from road-side units (RSUs) in VANETs. We also implement specialized handling of signed message forwarding to ensure the trustworthiness and authentication of RSU's application messages. We confidently assert that this scheme demonstrates resilience against major security threats while exhibiting computational efficiency in terms of complexity. Vehicular Ad hoc Networks (VANETs) promise us a way of safe driving with the help of a variety of potential applications mainly for road safety, traffic management, vehicle maintenance and driver assistance.

S. Busanelli, G. Ferrari, and L. Veltri [69], Vehicular Ad-hoc NETworks (VANETs) are witnessing an ever increasing interest.Ensuring security is of paramount importance to facilitate the successful implementation of commercial deployments, as the presence of malicious attacks can amplify the risk of accidents. Key management within VANETs presents additional challenges due to limited connectivity and potential difficulties in establishing communication with a central certification authority. In this manuscript, we put forth an innovative strategy for key management that aims to safeguard VANET communications. Specifically, we introduce a comprehensive framework designed for key group multicast, tailored to address the unique requirements of VANET communication. scenario. Nowadays, most of the vehicles available on the market possess sensorial, cognitive, and communication skills. In particular, leveraging on Inter-Vehicular Communications (IVCs)—a set of technologies that provides vehicles with networking capabilities-vehicles can create decentralized and self-organized vehicular networks, commonly denoted as Vehicular Ad-hoc NETworks (VANETs). VANETs may involve the use of either network interfaces mounted on the vehicles,

typically denoted as On-Board Units (OBUs), and/or fixed network nodes, usually referred as Road Side Units(RSUs).

A. Dhamgaye and N. Chavhan [70]. The rapid progress in Wireless Communication within Vehicular Adhoc Networks (VANETs) has created an emerging platform that captivates the attention of both industrialists and researchers. Vehicular admonitors are multi hop networks with no fixed infrastructure. Vehicular Ad Hoc Networks (VANETs) consist of mobile vehicles engaged in communication with each other, presenting a key challenge in efficiently routing data from source to destination. Designing an effective routing protocol for VANETs is a complex undertaking, further compounded by the vulnerability to various attacks due to the wireless medium. Given that these attacks can disrupt network operations, ensuring security becomes imperative for the successful deployment of such technology. This survey paper provides a concise overview of different routing protocols, while also highlighting the significant security issues and challenges associated with each protocol.

In their research, Huang et al. [71]Presented is an innovative scheme referred to as the anonymous batch authenticated and key agreement (ABAKA) protocol. This scheme aims to authenticate multiple requests originating from different vehicles and concurrently establish distinct session keys for each vehicle. In VANETs, where vehicle speeds range from 10 to 40 m/s (36-144 km/h), the necessity for such a scheme is evident.

Incorporating efficient authentication measures is an essential requirement in Vehicular Adhoc Networks (VANETs). In comparison to existing key agreement schemes, the proposed anonymous batch authenticated and key agreement (ABAKA) scheme excels in efficiently authenticating multiple requests through a single verification operation. Furthermore, ABAKA successfully negotiates a session key with each vehicle via a single broadcast message. To minimize verification delays and transmission overhead, elliptic curve cryptography is implemented. The foundation of ABAKA's security lies in its reliance on the unsolved NP-complete problem known as the elliptic curve discrete logarithm problem.. To address potential invalid request issues that could hinder batch verification, a detection algorithm has been devised. Extensive performance evaluations of ABAKA demonstrate its efficiency benefits, encompassing verification delay, transmission overhead, and cost for rebatch verifications. Simulation results reveal that ABAKA outperforms the existing elliptic curve digital signature algorithm (ECDSA)-based scheme, exhibiting lower message delay and message loss rate.

Expanding on the importance of intervehicular communication, Mershad and Artail [72] emphasize its central role in numerous industry and academic endeavors dedicated to improving the safety and efficiency of transportation systems. Vehicular ad hoc M. Raya and J. Hubaux [73] introduce an intelligent transport system within ad hoc networks, focusing on the exchange of road condition information among vehicles, and between vehicles and the road infrastructure. The security of the vehicular ad-hoc network (VANET) in the road condition information transferring system plays a critical role in ensuring the system's normal operation and efficient information transfer. Taking into account the inherent characteristics of ad hoc networks, this paper addresses VANET security concerns and proposes appropriate measures within the integrated intelligent transport system.

In their work, Y. Hao, Y. Cheng, C. Zhou, and W. In the pursuit of fortifying privacy within Vehicular Ad Hoc Networks (VANETs), a pioneering framework by Song [74] emerges, incorporating a distributed key management system founded on group signature. Unlike existing group signature schemes that rely on centralized key management, their framework enables distributed key management, facilitating the revocation of malicious vehicles, system maintenance, and accommodating heterogeneous security policies. In this framework, each road side unit (RSU) assumes the role of a key distributor for seamless key management within the VANET. To address the challenges posed by semi-trust road side units (RSUs) within the group, we have devised security protocols that aim to detect compromised RSUs and colluding malicious vehicles. Additionally, we have tackled the issue of high computation overhead resulting from the implementation of group signatures. To alleviate the verification burden, we propose a practical cooperative message authentication protocol that reduces the number of messages each vehicle needs to verify. We

In their research, Huang et al. [71]Presented is an innovative scheme referred to as the anonymous batch authenticated and key agreement (ABAKA) protocol. This scheme aims to authenticate multiple requests originating from different vehicles and concurrently establish distinct session keys for each vehicle. In VANETs, where vehicle speeds range from 10 to 40

m/s (36-144 km/h), the necessity for such a scheme is evident.
Incorporating efficient authentication measures is an essential requirement in Vehicular Adhoc Networks (VANETs). In comparison to existing key agreement schemes, the proposed anonymous batch authenticated and key agreement (ABAKA) scheme excels in efficiently authenticating multiple requests through a delve into the details of potential attacks and provide corresponding solutions. Moreover, we have developed an analytical model for the medium access control (MAC) layer and conducted NS2 simulations to evaluate the key distribution delay and the missed detection ratio of malicious messages. Our proposed key management framework is implemented in 802.11 based VANETs.

In their study, W. Shen, L. Liu, and X. Cao [75] emphasize the complex nature of vehicular ad hoc networks, which constitute a intricate cyber-physical system with interconnected physical and cyber domains. Within the physical domain, vehicles regularly broadcast their geographic information, leading to a significant increase in data traffic, particularly in densely populated areas. To address this challenge, the authors focus on mitigating the substantial computation overhead associated with safety message authentication. They propose a cooperative message authentication protocol (CMAP) that aims to reduce the computation burden on individual vehicles. Through CMAP, vehicles collaboratively share the responsibility of authenticating safety messages, optimizing the overall computational efficiencyTo enhance computational efficiency, vehicles in our proposed approach verify their safety message results cooperatively, significantly reducing the number of messages that each vehicle needs to verify individually. Additionally, we investigate verifier selection algorithms to achieve a high detection rate of invalid messages within a realistic 2-D road scenario. Within the realm of this paper, another noteworthy achievement manifests in the creation of a novel analytical model encompassing not only our Cooperative Message Authentication Protocol (CMAP), but also the prevailing probabilistic verification protocol, all while diligently considering the various intricacies involved. account the impact of hidden terminals. Through simulations conducted on a practical map, we present performance results that showcase the effectiveness of our CMAP in comparison to the existing method.
In their work, J. A. M. Naranjo, J. A. L. Ramos, and L. G. Casado [76] explore the practical applications of the Extended Euclidean algorithm in the context of security and privacy. They present three specific applications that leverage the algorithm's capabilities. Firstly, they propose a solution for privately distributing a secret to multiple recipients using a single multicast communication. This application is particularly useful for rekeying purposes in Secure Multicast scenarios. Secondly, they introduce an authentication mechanism suitable for environments lacking a public-key infrastructure. Lastly, they demonstrate how the Extended Euclidean algorithm can be utilized to achieve a zero-knowledge proof, reducing the number of messages exchanged between the involved parties, while incorporating a central server for assistance.
In their study, P. Vijayakumar, S. Bose, and A. Kannan [77] address the challenge of designing a key distribution protocol with minimal computation and storage complexity in secure multimedia multicast scenarios. They propose a new Key Distribution Protocol based on the Greatest Common Divisor (GCD), focusing on two key dimensions. Firstly, their protocol aims to reduce computation complexity by minimizing the number of multiplication operations during key updation through the use of the Karatsuba divide and conquer approach. Secondly, they target the reduction of stored information in the Group Center and group members during key content updates. The proposed algorithm is implemented and tested using a Cluster tree based key management scheme, demonstrating promising results. The paper includes a comparative analysis of various key distribution protocols, showcasing the significant reduction in computation and storage complexity achieved by the proposed algorithm.

In a related context, N. V. Vighnesh, N. Kavita, R. Shalini, and S. Sampalli [78] focus on the security aspects of Vehicular ad hoc networks (VANETs) considering the increasing challenges of safe driving and the demand for on-the-move infotainment services. The paper introduces a novel sender authentication scheme that leverages hash chaining, a well-known cryptographic concept, for authenticating vehicles. The authentication process takes place at an Authentication Centre, facilitated by the Road Side Units (RSUs) that assist in relaying information between vehicles and the Authentication Centre. The paper provides a detailed discussion of the scheme and presents a security analysis to evaluate its effectiveness.
L. Veltri, S. Cirani, S. Busanelli [79], and G. Ferrari delve into the diverse communication paradigms of ad hoc networks, including point-to-multipoint (multicast) and multipoint-to-point scenarios. To ensure secure communication in such scenarios, they propose a novel centralized approach that efficiently distributes and

manages a group key, referred to as the "group key," among multiple communication endpoints in generic ad hoc networks and the Internet of Things (IoT). The aim is to minimize computational overhead and network traffic resulting from changes in group membership due to user joins and leaves. The proposed protocol leverages two leave strategies: (i) a predetermined time selected during user group entry and (ii) an unpredictable time, such as membership revocation. The effectiveness of the proposed protocol is demonstrated through its application in two relevant scenarios: (i) secure data aggregation in the IoT and (ii) Vehicle-to-Vehicle (V2V) communications in Vehicular Ad hoc Networks (VANETs).

S. Busanelli, G. Ferrari, and L. Veltri [80] highlight the growing interest in Vehicular Ad-hoc NETworks (VANETs). Recognizing the importance of security in enabling commercial deployments and mitigating the risk of accidents caused by malicious attacks, they address the challenges of key management in VANETs. Given the limited connectivity and potential difficulties in communicating with a central certification authority, they propose a novel approach to key management that ensures secure VANET communications. Their proposal introduces a comprehensive framework for key group multicast, specifically tailored to VANET communication scenarios.

In their research, X. Lv, H. Li, and B. Wang [81] emphasize the significance of self-organizing group key agreement protocols in ensuring secure group communication within dynamic peer systems, without the need for a centralized administrator.In response to this particular necessity, a groundbreaking solution is introduced by them, presenting an inventive single-round self-organizing group key agreement protocol derived from the principles of the Chinese Remainder Theorem. In their approach, each group member contributes their individual public key to facilitate the negotiation of a shared encryption key, enabling decryption with unique decryption keys. Utilizing their respective secret keys, all group members can decrypt any ciphertext encrypted using the shared encryption key. To demonstrate the feasibility of their proposal, they instantiate a one-round self-organizing group key agreement protocol using the efficient and computationally inexpensive NTRU public key cryptosystem. Importantly, both the public key and the message in their protocol remain secure against known lattice attacks. Additionally, they provide a brief description of another concrete scheme based on the ElGamal public key cryptosystem, leveraging their generic idea.

3.CONCLUSION AND FUTURE ENHANCEMENT

In our study, we have introduced a novel dual authentication scheme aimed at enhancing the security of vehicles engaged in communication within the VANET environment. To achieve dual-mode authentication, we have employed two components: the hash code and fingerprint of each vehicle user involved in the communication. By integrating the fingerprint authentication technique with the hash code creation method, we effectively prevent malicious users from illicitly accessing the secret key of any VANET user and participating in VANET communication. Additionally, to counteract malicious users attempting to spoof authentication codes assigned to VANET users and sending erroneous messages to other vehicles, we have devised a new dual key management scheme. This scheme, implemented in our research, ensures computational efficiency and facilitates secure data transmission from Trusted Authorities (TA) to Primary Users (PUs) and from PUs to Secondary Users (SUs) through the utilization of two distinct group keys—one for PUs and another for SUs. Furthermore, our proposed algorithm incorporates the use of single broadcast messages from the TA to notify group members and facilitate the recovery of updated group keys. As part of future developments, we aim to explore new methodologies to safeguard the privacy of vehicle locations from potential intruders.

REFERENCES

[1] D. Upadhyay, S. Sampalli and B. Plourde, "Vulnerabilities' assessment and mitigation strategies for the small linux server Onion Omega2", Electronics, vol. 9, no. 6, pp. 967, 2020.

[2] D. Upadhyay and S. Sampalli, "VANET (supervisory control and data acquisition) systems: Vulnerability assessment and security recommendations", Comput. Security, vol. 89, Feb. 2020.

[3] Y. Cherdantseva et al., "A review of cyber security risk assessment methods for VANET systems", Comput. Security, vol. 56, pp. 1-27, Feb. 2016.

[4] Rezai, P. Keshavarzi and Z. Moravej, "Key management issue in VANET networks: A review", Int. J. Eng. Sci. Technol., vol. 20, no. 1, pp. 354-363, 2017.

[5] F. M. Salem, E. Ibrahim and O. Elghandour, "A lightweight authenticated key establishment scheme for secure smart grid communications", Int. J. Safety Security Eng., vol. 10, no. 4, pp. 549-558, 2020.

[6] D. Upadhyay, J. Manero, M. Zaman and S. Sampalli, "Gradient boosting feature selection with machine learning classifiers for intrusion detection on power grids", IEEE Trans. Netw. Service Manag., vol. 18, no. 1, pp. 1104-1116, Mar. 2021.

[7] D. Choi, S. Lee, D. Won and S. Kim, "Efficient secure group communications for VANET", IEEE Trans. Power Del., vol. 25, no. 2, pp. 714-722, Apr. 2010.
[8] T. C. Pramod and N. R. Sunitha, "Polynomial based scheme for secure VANET operations", Procedia Technol., vol. 21, pp. 474-481, Nov. 2015.
[9] Rezai, P. Keshavarzi and Z. Moravej, "Secure VANET communication by using a modified key management scheme", ISA Trans., vol. 52, no. 4, pp. 517-524, 2013.
[10] Rezai, P. Keshavarzi and Z. Moravej, "Advance hybrid key management architecture for VANET network security", Security Commun. Netw., vol. 9, no. 17, pp. 4358-4368, 2016.
[11] D. Choi, H. Jeong, D. Won and S. Kim, "Hybrid key management architecture for robust VANET systems", J. Inf. Sci. Eng., vol. 29, no. 2, pp. 281-298, 2013.
[12] R. Jiang, R. Lu, C. Lai, J. Luo and X. Shen, "Robust group key management with revocation and collusion resistance for VANET in smart grid", Proc. IEEE Global Commun. Conf. (GLOBECOM), pp. 802-807, 2013.
[13] Rezai, P. Keshavarzi and Z. Moravej, "A new key management scheme for VANET networks", Proc. 2nd Int. Symp. Comput. Sci. Eng., pp. 373-378, 2011.
[14] S. Ghosh and S. Sampalli, "A survey of security in VANET networks: Current issues and future challenges", IEEE Access, vol. 7, pp. 135812-135831, 2019.
[15] V. Manjunatha, A. Rao and A. Khan, "Complex key generation with secured seed exchange for vernam cipher in security applications", Mater. Today Proc., vol. 35, no. 3, pp. 497-500, 2021.
[16] R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa and S. Shenoi, "Security strategies for VANET networks", Proc. Int. Conf. Crit. Infrastruct. Protect., pp. 117-131, 2007.
[17] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh and B. Movali, "A lightweight key management protocol for secure communication in smart grids", Electr. Power Syst. Res., vol. 178, Jan. 2020.
[18] R. Dawson, C. Boyd, E. Dawson and J. M. G. Nieto, "SKMA—A key management architecture for VANET systems", Proc. 4th Aust. Symp. Grid Comput. e-Res. (AusGrid) 4th Aust. Inf. Security Workshop (Network Security) (AISW-NetSec), vol. 54, pp. 183-192, 2006.
[19] D. Choi, H. Kim, D. Won and S. Kim, "Advanced key-management architecture for secure VANET communications", IEEE Trans. Power Del., vol. 24, no. 3, pp. 1154-1163, Jul. 2009.
[20] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid", IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 375-381, Jun. 2011.
[21] D. J. Kang, J. J. Lee, B. H. Kim and D. Hur, "Proposal strategies of key management for data encryption in VANET network of electric power systems", Int. J. Electr. Power Energy Syst., vol. 33, no. 9, pp. 1521-1526, 2011.
[22] T. C. Pramod, G. S. Thejas, S. S. Iyengar and N. Sunitha, "CKMI: Comprehensive key management infrastructure design for vehicles automation and control systems", Future Internet, vol. 11, no. 6, pp. 126, 2019.
[23] T. M. D. Hadley and K. A. Huston, AGA-12 Part 2 Performance Test Results, Oct. 2020, [online] Available: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/9-AGA-12_Part_2_Performance.pdf.
[24] D. Abbasinezhad-Mood, A. Ostad-Sharif and M. Nikooghadam, "Novel anonymous key establishment protocol for isolated smart meters", IEEE Trans. Ind. Electron., vol. 67, no. 4, pp. 2844-2851, Apr. 2020.
[25] N. Saxena, B. J. Choi and R. Lu, "Authentication and authorization scheme for various user roles and devices in smart grid", IEEE Trans. Inf. Forensics Security, vol. 11, pp. 907-921, 2015.
[26] K. Mahmood, S. A. Chaudhry, H. Naqvi, T. Shon and H. F. Ahmad, "A lightweight message authentication scheme for smart grid communications in power sector", Comput. Electr. Eng., vol. 52, pp. 114-124, May 2016.
[27] M. Keshk, E. Sitnikova, N. Moustafa, J. Hu and I. Khalil, "An integrated framework for privacy-preserving based anomaly detection for cyber-physical systems", IEEE Trans. Sustain. Comput., vol. 6, no. 1, pp. 66-79, Jan.–Mar. 2021.
[28] J. Qian, C. Hua, X. Guan, T. Xin and L. Zhang, "A trusted-id referenced key scheme for securing VANET communication in iron and steel plants", IEEE Access, vol. 7, pp. 46947-46958, 2019.
[29] D. G. Brosas, A. M. Sison and R. P. Medina, "Modified OTP based Vernam Cipher algorithm using multilevel encryption method", Proc. IEEE Eurasia Conf. IOT Commun. Eng. (ECICE), pp. 201-204, 2019.
[30] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination", Proc. 7th Int. Symp. Resilient Control Syst. (ISRCS), pp. 1-8, Aug. 2014.
[31] R. Zazkis, "Representing numbers: Prime and irrational", Int. J. Math. Educ. Sci. Technol., vol. 36, no. 2, pp. 207-217, 2005.

[32] Blake (Hash Function), May 2021, [online] Available: https://en.wikipedia.org/wiki/BLAKE_(hash_function).
[33] Embedded TLS Library for Applications Devices IoT and the Cloud, Aug. 2020, [online] Available: https://www.wolfssl.com/download.
[34] The NTRU Project, Aug. 2020, [online] Available: https://tbuktu.github.io/ntru/.
[35] J.-P. Aumasson, S. Neves, Z. Wilcox-O'Hearn and C. Winnerlein, "BLAKE2: Simpler smaller fast as MD5", Proc. Int. Conf. Appl. Cryptogr. Netw. Security, pp. 119-135, 2013.
[36] J. O'Connor and J.-P. Aumasson, BLAKE2: Simpler Smaller Fast as MD5, Feb. 2021, [online] Available: https://www.blake2.net/blake2.pdf.
[37] J. O'Connor, S. Neves and Z. Winnerlein, Blake3—One Function Fast Everywhere, Feb. 2021, [online] Available: https://github.com/BLAKE3-team/BLAKE3-specs/raw/master/blake3.pdf.
[38] J. O'Connor, S. Neves and Z. Winnerlein, Blake3 is an Extremely Fast Parallel Cryptographic Hash, Feb. 2021, [online] Available: https:/www.infoq.com/news/2020/01/blake3-fast-crypto-hash/.
[39] H. Delfs, H. Knebl and H. Knebl, Introduction to Cryptography, New York, NY, USA:Springer, vol. 2, 2002.
[40] A. Kamal and A. M. Youssef, "An FPGA Implementation of the NTRU Encrypt cryptosystem", Proc. Int. Conf. Microelectron., pp. 209-212, 2009.
[41] J. Hermans, F. Vercauteren and B. Preneel, "Speed records for NTRU", Proc. Cryptogr. Track RSA Conf., pp. 73-88, 2010.
[42] J. N. Gaithuru and M. Bakhtiari, "Insight into the operation of NTRU and a comparative study of NTRU RSA and ECC public key cryptosystems", Proc. 8th. Malaysian Softw. Eng. Conf. (MySEC), pp. 273-278, 2014.
[43] D. Stehlé and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices", Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn., pp. 27-47, 2011.
[44] Jacomme and S. Kremer, "An extensive formal analysis of multi-factor authentication protocols", ACM Trans. Privacy Security, vol. 24, no. 2, pp. 1-34, 2021.
[45] N. Mouha and A. Hailane, "The application of formal methods to real-world cryptographic algorithms protocols and systems", Computer, vol. 54, no. 1, pp. 29-38, Jan. 2021.
[46] S. Szymoniak, "Security protocols analysis including various time parameters", Math. Biosci. Eng., vol. 18, no. 2, pp. 1136-1153, 2021.
[47] N. Dalal, J. Shah, K. Hisaria and D. Jinwala, "A comparative analysis of tools for verification of security protocols", Int. J. Commun. Netw. Syst. Sci., vol. 3, no. 10, pp. 779, 2010.
[48] H. Shinde, A. Umbarkar and N. Pillai, "Cryptographic protocols specification and verification tools-A survey", ICTACT J. Commun. Technol., vol. 8, no. 2, pp. 1533-1539, 2017.
[49] J. Cremers, "The scyther tool: Verification falsification and analysis of security protocols", Proc. Int. Conf. Comput. Aided Verification, pp. 414-418, 2008.
[50] X. Wang, D. Feng, X. Lai and H. Yu, "Collisions for hash functions MD4 MD5 HAVAL-128 and RIPEMD", 2004.
[51] M. Stevens, E. Bursztein, P. Karpman, A. Albertini and Y. Markov, "The first collision for full SHA-1", Proc. Annu. Int. Cryptol. Conf., pp. 570-596, 2017.
[52] Y. Sasaki, L. Wang and K. Aoki, "Preimage attacks on 41-step SHA-256 and 46-step SHA-512", 2009.
[53] A. Osvik, "Fast embedded software hashing", 2012.
[54] J. Vidali, P. Nose and E. Pašalić, "Collisions for variants of the BLAKE hash function", Inf. Process. Lett., vol. 110, no. 14, pp. 585-590, 2010.
[55] J. Daemen and G. Van Assche, "Producing collisions for PANAMA instantaneously", Proc. Int. Workshop Fast Softw. Encrypt., pp. 1-18, 2007.
[56] M. Coutinho, R. T. De Sousa and F. Borges, "Continuous diffusion analysis", IEEE Access, vol. 8, pp. 123735-123745, 2020.
[57] N. Abdoun, Design Implementation and Analysis of Keyed Hash Functions Based on Chaotic Maps and Neural Networks, 2019, [online] Available: https://hal.archives-ouvertes.fr/tel-02271074/document.
[58] N. Abdoun, S. E. Assad, T. M. Hoang, O. Deforges, R. Assaf and M. Khalil, "Designing two secure keyed hash functions based on sponge construction and the chaotic neural network", Entropy, vol. 22, no. 9, pp. 1012, 2020, [online] Available: https://www.mdpi.com/1099-4300/22/9/1012.
[59] S. Al-Kuwari, J. H. Davenport and R. J. Bradford, "Cryptographic hash functions: Recent design trends and security notions", 2011, [online] Available: https://eprint.iacr.org/2011/565.
[60] H. Feistel, "Cryptography and computer privacy", Sci. Amer., vol. 228, no. 5, pp. 15-23, 1973, [online] Available: http://www.jstor.org/stable/24923044.
[61] M. Stevens, "Attacks on hash functions and applications", 2012.
[62] H. Wang, Z. Ma and C. Ma, "An efficient quantum meet-in-the-middle attack against NTRU-2005", Chin. Sci. Bull., vol. 58, no. 28, pp. 3514-3518, 2013.

[63] S. N. Kumar, "Review on network security and cryptography", Int. Trans. Electr. Comput. Eng. Syst., vol. 3, no. 1, pp. 1-11, 2015.
[64] S. Biswas, J. Misic, and V. Misic, "ID-based Safety Message Authentication for Security and Trust in Vehicular Networks", Proc. of 31st Int'l Conf. on Distributed Computing Systems Workshops (ICDCSW), Minneapolis, Minnesota, June 2011.
[65] S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived Key Management for Secure Communications in VANETs", Proc. of ITST 2011, St. Petersburg, Russia, Aug. 2011.
[66] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET," Int. J. Comput. Sci., vol. 2, no. 1, pp. 88–96, 2013.
[67] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262, Jan. 2011.
[68] S. Biswas, J. Misic, and V. Misic, "ID-based Safety Message Authentication for Security and Trust in Vehicular Networks", Proc. of 31st Int'l Conf. on Distributed Computing Systems Workshops (ICDCSW), Minneapolis, Minnesota, June 2011.
[69] S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived Key Management for Secure Communications in VANETs", Proc. of ITST 2011, St. Petersburg, Russia, Aug. 2011.
[70] A. Dhamgaye and N. Chavhan, "Survey on security challenges in VANET," Int. J. Comput. Sci., vol. 2, no. 1, pp. 88–96, 2013.
[71] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262, Jan. 2011.
[72] K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular Ad Hoc networks," IEEE Trans. Veh. Technol., vol. 62, no. 2, pp. 536–551, Feb. 2013.
[73] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39–68, Jan. 2007.
[74] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 616–629, Mar. 2011.
[75] W. Shen, L. Liu, and X. Cao, "Cooperative message authentication in vehicular cyber-physical systems," IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, pp. 84–97, Jun. 2013.
[76] J. A. M. Naranjo, J. A. L. Ramos, and L. G. Casado, "A suite of algorithms for key distribution and authentication in centralized secure multicast environments," J. Comput. Appl. Math., vol. 236, no. 12, pp. 3042–3051, Jun. 2012.
[77] P. Vijayakumar, S. Bose, and A. Kannan, "Centralized key distribution protocol using the greatest common divisor method," Comput. Math. Appl., vol. 65, no. 9, pp. 1360–1368, May 2013.
[78] N. V. Vighnesh, N. Kavita, R. Shalini, and S. Sampalli, "A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks," in Proc. IEEE Symp. ISWTA, Langkawi, Malaysia, 2011, pp. 96–101.
[79] L. Veltri, S. Cirani, S. Busanelli, and G. Ferrari, "A novel batch based group key management protocol applied to the Internet of things," Ad Hoc Netw., vol. 11, no. 8, pp. 2724–2737, Nov. 2013.
[80] S. Busanelli, G. Ferrari, and L. Veltri, "Short-lived key management for secure communications in VANETs," in Proc. IEEE Int. Conf. ITST, St. Petersburg, Russia, 2011, pp. 613–618.
[81] X. Lv, H. Li, and B. Wang, "Group key agreement for secure group communication in dynamic peer systems," J. Parallel Distrib. Comput., vol. 72, no. 10, pp. 1195–1200, Oct. 2012.