A Lightweight Certificate Authorization and Revocation Scheme for Vehicular Ad-hoc Networks

Mashail Alhamidi*

Department of Computer Science, Tabuk, Saudi Arabia.

Mashailalhamidi@outlook.com

A Lightweight Certificate Authorization and Revocation Scheme for Vehicular Ad-hoc Networks

Abstract – Vehicular Ad-hoc Networks (VANETs) are fundamental to the evolving transportation landscape. VANETs are promoting both safety and efficiency. Ensuring the security and performance of VANETs is crucial, as they become deeply intertwined with daily travel. The researcher deeply explored the current certificate management schemes within VANETs. This research highlighted the key challenges and shortcomings associated with the current certificate management schemes from the literature. To keep a balance between robust security and optimal performance, the researcher proposed a lightweight approach that combines a dynamic Certificate Authority (CA) framework with RSA encryption. The proposed scheme was rigorously tested under three specific modes using the NS-2 simulator. The researcher leveraged metrics such as latency, jitter, and Packet Delivery Ratio (PDR) as performance benchmarks. The results indicate that the method delivers competitive performance on par with less secure settings, even with its advanced security features. This research sets the foundation for a more secure and efficient VANET paradigm and directed us towards a safer vehicular communication future.

Keywords: Vehicular Ad-hoc Networks, Performance, Security, Certificate Authority (CA)

1. INTRODUCTION

The recent integration of modern Information and Communication Technology (ICT) with transport infrastructure has led to the creation of Intelligent Transportation Systems (ITS). These systems use advanced technology to improve transportation's efficiency, safety, and security. Vehicular Ad Hoc Networks (VANETs) are one main part of ITS (Gautam, 2021). In VANETs, vehicles communicate with each other and with nearby structures, called Road Side Units (RSUs). This helps them share important information and supports different applications. In VANETs, vehicles act like moving parts of a wireless network. They create a quick network without needing any already set up system. These networks let vehicles tell each other about the road, traffic, accidents, and

other things. This helps in managing traffic, preventing crashes, and making the roads safer.

However, it is tough to make sure that VANETs have safe and dependable communication. This is because these networks keep changing, and they need strong safety tools. Traffic jams in cities have become a big issue due to the high density of the vehicles on roads. Apart from being annoying and wasting time, road accidents cost the world around $500 billion every year. What is perhaps more shocking is that over 1.35 million individuals are killed in vehicle accidents per year (Ptak, 2019). So, ITS use VANETs as a key part. Vehicles share road information through a wireless system in VANET to encourage careful driving. Therefore, safety and good performance are crucial for VANETs to work well.

A. *VANET's SECURITY*

Security is crucial in VANETs because vehicles are always communicating with each other. They keep sharing important details about where they're going, what they plan to do, and what's around them. This constant chat helps make transportation smarter. It helps reduce traffic jams and avoid potential road accidents. However, due to the wireless nature of communication between nodes in VANET, they are vulnerable to various cyber-attacks. Bad actors can pose risks like penetrating into the system or pretending to be another vehicle. This can mess up the real message and put both the car and the people inside at risk. Hence, having safe communication is not just a technical need; it's absolutely essential. We need strong ways to check messages, like the Certificate Assignment and Revocation Scheme. This helps make sure messages are real and come from safe places.

B. VANET's PERFORMANCE

Security is the base, but performance makes VANETs practical in real life. VANETs need to work fast because vehicles move quickly and conditions change all the time. Communication delays are not encouraged in VANETs. For instance, if a warning about a sudden stop from a car in front comes late, it can cause big crashes on the road. How the system processes information, how it stores data, and how it sends messages are as important as the message content itself. Old methods like Certificate Revocation Lists (CRLs) had problems. They become troublesome, i.e., make the system slower and use up more storage, when growing in volume. Ultimately, they affected the whole system's speed.

C. PROBLEM STATEMENT

Many security methods in VANETs use Certificate Revocation Lists (CRLs) (Khodaei, Mohammad, and Panos Papadimitratos, 2018) (Khan, Taimur, Naveed Ahmad, Yue Cao, Syed Asim Jalal, Muhammad Asif, Sana ul Haq, and Haitham Cruichshank, 2017). But this approach has problems. Even though CRLs are made to boost security, they can also be weak spots. Bad actors might target these lists because they have all the revoked certificates. If they get into these lists, they can create or copy valid certificates. This can result in fake or harmful communications within the VANET. As VANETs grow and get more complex, CRLs become bigger. Handling, changing, and checking these big lists needs a lot of computational power (Khan, Taimur, Naveed Ahmad, Yue Cao, Syed Asim Jalal, Muhammad Asif, Sana ul Haq, and Haitham Cruichshank, 2017). This can cost more and put pressure on the car's onboard systems.

Another issue associated with traditional CRLs-based certification schemes is that every time a vehicle needs to check the CRLs to communicate or confirm

something, it takes time (Azam, Farooque, Sunil Kumar Yadav, Neeraj Priyadarshi, Sanjeevikumar Padmanaban, and Ramesh C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," IEEE access , vol. 9, pp. 31309-31321, 2021, 2021). Even small delays are a big deal in VANETs, where every split-second counts. If it takes too long to check the CRLs, vehicles might make decisions late. This can be risky for safety.

D. PROPOSED SOLUTION

Given the problems with the usual Certificate Revocation Lists (CRLs) in VANETs, we proposed a new secure and reliable certificate assignment and revocation scheme. Instead of using a static list, this method uses a central certification authority that assigns and revokes certificates in real-time. When vehicles want to communicate with each other, they get special public and private key pairs just for that particular communication instance. When they're done communicating, the central certification authority revokes the keys. This way, we avoid the issues that come with traditional CRLs based approaches. Moreover, it saves computational resources and makes things faster. This means vehicles can quickly check if messages are safe. Moreover, it's safer because there's less chance for bad actors to misuse keys for a long time. And we don't have the risks that come with CRLs that don't change and can be hacked. In short, our new method is better than the old CRL ways, as it has the potential to make VANETs both safer and faster.

2. RELATED WORKS AND BACKGROUND

A. BACKGROUND

VANET is a particular kind of Mobile Ad-hoc Networks (MANETs). It is built

especially for vehicles to communicate to each other [5]. The way VANET is set up has three main parts:

- On-Board Units (OBUs) inside the vehicles.
- Road-Side Units (RSUs) positioned beside roadways.
- Central Authority (CA), which act as the main control centre.

Figure 1 shows the basic structure of VANET.

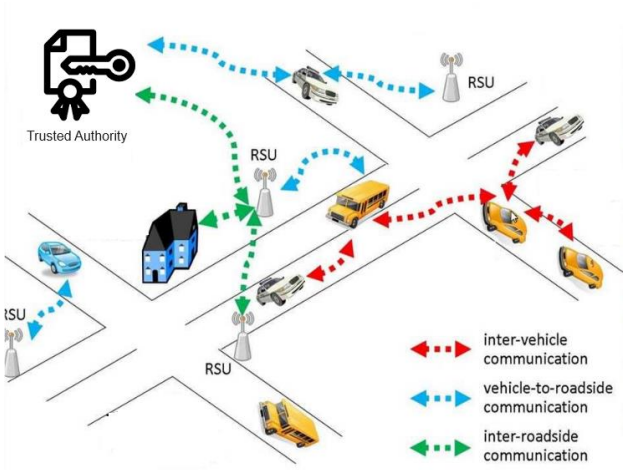

Figure 1 The Basic Architecture of VANETs.

Source: Adapted from public domain.

As shown in Figure 1, vehicles are the main parts of these networks having Onboard Units (OBUs) inside them. Every car has one OBU. These OBUs do two main things: they let vehicles communicate with each other, and they share a lot of details about the car, like how fast it is going, where it is, which way it is heading, and other data from sensors (Manvi, S. S., and M. S. Kakkasageri, 2008). Roadside Units (RSUs) are like signposts that are set up in key places, like crossroads, traffic lights, and rest areas. What do RSUs do? They help pass on information across the network and fill in gaps where vehicles can not communicate directly to each other. RSUs also give vehicles extra services, like internet, updates about traffic, and warnings about local

issues (Vegni, Anna Maria, Claudia Campolo, Antonella Molinaro, and Thomas DC Little, 2013).

Then there is the Centralized Trusted Authority (TA). It performs a lot of critical tasks in VANETs, such as assignment of security keys, registering vehicles, and making sure the whole network is safe (Abbas, Sohail, Manar Abu Talib, Afaf Ahmed, Faheem Khan, Shabir Ahmad, and Do-Hyeun Kim, 2021). In some VANET designs, TA also distribute and revoke certificates.

B. SECURITY CHALLENGES TO VANET

Based on the research (Mokhtar, Bassem, and Mohamed Azab, 2015) (Khan, Shawal, Ishita Sharma, Mazzamal Aslam, Muhammad Zahid Khan, and Shahzad Khan, 2021), VANETs face several big security issues:

- Vehicles move quickly, so it is tough to check if messages are from a real source. Fake messages can cause crashes or traffic jams. Plus, with vehicles always joining and leaving the network, checking the truth of so many messages become tricky.
- While we need to make sure messages are genuine, we also need to protect the privacy of drivers and passengers. It is hard to balance checking messages and not giving away too much information. Attackers could track where a car goes. Some solutions, like changing fake names regularly, can help, but they come with their problems.
- A bad actor might pretend to be many vehicles by using fake identities. This can feed the wrong information into the system, mess up traffic, or even cause accidents.

- Attackers can take old messages and send them again. For example, using an old "roadblock ahead" message can wrongly reroute traffic.
- Attackers can overload the network with useless or harmful data, making VANET services stop working. Since some VANET messages warn of crashes, blocking these can be very dangerous.
- Because VANETs use wireless communication, there is a risk attackers could listen in and pull-out private details from the messages.

C. PERFORMANCE CHALLENGES TO VANET

Based on studies (Al-Sultan, Saif, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan, 2014) (Sharma, Surbhi, and Baijnath Kaushik, 2019), the following is a list of the main challenges faced by VANETs:

- Vehicles in VANETs keep moving, which means the network setup changes a lot. This can break communication links, making us lose messages or not finish sending data.
- In cities, there can be thousands of vehicles communicating at once. The challenge is to make sure the VANET system can manage this without a drop in quality.
- With more and more vehicles trying to use the network, there is a chance of overcrowding the communication paths. This can slow down or even block messages, which is bad for services that need real-time information.
- Services that give quick alerts, like warnings about crashes, need super-fast communication. Making sure messages get sent and received quickly, especially when there are lots of vehicles around, is tough.

- Cities have lots of wireless devices. These can mess with the quality of VANET communication.
- The communication tools in vehicles, called OBUs, might not be super powerful. They could have less processing speed, storage, or battery life. So, it is a challenge to get good performance while keeping within these limits.
- Making VANETs safe is crucial, but safety measures can slow things down. The goal is to keep the system safe without making it too slow.

D. EXISTING CERTIFICATION SCHEMES

The VANETs domain has observed a variety of certificate schemes, as discussed by the authors in (Manvi, Sunilkumar S., and Shrikant Tangade, 2017). Each tailored to address the unique challenges posed by the dynamic nature of vehicular networks. While each scheme offers its own set of advantages, they also come with inherent challenges that researchers and practitioners need to consider.

PKI-based Schemes

In PKI-based schemes for VANETs, vehicles are provided with unique digital certificates issued by a centralized Certificate Authority (CA). These certificates, functioning like electronic passports, authenticate the messages circulated within the vehicular network. While PKI establishes a foundational layer of trust, challenges arise in VANETs due to the network's dynamic nature and concerns about vehicle tracking. To address privacy issues, vehicles can adopt pseudonymous certificates, allowing them to periodically change identities and prevent continuous tracking, while maintaining message authenticity.

Pseudonymous Certificate Systems

Pseudonymous certificate systems address the dual needs of authentication and privacy in VANETs. Vehicles are equipped with multiple digital certificates, rather than a single static one, all issued by a trusted Certificate Authority. Although these certificates are linked to the vehicle, they do not disclose its true identity. As a result, a vehicle can switch between its certificates periodically, appearing as different entities in the network and thwarting potential trackers. It is vital, however, that message authenticity remains uncompromised. Even if a receiving entity hasn't encountered a particular certificate before, it should validate the certificate's authenticity, trusting the underlying cryptographic assurances. This approach adeptly balances privacy and security in VANETs, shielding vehicles from continuous tracking while upholding communication integrity.

Identity-Based Cryptography (IBC)

Identity-Based Cryptography (IBC) revolutionizes traditional cryptographic systems by using an entity's unique identity, such as an email or vehicle license plate, as its public key. This technique eliminates the need for digital certificates. While PKI demands rigorous certificate management like issuance, storage, and revocation, IBC simplifies this process. Thus, it is especially beneficial for large networks like VANETs. However, the effectiveness of IBC hinges on the security of the Private Key Generator (PKG). PKG is a centralized component tasked with producing private keys based on identities. A breach of PKG endangers the network's safety, as malevolent actors could generate unauthorized private keys to harm the integrity of VANETs.

Regional-based Certificate Management Schemes

Regional-based certificate management divides VANETs into distinct geographical

areas, each with its local certificate authority (LCA) to handle digital certificate tasks within its territory. This localized approach offers benefits like improved scalability, efficient management, swift operations, region-specific revocations, and heightened privacy. However, it also introduces complexities. Vehicles transitioning between regions require inter-region LCA collaborations to validate existing credentials. Moreover, ensuring consistent security measures across LCAs and protecting them from threats are paramount challenges to address.

Decentralized Certificate Authority Schemes

Distributed ledger technologies like blockchain have ignited a shift from centralized to decentralized certificate authority structures in VANETs, aiming for heightened security and reliability. Traditional centralized CAs, though pivotal in many security systems, present a vulnerability as a single point of failure. In vast, dynamic environments like VANETs, this centralized weakness is particularly concerning. Decentralized Certificate Authority systems, underpinned by blockchain, distribute certificate management tasks across numerous network nodes. Through consensus mechanisms, certificates are collaboratively issued, renewed, and revoked, eliminating a singular point of failure. This decentralization offers increased security, transparency, immutability, trust automation, reduced overheads, and broader network participation. Nonetheless, challenges persist, including the computational demands of consensus algorithms, potential scalability concerns, and ensuring smooth inter-node communication. Table 1 presents the summary of existing certificate schemes in VANETs.

Table 1. Summary of existing Certification Schemes

Certificate Scheme	**Benefits**	**Challenges**
PKI-based	Established trust framework	Privacy concerns due to

Schemes	using secure asymmetric cryptography	potential vehicle tracking and certificate management overhead
Pseudonymous Certificate Systems	Offers balance between authentication and privacy. Moreover, prevents continuous tracking of vehicles	Need for frequent certificate switching. Faces complexity in certificate validation
Identity-based Certificate Schemes	Simplified certificate management via direct use of identity as public key	Reliance on the security of the PKG, which can be a single point of potential failure
Regional-based Certificate Management	Scalable, and offers efficient localized certificate management to reduced latency	Need for inter-region communication. Security standardization across LCAs
Decentralized Certificate Authority	Enhanced security and less overhead on central authority. Moreover, it offers transparency and immutability	Computational overhead of consensus algorithms. Scalability issues and complex inter-node communication

3. PROPOSED SCHEME

In the proposed secure VANET certification scheme, the communication process is divided into three phases: Start of Communication, Transmission of Messages, and End of Communication.

A. START OF COMMUNICATION

When a vehicle (node) decides to commence a secure communication, it reaches out to the Certificate Authority (CA). In response, the CA formulates a unique pair of encryption keys. The public key P_{key} is dispatched to the initiating vehicle for its use, while the private key P_{vkey} is securely retained by the CA itself.

B. TRANSMISSION OF MESSAGES

The sender vehicle encrypts its outgoing message using the public key in its possession to ensure that it is protected from any unintended recipients. This coded message then travels to its designated receiver. Upon its arrival, the receiver approaches the CA, presenting the sender's public key P_{key} as a token to request the matching private key. After verification of the public key and the receiver's identity, the CA grants the

corresponding private key P_{vkey} . This empowers the receiver to decrypt and access the original message, thereby achieving a secure information exchange. This flow can be summarized as:

- Sender uses the public key to encrypt its message and sends it onward.
- The receiver, upon intercepting this message, liaises with the CA, sharing the sender's public key, and seeks its matching private key.
- Following a successful validation, the CA releases the private key to the receiver.
- Equipped with this private key, the receiver can now decrypt the received message, ensuring its confidentiality remains intact.

C. END OF COMMUNICATION

It is vital that the utilized encryption keys be deactivated to prevent any subsequent misuse after the termination of communication. Thus, both vehicles relay a “session termination” alert to the CA. This signal cues the CA to invalidate and erase both the shared public and private keys. However, in situations where this termination alert may be impeded, the CA has a built-in fail-safe. It operates on a pre-set timer. If this countdown concludes without any sign-off from the nodes, the CA autonomously annuls the keys, thus ensuring the network's resilience even under unforeseen disruptions.

Given that:

$P_{key}, P_{vkey} = GenerateKeys()$function is used to generate the pair of public and private keys. The revocation of the keys will be done based on the threshold time as:

$$If\ Time_{current} - Time_{lastComm} > T_{threshold}, Revoke(P_{key}, P_{vkey})$$Where;

$Time_{current}$ and $Time_{lastComm}$ are the current time and the time when the communication performed between nodes using same keys, respectively.

Thus, the pseudo code of the suggested certificate authorization and revocation scheme is given as:

```
FUNCTION SECURECOMMUNICATION (SOURCE_NODE, DEST_NODE, MESSAGE):
    #Certificate Authority (CA) Functions
    Class CertificateAuthority:
        #Generate a pair of keys
        Function GenerateEncryptionKeys ():
            public_key, private_key = GenerateUniqueKeyPair ()
            StorePrivateKey(private_key)
            Return public_key
        #validate request and provide private key
        Function ProvidePrivateKey(requested_public_key):
            If IsValidRequest(requested_public_key):
                Return FetchStoredPrivateKey(requested_public_key)
            Return NULL
        #Revoke keys based on a session termination or timeout
        FUNCTION REVOKEKEYS ():
            RemoveStoredPrivateKey ()
            RemovePublicKey ()
    CA = CertificateAuthority ()
    #START OF COMMUNICATION
    Function InitiateCommunication():
        Return CA.GenerateEncryptionKeys ()
    #TRANSMISSION OF MESSAGES
    Function TransmitMessage (message, public_key):
        encrypted_message = Encrypt (message, public_key)
        source_node.Send(encrypted_message, dest_node)
        requested_private_key = dest_node.RequestPrivateKeyFromCA(public_key)
        If CA.IsValidRequest(requested_private_key):
            Return CA.ProvidePrivateKey(requested_private_key)
        Return NULL
    #END OF COMMUNICATION
    Function TerminateCommunication ():
        source_node.NotifySessionEnd ()
        dest_node.NotifySessionEnd ()
        CA.RevokeKeys ()
        Return TRUE
    #MAIN COMMUNICATION WORKFLOW
    public_key = InitiateCommunication ()
    private_key = TransmitMessage (message, public_key)
    If private_key:
        decrypted_message = Decrypt (encrypted_message, private_key)
        TerminateCommunication ()
        Return decrypted_message
    Return "Communication Error"
EndFunction
```

D. CRYPTOGRAPHIC SCHEME

We've implemented the RSA encryption algorithm in our proposed scheme. RSA a highly regarded public-key cryptosystem renowned for its strength and dependability. RSA forms the cornerstone of our cryptographic protocols, guaranteeing the confidentiality and integrity of messages exchanged within the VANET ecosystem. RSA provides formidable security measures by harnessing the mathematical complexities of large prime numbers to effectively safeguarding against potential attack vectors. This choice of encryption methodology aligns seamlessly with the dynamic and expansive nature of vehicular networks, ensuring robust protection in this challenging environment. Figure 2 highlights the encryption and decryption process using RSA.

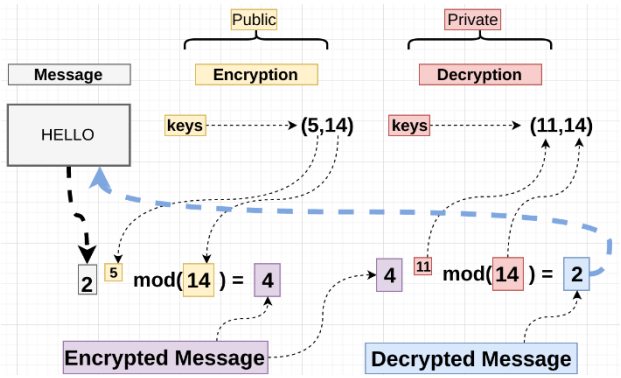

Figure 2. Encryption and Decryption process using RSA.
Source: Adapted from public domain.

4. SIMULATION AND TESTING

To comprehensively evaluate the impact of our proposed scheme on the performance of VANETs, we conducted simulations in three distinct environments, as described below:

A. NORMAL MODE SIMULATION

In this environment, we simulate the VANET without any encryption or Certificate Authority (CA) involvement. Vehicles communicate freely without encryption, similar to a non-secure VANET scenario. The purpose of this simulation is to establish a

baseline performance for VANET communication in an unsecured environment and allow us to quantify the improvements achieved by our proposed scheme.

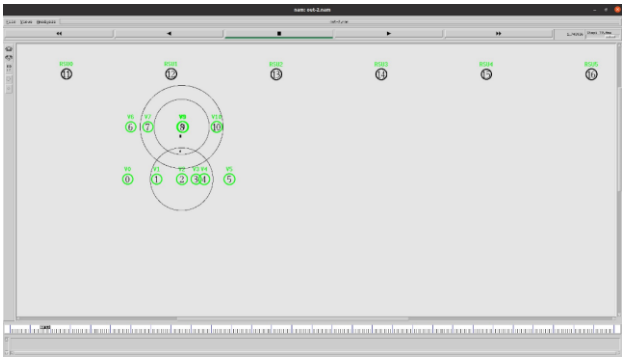

Figure 2. Simulation in Normal Mode (Without Encryption and CA Scheme)

B. SIMULATION WITH RSA ENCRYPTION WITHOUT PROPOSED CA SCHEME

In this environment, we introduce RSA encryption to the VANET but without the proposed Certificate Authority (CA) scheme. Vehicles use RSA encryption for secure communication, but key management and certificate issuance are not part of the system. This simulation helps us assess the impact of RSA encryption alone on VANET performance, considering its computational overhead and security enhancements.

Figure 3. Simulation with RSA Encryption without Proposed CA Scheme

C. SIMULATION WITH RSA AND THE PROPOSED CERTIFICATION SCHEME

This is the core environment where we implement both RSA encryption and our

proposed certification scheme, which includes the CA (as shown in Figure 5). Vehicles employ RSA encryption for secure communication, and the CA dynamically manages encryption keys and certificates. This simulation aims to evaluate the overall impact of our proposed scheme, considering its security benefits, computational efficiency, and overall performance enhancement.

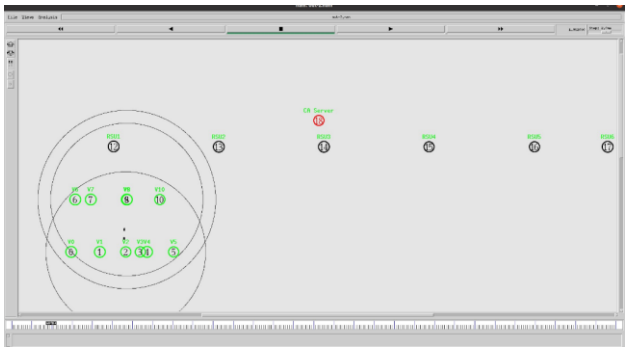

Figure 4. Simulation with RSA Encryption and Proposed CA Scheme

For fair analysis, we used the static parameters throughout all the simulation environments as given in Table 2 below.

Table 2. Network Parameters used in Simulations

VANET Parameter	Values
Time of Simulation	60 Seconds
Area of Simulation	1000 x 1000 Meters
Number of vehicles in VANET	10
Number of RSUs in VANET	7
Number of CAs	1
Packets Interval Time	0 01. 0.05, and 0.08 seconds
Vehicles Speed	20 Meter/Second
Packets Queue Length	50
Routing Protocol	Ad-Hoc On Demand

5. RESULTS AND ANALYSIS

In order to evaluate the impact of proposed CA scheme on VANETs performance, we choose key performance metrics such as, end to end delay, packet delivery ration and jitter. End-to-end delay is the time it takes for a data packet to travel from the sender node to the receiver node in a network and be successfully received and processed

(Singal, Gaurav, Vijay Laxmi, Vijay Rao, Swati Todi, and Manoj Singh Gaur, 2017). It measures the latency or delay in data transmission. End-to-end delay is a critical metric in VANETs because it directly affects the responsiveness of time-sensitive applications, such as collision warnings or traffic signal information. Lower end-to-end delay indicates faster communication and quicker responses, which are crucial for ensuring safety in vehicular networks. It is typically measured in Milliseconds (MS) and is calculated as the time elapsed between packet generation at the sender and successful reception and processing at the receiver.

As shown in Figure 6, the end-to-end delay with CA is slightly higher than the other two scenarios, and it can be justified because there is always a trade-off between security and performance. By considering the importance of security in VANETs, this little but extra latency is negotiable.

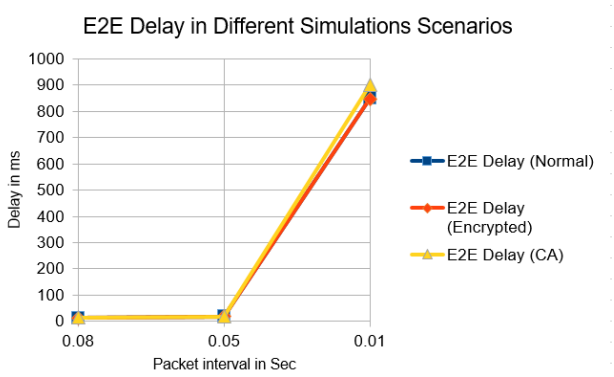

Figure 5. E2E Delay in Different Simulations Scenarios

Jitter refers to the variation in the delay of received packets in a network (Zheng, Li, Liren Zhang, and Dong Xu, 2001). It quantifies the irregularity in the timing of packet arrivals at the receiver. Jitter is essentially a measure of packet delay variability. Jitter can impact the quality of service in VANETs, especially for real-time applications. For example, in applications like voice communication or video streaming, consistent packet arrival times are critical to maintaining communication quality. As

shown in Figure 7, jitter was observed to be relatively higher in the simulation scenario where our proposed Certificate Authority (CA) scheme was implemented within the VANET. This is because the CA scheme introduces additional steps related to certificate issuance, validation, and revocation. While this increase in jitter may be notable, it is an acceptable trade-off considering the paramount importance of security in VANETs. The CA scheme's ability to enhance communication security and reliability outweighs the marginal variations in jitter.

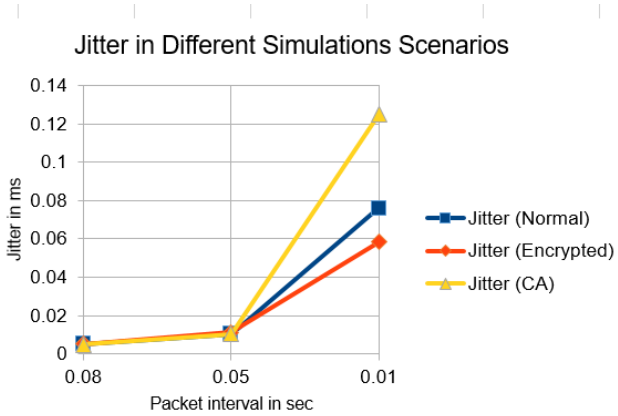

Figure 6. Jitter in Different Simulations Scenarios

Packet delivery ratio (PDR) is a metric that quantifies the percentage of data packets sent by the sender node that are successfully received by the intended receiver node (Wang, Jiliang, Yunhao Liu, Yuan He, Wei Dong, and Mo Li, 2013). It reflects the reliability and effectiveness of data transmission in the network. PDR is vital in VANETs because it directly relates to the reliability of communication. High PDR indicates that a significant portion of transmitted data reaches its destination, which is crucial for applications like traffic safety warnings and information dissemination. As depicted in Figure 8, the PDR is almost equal in all three simulation scenarios. A very small number of packets seemed to be dropped in the proposed CA scheme-based simulation scenario. This little drop in packets can be attributed to those

acknowledgement packets that are not received by the CA after the termination of communication between two nodes.

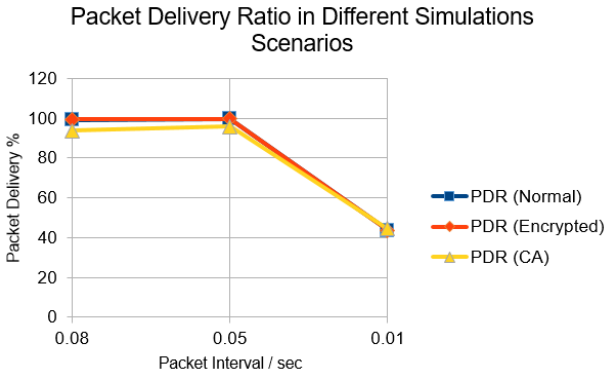

Figure 7. Packet Delivery Ratio in Different Simulations Scenarios

6. CONCLUSION

Vehicular Ad-hoc Networks (VANETs) have revolutionized vehicular communication by providing significant benefits from traffic management to enhanced road safety. In our research, we deeply explored the performance and security dimensions of VANETs with a special focus on the challenges presented by traditional certificate management schemes. We introduced a novel scheme that harnesses the power of RSA encryption in combination with Certificate Authority (CA) management. Our results indicate that this scheme effectively tackles the primary security issues, imposing only a negligible performance cost. Further, our simulation results clearly highlight the superior performance of our method, consistently maintaining key metrics such as end-to-end packets delay, jitter, and PDR even with the integration of additional security measures.

Acknowledgement

The author deeply appreciates Allah for his guidance and strength, which enabled the successful completion of this research. This work is a manifestation of the author's deep gratitude to Allah for the blessings bestowed upon them. Sincere gratitude is extended to all who generously

supported and provided invaluable assistance, including those whose prior research and publications contributed significantly. Heartfelt thanks are also conveyed to family, friends, and esteemed colleagues for their unwavering support, belief in this endeavor, and continuous inspiration. Additionally, the author is profoundly grateful to all who made meaningful contributions, directly or indirectly, ensuring the successful completion of this substantial work.

References

Abbas, Sohail, Manar Abu Talib, Afaf Ahmed, Faheem Khan, Shabir Ahmad, and Do-Hyeun Kim. (2021). Blockchain-based authentication in internet of vehicles: A survey. *Sensors, 21*(23).

Al-Sultan, Saif, Moath M. Al-Doori, Ali H. Al-Bayatti, and Hussien Zedan. (2014). A comprehensive survey on vehicular ad hoc network. *Journal of network and computer applications, 37*, 380-392.

Azam, Farooque, Sunil Kumar Yadav, Neeraj Priyadarshi, Sanjeevikumar Padmanaban, and Ramesh C. Bansal, "A comprehensive review of authentication schemes in vehicular ad-hoc network," IEEE access , vol. 9, pp. 31309-31321, 2021. (2021). A comprehensive review of authentication schemes in vehicular ad-hoc network. *IEEE access, 9*, 31309-31321.

Gautam, V. (2021). Analysis and application of vehicular ad hoc network as intelligent transportation system. *In Mobile Radio Communications and 5G Networks: Proceedings of MRCN*.

Khan, Shawal, Ishita Sharma, Mazzamal Aslam, Muhammad Zahid Khan, and Shahzad Khan. (2021). Security challenges of location privacy in VANETs and state-of-the-art solutions: A survey. *Future Internet, 13*(4).

Khan, Taimur, Naveed Ahmad, Yue Cao, Syed Asim Jalal, Muhammad Asif, Sana ul Haq, and Haitham Cruichshank. (2017). Certificate revocation in vehicular ad hoc networks techniques and protocols: a survey. *Science China Information Sciences, 60*, 1-18.

Khodaei, Mohammad, and Panos Papadimitratos. (2018). Efficient, scalable, and resilient vehicle-centric certificate revocation list distribution in VANETs. *In Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks.*

Manvi, S. S., and M. S. Kakkasageri. (2008). Issues in mobile ad hoc networks for vehicular communication. *IETE Technical Review, 25*(2), 59-72.

Manvi, Sunilkumar S., and Shrikant Tangade. (2017). A survey on authentication schemes in VANETs for secured communication. *Vehicular Communications , 9*, 19-30.

Mokhtar, Bassem, and Mohamed Azab. (2015). Survey on security issues in vehicular ad hoc networks. *Alexandria engineering journal, 54*(4), 1115-1126.

Ptak, M. (2019). Method to assess and enhance vulnerable road user safety during impact loading. *Applied Sciences, 9*(5).

Sharma, Surbhi, and Baijnath Kaushik. (2019). A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications, 20*.

Singal, Gaurav, Vijay Laxmi, Vijay Rao, Swati Todi, and Manoj Singh Gaur. (2017). Improved multicast routing in MANETs using link stability and route stability. *International Journal of Communication Systems , 30*(11).

Vegni, Anna Maria, Claudia Campolo, Antonella Molinaro, and Thomas DC Little. (2013). Modeling of intermittent connectivity in opportunistic networks: The case of vehicular ad hoc networks. *Routing in Opportunistic Networks* , 179-207.

Wang, Jiliang, Yunhao Liu, Yuan He, Wei Dong, and Mo Li. (2013). QoF: Towards comprehensive path quality measurement in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems , 25*(4), 1003-1013.

Zheng, Li, Liren Zhang, and Dong Xu. (2001). Characteristics of network delay and delay jitter and its effect on voice over IP (VoIP). *In ICC 2001. IEEE International Conference on Communications.*