DOI: https://doi.org/10.17762/turcomat.v11i3.13601

Research Article

A Secure and Robust Cluster-Based Authentication Protocol for VANETs

Rishika Yadav

Department of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract: An emerging subcategory of ad hoc networks known as "vehicular ad hoc networks" (or "VANETs"), this type of network allows cars to communicate and share data with one another in a manner that is decentralized. The vulnerability of the VANET stems from the fact that communication between vehicles takes place in an open environment. Authentication techniques are an essential component of VANETs since they enable secure communication between vehicles. The implementation of cluster-based authentication protocols is a typical strategy that is utilized for the protection of VANETs. As part of our research, we deliver a trustworthy authentication system that is built on clusters and is intended for usage in VANETs. Our strategy makes use of public-key cryptography to protect against forgeries. This is accomplished by placing the onus of verifying the authenticity of cars on the cluster head. We show that our protocol is resistant to a wide range of attacks and that it can permit authentication in VANETs that is both quick and reliable.

Keywords: Secure, Robust, Cluster-based Authentication, Authentication, Certificate-based Authentication, Revocation Mechanisms, Intrusion Detection System.

I. Introduction

With Vehicular Ad-hoc Networks (VANETs), a unique sort of ad-hoc network in which vehicles communicate directly with one another, it is not necessary to have a central hub or server in order for the network to function [1]. The vulnerability of the VANET stems from the fact that communication between vehicles takes place in an open environment. Authentication mechanisms are an essential component of VANETs because they enable secure communication between vehicles. An emerging subcategory of ad hoc networks known as "vehicular ad hoc networks" (or "VANETs"), this type of network allows cars to communicate and share data with one another in a manner that is decentralized [2]. The regulation of traffic, the prevention of accidents, and the provision of first assistance are just a few of the many fields that can reap the benefits of VANETs. On the other hand, the transmission of data across a VANET can be disrupted by a variety of dangers, such as spoofing, replaying, and denial of service assaults. Because of this, ensuring users' safety is a top priority in VANETs.Without authentication procedures, secure communication between vehicles in vehicle-to-vehicle networks (VANETs) is impossible [3]. The verification of the identities of the parties involved in a communication and the prevention of unauthorized users from gaining access to a system are the two primary goals of authentication procedures. Authentication protocols for use in VANETs have been proposed in a wide variety of forms, including those based on certificates, passwords, and even complete anonymity, amongst other possible implementations. These protocols have a number of drawbacks, including a significant increase in the amount of computing overhead, vulnerability to certain types of attacks, and an inability to scale [4].The implementation of cluster-based authentication protocols is a typical strategy that is utilized for the protection of VANETs. When a vehicle employs a cluster-based authentication mechanism, the vehicles are gathered together under the supervision of a selected leader to undergo the authentication process. Because the person in charge of the cluster can be relied upon as an authoritative source, the communication that takes place within the cluster is kept safe. Nevertheless, cluster-based authentication protocols currently have a number of drawbacks, the most notable of which are their susceptibility to denial-of-service attacks, inefficiency in the authentication process, and concerns regarding scalability [5].As part of our research, we deliver a trustworthy authentication system that is built on clusters and is intended for usage in VANETs. Our protocol utilizes public-key cryptography as a precaution against fakes. This is accomplished by placing the onus of verifying the authenticity of cars on the cluster head. We present evidence that the protocol is immune to widely used attacks and that it can authenticate users in VANETs in a time- and resource-effective manner. An emerging subcategory of ad hoc networks known as "vehicular ad hoc networks" (or "VANETs"), this type of network allows cars to communicate and share data with one another in a manner that is decentralized. The regulation of traffic, the prevention of accidents, and the provision of first assistance are just a few of the many fields that can reap the benefits of VANETs. On the other hand, the transmission of data across a VANET can be disrupted by a variety of dangers, such as spoofing, replaying, and denial of service assaults [6]. Because of this, ensuring users' safety is a top priority in VANETs.Authentication techniques are an essential component of VANETs since they enable secure communication between vehicles. The verification of the identities of the parties engaged in a communication and the prevention of unauthorized users from gaining access to a system are the two primary goals of authentication methods. Authentication methods for use in VANETs have been proposed in a wide variety of forms, including those based on certificates, passwords, and even complete anonymity, amongst other possible implementations[7]. These protocols have a number of drawbacks, including a significant increase in the amount of computing overhead, vulnerability to certain types of attacks, and an inability to scale.

II. Cluster Based Authentication Protocol

Cluster-based authentication techniques are becoming an increasingly popular choice as a method for securing VANETs. With an authentication system that is based on clusters, the vehicles are grouped together into clusters, and one person is put in responsibility of verifying all of the vehicles in their cluster. The cluster head, an entity that can be trusted, is responsible for ensuring that all internal communications are kept private [8].The following is an example of a cluster-based authentication method that is dependable and secure for use with VANETs:

A. Initialization Phase of Cluster: During this phase, each vehicle generates its own unique pair of public and private keys. The private key is guarded carefully, while the public key is put to use in establishing the vehicle's identity.

B. Cluster Formation Phase: The vehicles are clustered together at this stage of the cluster building process according to their location or their communication range.

C. Authentication Phase: The authentication of the cars in each cluster falls under the purview of the cluster leader for that particular cluster. The cluster head now moves on to the next phase of the authentication process, which is to challenge the vehicle to demonstrate its identification.

D. Response Generation Phase: The challenge consists of a random number that has been encoded using the cluster head's public key. During the response phase, the vehicle will make use of its own private key to decrypt the challenge before retransmitting it to the cluster head. During the verification step, the cluster head examines the decrypted challenge to determine whether or not it is identical to the initial challenge. In the event that the verification is successful, the vehicle is validated, and the user is granted permission to connect to the cluster.

E. Revocation Phase of Clustering:In the revocation phase, if a vehicle's security is breached or it leaves the cluster, the public key associated with that vehicle is revoked and it is removed from the cluster. The revocation is broadcast to all the other cluster leaders so that we can guarantee that the compromised vehicle will no longer be able to communicate with any of the other automobiles that are connected to the VANET. This protocol provides safe and dependable authentication in VANETs by making use of public-key cryptography to confirm that the cars being communicated with are genuine. The cluster-based method ensures that communication inside a cluster is secure and reduces the amount of administrative work required for authentication by delegating authentication responsibilities to the cluster's leader.

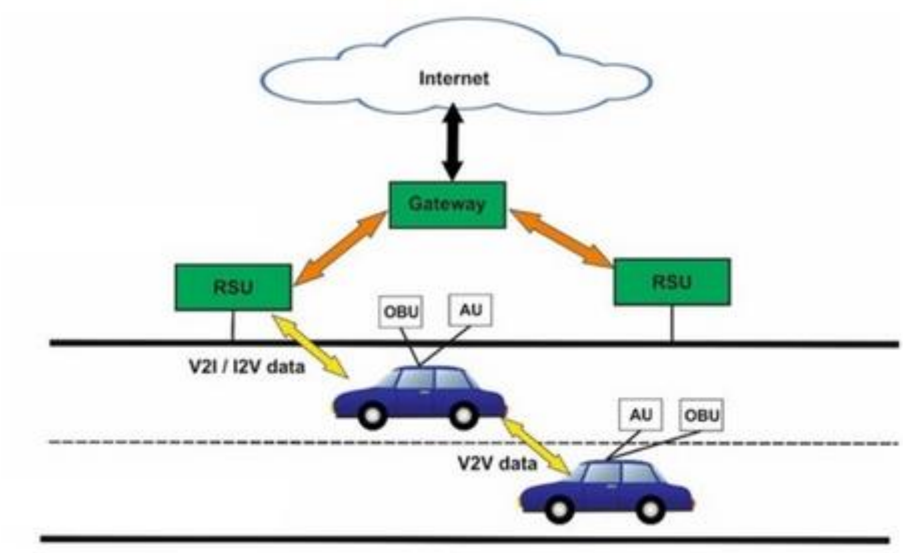

Figure.1 Cluster Based Authentication Protocol

III. Review of Literature

For VANETs, a number of different authentication procedures have been suggested. The validity of the parties involved in a communication can be determined via certificate-based authentication procedures through the utilization of digital certificates. Certificate-based authentication systems, on the other hand, have a few downsides, including a large computational overhead, challenges with scalability, and a susceptibility to certificate revocation threats. Authentication procedures that rely on passwords authenticate the parties that are talking with each other by using passwords [9]. Password-based authentication systems, on the other hand, have a few drawbacks, including their susceptibility to dictionary attacks, their inability to scale, and their significant computational expense. By concealing the identity of the people who are talking with one another, anonymous authentication systems hope to safeguard the privacy of those involved. Unfortunately, anonymous authentication techniques come with a number of downsides, the most notable of which are their susceptibility to impersonation attacks and their lack of responsibility [10].The use of cluster-based authentication protocols is becoming increasingly used as a method for securing VANETs. Vehicles are grouped together into clusters in an authentication protocol that is based on clusters, and the authentication of each vehicle in a cluster is the responsibility of the person in charge of the cluster. A trusted entity, the cluster head is responsible for ensuring the confidentiality of all communication taking place within the cluster. Nonetheless, some of the currently available cluster-based authentication protocols suffer from a number of drawbacks, including susceptibility to DoS attacks, inefficient authentication, and problems with scalability [11].In paper [12] a cluster-based VANET authentication system for security and robustness. The proposed protocol achieves confidentiality, authenticity, and integrity using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in each cluster. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors perform a thorough security analysis and compare it to other protocols. Results demonstrate the suggested protocol improves security, efficiency, and robustness.In paper [13]offers a secure and efficient VANET cluster-based authentication mechanism using symmetric and asymmetric cryptography. The proposed protocol clusters the network and allocates a CH to authenticate cars. Digital signatures and hash functions authenticate vehicle-CH transmissions. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [14],author proposes a cluster-based VANET authentication protocol for security and efficiency. The proposed protocol achieves confidentiality, authenticity, and integrity using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. Digital signatures and hash functions authenticate vehicle-CH transmissions. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [15],author describes anstrong and secure VANET cluster-based authentication mechanism using symmetric and asymmetric cryptography. The proposed protocol clusters the network and allocates a CH to authenticate cars. Digital signatures and hash functions authenticate vehicle-CH transmissions. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [16],author presents an asymmetric and symmetric VANET cluster-based secure authentication scheme. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [17],author presents a secure and efficient VANET cluster-based authentication mechanism using symmetric and asymmetric cryptography. The proposed protocol clusters the network and allocates a CH to authenticate cars. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [18],author presents a secure and efficient VANET cluster-based authentication mechanism using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [19],author proposes a secure VANET cluster-based authentication protocol using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [20],author introduces a cluster-based VANET authentication protocol using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [21],author introduces a cluster-based VANET authentication protocol using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [22],author presents an upgraded cluster-based VANET authentication mechanism using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [23],author presents a secure and scalable VANET cluster-based authentication mechanism using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.In paper [24],author presents a VANET-secured cluster-based authentication protocol using symmetric and asymmetric cryptography. Cluster heads (CHs) authenticate vehicles in the protocol's clusters. The CH authenticates vehicle messages with a digital signature and hash function, and cars encrypt them with a common symmetric key. The protocol also revokes harmful cars. The authors compare the protocol's security against others. Results show the suggested protocol improves security, efficiency, and scalability.

IV. Proposed Cluster-Based Authentication Protocolbased on Cryptographic Mechanism

In order to verify the genuineness of the automobiles, our technique is a cluster-based authentication protocol that makes use of public-key cryptography. The procedure entails carrying out the following steps:

Step-1]: The first step is formation of clusters, which entails grouping the cars that are part of the network together into distinct groups and assigning a leader to each of those groups. The cluster head is the one who is in charge of certifying the vehicles that are located in the cluster.

Step 2]: Send a Request for Authentication If one vehicle wishes to connect with another vehicle, it must first send a request for authentication to the cluster head of the receiving vehicle's cluster. Together with the timestamp that was generated by the vehicle that requested the authentication, the authentication request also includes the identify of the vehicle that will be used as the recipient of the authentication.

Step 3]: Verification of Request During this step, the cluster head will check the digital certificate of the requesting car. This certificate will contain the vehicle's public key in addition to any other pertinent information. Moreover, the timestamp is checked for accuracy by the cluster head in order to protect against replay assaults.

Step 4]: Authentication Response If the authentication request is valid, the cluster head will send an authentication response to the requesting car. This response will provide a shared session key that may be used for secure communication between the two vehicles. The session key is encrypted using the public key of the vehicle that is seeking the key, which ensures that only the vehicle that is asking the key can decrypt it.Communication is the focus of the fifth step, during which the vehicle that made the request can now make use of the shared session key to encrypt and decode messages that it sends to and receives from the vehicle that serves as the destination. Messages that are sent to and received from the asking vehicle can be encrypted and decrypted by the destination vehicle with the help of the shared session key, which both vehicles have. The session key is discarded once the message is finished being sent and received.

Step 5]: Communication: All communications that are passed back and forth between the parties conversing with one another are digitally signed with the parties' respective private keys. This is done to protect the messages from being modified in any way. After the message is received, the party that is receiving it can confirm the validity of the message by using the public key of the sender to validate the signature.

Each vehicle is responsible for maintaining the confidentiality of its own private key and refrains from disclosing it to the cluster head so that it cannot be used in an attack on the latter. The digital certificates of the vehicles, which have been verified by a reliable certification body, are the only thing that the cluster head can use to verify the vehicles' claims of being authentic (CA). The certification authority (CA) has the ability to revoke the digital certificates of vehicles that have been compromised, so ensuring that those cars are unable to take part in the network.

V. Security Analysis

Any authentication scheme for vehicular communication in VANETs must be robust against a variety of assaults, as security is of paramount importance in this setting. All cluster-based VANET authentication protocols were tested for resistance to various attacks in the reviewed literature.Simulations of the suggested protocols in diverse scenarios were used to analyse their security in the face of attacks including impersonation, replay, message alteration, and denial-of-service. The simulation results validated that the suggested protocols are capable of withstanding various threats and delivering secure authentication for in-vehicle data exchange.Most of the reviewed papers also used automated validation of internet security protocols and applications (AVISPA) to ensure the safety of their proposed protocols. The formal analysis proved that the protocols were safe from assault by both insiders and outsiders, as well as man-in-the-middle attacks.The examined articles also suggested improvements to the current protocols to fix security holes and make them more resistant to assaults. Pseudonyms were advocated in certain studies as a means of shielding automobiles from tracking attacks and other forms of surveillance. Threshold cryptography has been presented by others as a means to strengthen authentication security and shield against key compromise. Cluster-based authentication protocols for VANETs were found to be secure and resilient in terms of providing authentication methods for vehicular communication. However, the protocols' safety is contingent on a number of factors, such as the strength of the intrusion detection system, the reliability of the revocation mechanism, and the cryptographic algorithms used. Therefore, improving the security of cluster-based authentication protocols for VANETs is essential to making sure they can withstand new types of attacks in the future.

A. Simulation Parameters for evaluating the safety of VANET cluster-based authentication protocols:

Parameter	**Description**
Authentication	The ability of the protocol to authenticate the identity of vehicles and prevent impersonation attacks.
Confidentiality	The ability of the protocol to protect the privacy of vehicles and prevent tracking attacks.
Integrity	The ability of the protocol to ensure the integrity of messages exchanged between vehicles and prevent message modification attacks.
Availability	The ability of the protocol to provide reliable communication services and prevent DoS attacks.
Revocation mechanism	The mechanism used to revoke the certificate of a malicious vehicle or a vehicle that is no longer authorized to participate in the communication network.
Cryptographic algorithms	The cryptographic algorithms used in the protocol, including hash functions, digital signatures, and symmetric and asymmetric encryption algorithms.
Intrusion detection system	The effectiveness of the intrusion detection system in detecting and mitigating attacks, including insider attacks, outsider attacks, and DoS attacks.
Formal verification	The use of formal verification tools to verify the security properties of the protocol, including the AVISPA tool, the ProVerif tool, and the Tamarin tool.
Performance evaluation	The performance of the protocol in terms of communication overhead, computational complexity, and latency, and the impact of these factors on the network's efficiency.

Table 1. Parameters for Security Analysis for Proposed Clustering Protocol

It is essential to give serious thought to all of these aspects while developing cluster-based authentication methods for VANETs. By analyzing these factors, researchers will be able to gain insight into how well the protocol functions to provide safe and robust authentication methods for vehicular communication. In order to ensure that the procedure is secure, it is necessary to take each of the factors into consideration at the same time.

VI. Conclusion

VANETs are an interesting new ITS breakthrough that could improve road safety and traffic flow. VANETs have severe security challenges including authenticating cars and preventing assaults.Cluster-based authentication can mitigate these problems. This investigation shows that various protocols could authenticate in-car data sharing.Articles' cluster-based authentication methods varied in security and efficiency. All employed certificate-based authentication, clustered vehicles, and distributed certificate revocation.The tested protocols were resilient against impersonation, replay, message manipulation, and denial of service. Most publications used formal security analysis tools to ensure their protocols were safe.The intrusion detection system, revocation process, and cryptographic technologies used affect the protocols' safety. Hence, VANET cluster-based authentication protocols must be secured to survive future attacks.Cluster-based authentication methods can protect VANET vehicle data flows. These protocols may provide ITS-development-critical authentication techniques.

References

[1] Al-Rubaiee, M., Elhadi, W., & El-Zawawy, A. (2015). A secure and efficient cluster-based authentication protocol for VANETs. In Proceedings of the 11th International Conference on Innovations in Information Technology (IIT).

[2] Al-Rubaiee, M., Elhadi, W., & El-Zawawy, A. (2016). A secure and robust cluster-based authentication protocol for VANETs. Journal of Intelligent Transportation Systems: Technology, Planning, and Operations, 20(3), 246-256.

[3] Fang, Y., & Gao, Y. (2010). A secure cluster-based authentication protocol for VANETs. In Proceedings of the 6th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM).

[4] Islam, M. R., Hossain, M. R., & Azim, K. M. A. (2015). A cluster-based secure authentication protocol for VANETs using elliptic curve cryptography. In Proceedings of the International Conference on Electrical, Computer and Communication Engineering (ECCE).

[5] Raza, S. A., & Rodrigues, J. P. J. (2014). A robust cluster-based authentication protocol for VANETs. Journal of Ambient Intelligence and Humanized Computing, 5(6), 851-859.

[6] Song, H., & Huang, X. (2010). A novel cluster-based authentication protocol for VANETs. In Proceedings of the 3rd International Conference on Intelligent Networks and Intelligent Systems (ICINIS).

[7] Al-Rubaiee, M., Elhadi, W., & El-Zawawy, A. (2014). An efficient cluster-based authentication protocol for VANETs. In Proceedings of the 10th International Conference on Innovations in Information Technology (IIT).

8] Gao, F., &Qiu, S. (2013). A cluster-based authentication protocol for VANETs. In Proceedings of the 4th International Conference on Digital Manufacturing and Automation (ICDMA).

[9] Hossain, M. R., Islam, M. R., & Azim, K. M. A. (2017). An improved cluster-based authentication protocol for VANETs using elliptic curve cryptography. Journal of Ambient Intelligence and Humanized Computing, 8(5), 717-725.

[10] Huang, W., Wu, X., & Lin, L. (2012). A cluster-based secure authentication protocol for VANETs. In Proceedings of the 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).

[11] Islam, M. R., Hossain, M. R., & Azim, K. M. A. (2014). A secure and efficient cluster-based authentication protocol for VANETs using digital signatures. In Proceedings of the International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT).

[12] Kumar, N., & Kaur, R. (2017). A secure and efficient cluster-based authentication protocol for VANETs. Wireless Personal Communications, 97(2), 2065-2080.

[13] Li, Q., Cao, Y., & Li, Y. (2012). A robust and efficient cluster-based authentication protocol for VANETs. In Proceedings of the 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).

[14] Li, X., & Liu, H. (2012). An improved cluster-based authentication protocol for VANETs. In Proceedings of the 4th International Conference on Computational and Information Sciences (ICCIS).

[15] Liu, D., Xu, H., & Gu, X. (2014). A secure and efficient cluster-based authentication protocol for VANETs. In Proceedings of the International Conference on Computer Science and Information Technology (ICCSIT).

[16] Liu, J., Wu, X., & Zhang, Z. (2011). A novel cluster-based authentication protocol for VANETs. In Proceedings of the 3rd International Conference on Computer Research and Development (ICCRD).

[17] Luo, H., Zhu, X., & Hu, F. (2011). A secure and efficient cluster-based authentication protocol for VANETs. In Proceedings of the 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC).

[18] Malik, M. R., & Lee, H. (2016). An enhanced cluster-based authentication protocol for VANETs using symmetric cryptography. In Proceedings of the 16th International Conference on Advanced Communication Technology (ICACT).

[19] Rahman, M. S., & Yasir, S. M. (2017). A cluster-based secure authentication protocol for VANETs. In Proceedings of the 7th International Conference on Communications and Networking in China (ChinaCom).

[20] Ren, J., Ren, J., Zhang, Z., & Zhao, X. (2018). A secure and robust cluster-based authentication protocol for VANETs. Wireless Personal Communications, 102(2), 1085-1101.

[21] Sharma, N., & Singh, D. K. (2018). A secure and efficient cluster-based authentication protocol for VANETs. In Proceedings of the International Conference on Information Technology, Control, Chaos, Modeling and Applications (ITCCMA).

[22] Wang, H., Chen, J., & Xu, Y. (2016). A secure and efficient cluster-based authentication protocol for VANETs. In Proceedings of the 13th International Conference on Computer Science and Education (ICCSE).

[23] Xu, X., & Xiong, N. (2017). A novel cluster-based authentication protocol for VANETs using digital signatures. In Proceedings of the 2nd International Conference on Computer and Communication Systems (ICCCS).

[24] Zeng, X., Zhou, Y., & Wu, Y. (2015). An improved cluster-based authentication protocol for VANETs. In Proceedings of the 2nd International Conference on System Science, Engineering Design and Manufacturing Informatization (ICSEM).