ISSN No:-2456-2165

VANET Security: Mitigating Threats and Enhancing Road Safety

Nirmana M.P.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Herath H.M.I.D.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Dias L.S.
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Afridh W.M.
Department of Computer Science and Software Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka

Abstract:- Vehicular Ad-Hoc Networks, or VANETs, hold great promise for improving traffic control and road safety. However, the constantly changing character of VANETs—which are distinguished by high mobility, a sizable network, and geographic significance—presents particular security difficulties. Particularly dangerous are Sybil attacks, in which malevolent nodes impersonate trustworthy automobiles and have the capacity to cause fatalities and serious accidents. This abstract explores the first part of our study, which focuses on mitigating the serious threat posed by Sybil attacks in VANETs. To lessen this threat, previous research has investigated anomaly detection systems, public key infrastructures (PKI), and cryptographic techniques. Furthermore, methods like group signatures, certificate revocation, and pseudonym modifications have been used to guarantee the integrity and reliability of VANET communication. Through the introduction of a novel technique that enhances VANET security by creating distinct hash values using an intersection of serial keys and device IDs, our research seeks to add to this body of knowledge. Sybil attacks are effectively prevented by these distinct hashes, which make it easier to verify the location of vehicles and authentic connections. Our project aims to provide a strong security foundation for VANETs, lowering the hazards caused by malicious behavior and protecting road users' lives by expanding on the knowledge gained from earlier research. As we proceed, we acknowledge the value of security protocols in VANETs and the necessity of tackling Sybil attacks to guarantee the reliability of communication in these networks. This component, which is part of a larger initiative, uses VANET technology to help make improved security and safety for public transportation a reality.

I. INTRODUCTION & LITERATURE REVIEW

In a time of lightning-fast growth in technology, the development of transportation networks has been nothing short of amazing. A particular innovation that demonstrates the cooperation of state-of-the-art technology with the contemporary demand for safer, more effective roads is the Vehicular Network. VANETs represent a paradigm change in how we view traffic control and highway safety, not just a step forward in the field of automobile communication. VANETs are becoming extremely popular due to their likelihood to completely change the transportation industry. These wireless networks create possibilities for immediate exchange of data by allowing cars to interact with outside infrastructure as well as one another. As a result, the foundation for more secure and efficient public transportation has been established by this connectivity. But innovation also carries responsibility, and the use of VANETs presents a fresh set of security issues that require our full attention. This research is urgent because of the stark reality that attacks on VANETs might have catastrophic effects [1]. The communication that is essential for preventing accidents, anticipating traffic patterns, and promoting general road safety could be hampered by malicious activity in VANETs. In fact, the same characteristics that have distinguished VANETs apart from typical networks and made them vulnerable to particular risks to safety are also what renders them so intriguing in terms of accessibility, network capacity, and regional significance [2].

The primary focus of the study we are conducting is to maximize the efficacy of VANETs to improve motorist safety while simultaneously guaranteeing their dependability and safety. In order to achieve this, we have created an efficient communication network that makes it easier for cars to share vital data regarding impending collisions and traffic jams. Our goal is to greatly lower the risks related to attacks on VANETs by fixing the vulnerabilities that are inherent in VANETs and offering an encrypted network for vehicle-to-vehicle and

vehicle-to-infrastructure communication. This work is organized to explore the various safety issues that VANETs pose, the importance of dependable vehicle-to-vehicle communication of data, and the system we have created to address these problems. In order to achieve our shared goal of safer and more effective accessibility on our roads, we will investigate current security risks and suggest innovative remedies. As we set out on this adventure, we understand how crucial a reliable, secure, and cost-effective VANET system is. We are getting closer to a time when effortless information sharing amongst cars opens the door to an increasingly connected, less hazardous globe on the roads with every step we take. Our research aims to make significant improvements to this endeavor, helping to realize all that is possible of VANETs and promoting safer travel for all [2] [3].

Vehicle Ad-Hoc Networks have the potential to completely change how we travel and guarantee the secure travel of our routes. But this revolutionary perspective also presents an urgent difficulty: protecting these networks from numerous dangers that might result in far-reaching effects on people's lives. Being the forerunners of this research project, we understand how crucial it is to solve the security problems with VANETs while also utilizing their potential to improve traffic safety.

Our group's mission is clear: using a multifaceted strategy that includes four unique components, each tailored to address a particular challenge, we will strengthen both the safety and instantaneous interaction features of VANETs [3].

- *Install the malicious node detection system for Sybil Attack:*

We present a novel approach to prevent Sybil attacks and guarantee that our VANETs are networks are free of malicious users. By combining the serial key and device ID, this technique creates a unique hash that makes it possible to confirm the authenticity of interactions as well as the precise positioning of individual vehicles. We strengthen the trustworthiness of the VANET by thwarting the infamous Sybil attack.

- *Amendments on Traffic in Real Time Through Sockets:*

Transmitting information regarding traffic in an accurate way is a crucial component of road safety. Our study incorporates socket interaction to deliver real-time traffic updates, guaranteeing that all vehicles on the network have access to the most recent data. This part provides a workable way to reduce traffic-related incidents and gridlock, resulting in safer and more effective roads [4].

- *Effective Cooperative Authentication Protocol for Privacy Protection:*

The study we conducted presents novel shared authentication procedures to improve security. This protocol fixes the flaws in the current Vehicle-to-Vehicle (V2V) authentication process systems in addition to guaranteeing secure V2V communication. As a result, there is reliable and trustworthy vehicle communication over a safer, more robust network.

- *Identity Validation and Request Tracking:*

Our research group has developed an application that monitors the quantity of recognition requests, improving the security of VANETs by preventing unintentional access in situations where safety and confidentiality are critical. By making certain that only those with permission are able to make use of the network, this painstaking monitoring mechanism provides an extra line of defense toward any possible dangers [5].

- *Real-Time Vehicle Movement Monitoring:*

We've created a real-time vehicle movement monitoring system to track vehicle movements within the VANET in an era where data-driven insights and surveillance are essential for maintaining security. For the purpose of managing traffic and preventing accidents, this component offers crucial insights into vehicle behavior and traffic patterns.

We comprehend completely that the combined effect of these four elements will bring in a new era of communication and security for VANETs as we set out on this journey. With the help of our research, we hope to create a safer and more connected world where VANETs serve as both a technological marvel and a symbol of dedication to ensuring the safety of all road users. This document functions as our road map, offering a thorough analysis of every element and its importance within the larger framework of VANET communication and security [6].

The Sybil attack, in which a single malicious node adopts numerous false identities to compromise the reliability of the system, is one of the most prevalent risks to VANETs. Multiple approaches have been investigated in research to address this challenge. In order to identify Sybil nodes, Shamal et al. (2019) presented a novel method utilizing location identification and distinct device identifiers. By guaranteeing that in the network, only valid connections are made, this technique improves security. For roads to be safer and more effective, real-time traffic information exchange is essential. Previous work by Wang et al. (2020) concentrated on using Vehicle-to-Everything (V2X) contact to facilitate real-time traffic revisions, lowering traffic and the danger of accidents. Their research emphasizes the value of timely information sharing and establishes the framework for our method of incorporating socket-based communication for traffic updates in VANETs [7].

Moderate mobility, an ever-changing network size, and spatial relevance are some of the distinctive features of VANETs that create a unique set of security issues. Attacks on VANETs have serious repercussions that could result in mishaps and fatalities. The Sybil malware infection is one of the most well-known threats; malicious nodes pose as genuine cars, spreading false information and possibly posing a threat to human life. This problem has been tackled by a number of

research projects using anomaly detection, secure authentication, and cryptographic techniques. Methods for reducing security risks and guaranteeing reliability in VANET communication have been investigated, including group signatures, fictitious name changes, and certificate cancellation. One of the main features of VANETs is instantaneous data exchange, which could completely transform the administration of traffic and road safety. A great deal of research has gone into creating reliable interaction protocols that will allow cars to exchange real-time traffic and accident information. Various communication protocols have been investigated to facilitate dependable vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, including Dedicated Short-Range Communication (DSRC), IEEE 802.11p, and Cellular-V2X. The foundation of communication systems intended to deliver timely updates about accidents, traffic jams, road hazards, and other vital information is made up of these protocols. As a result of data collection and exchange within VANETs, privacy and anonymity issues have surfaced. Pseudonym management plans, confidentiality gathering of information, as well as the use of encrypted hardware components for safeguarding identities of users are some of the approaches that researchers have suggested to address these problems. A major concern in this field has been finding a balance between protecting user privacy and sharing data for safety.

II. METHODOLOGY

In the methodology section, it is explained how the device ID and serial number combined to form the unique identification number are used by the proposed system to identify individual vehicles. This also explains how the malicious node is located and how our suggested system counteracts Sybil attacks. By sending and receiving messages using their individual IDs, onboard wireless communication devices allow vehicles to communicate with roadside infrastructures (RSU) for vehicle-to-infrastructure communication as well as with other vehicles.

A. Identify the malicious node in Sybil attacks –

In Sybil attacks, the attacker maliciously claims or steals numerous identities and utilizes them to disrupt the VANET's operation by propagating fake identities. The shortcoming of Sybil attack detection systems, which are built on critical infrastructure for detecting such attacks, is that the algorithm cannot identify the rogue node that launched the attack. To detect the malicious Sybil attack node, our approach employs a combination of location verification, unique ID verification, statical analysis, and neighbor detection [8].

- *Location Verification –*

Verifying a node's location through GPS is known as location verification. Different drivers cannot operate two different vehicles in the same manner because they are each driving for their own comfort and needs. Finding two or more nodes that have comparable motion trajectories allows one to identify the Sybil node. There are various processes involved in the location verification process. First, each node broadcasts its claimed location and unique identifier to the network. Second, additional network nodes receive these location claims and utilize their own location-based services to validate the claims' accuracy. The node is regarded as authentic if the stated location matches the physical location within a set threshold. Otherwise, the node is identified as a possible Sybil node. Furthermore, powerful machine learning techniques like deep learning or support vector machines can be utilized to examine location data and find abnormalities that may indicate the presence of Sybil nodes. Also if multiple nodes are found in the exact physical location, it is possibly a malicious node [9].

- *ID Verification –*

Basically, a unique hash value will be generated using the device ID and the serial key of the product and it will be used to verify the connection with the server.

- *Statical Analysis –*

Statistical network traffic analysis can aid in the detection of Sybil attacks. Malicious nodes frequently generate traffic that differs dramatically from genuine nodes. As a result, statistical analysis can be utilized to discover nodes that produce unusual traffic patterns. The main idea is to evaluate the statistical features of network data in order to find anomalies that differentiate Sybil nodes from legitimate nodes. To represent the statistical features of network traffic, such as probability distributions, correlation matrices, or principal component analysis (PCA) coefficients, statistical models are built [4].

- *Neighbor Detection –*

The primary idea is to detect Sybil nodes by monitoring their network behavior and connections to surrounding nodes. Each node keeps a list of its neighbors, which can be accomplished through several approaches like as beaconing or broadcasting. Then, each node examines its neighbors' activity, such as communication patterns and traffic levels, to discover anomalies and identify potential Sybil nodes. The accuracy of neighbor detection can be improved by employing trust-based models to assess the reputation and dependability of surrounding nodes, or by employing machine learning approaches to detect anomalies in network behavior. In neighbor detection, a node that is linked to numerous neighbors using the same IP/MAC address is most likely a malicious node [10].

B. Implementing solutions to V2V authentication requirements in VANET –

- *Hybrid Location Tracking -*

In this proposed system, the initial geo-location is obtained using GPS. In parallel with this, an Accelerometer is employed to monitor the vehicle's movements. A conventional VANET typically relies solely on the Accelerometer for location tracking, but this system utilizes both. Initially, the

location is tracked using GPS, and subsequently, it is tracked based on data from the Accelerometer.

The Load Balancing Routing Protocol (LBRP) calculates and configures routes based on node locations, eliminating the need for the construction of routing tables. The protocol comprises three components: beaconing, location, and forwarding services [11].

A drawback of this protocol is its reliance on the Global Positioning System (GPS) for accurate vehicle location, which may pose challenges in areas with weak satellite signals, such as tunnels. However, it excels in highway environments and offers optimal performance. Furthermore, it is particularly efficient in high-mobility settings.

➢ *Authentication between vehicle infrastructure –*

Numerous attacks on the VANET can be rendered less effective by utilizing the authentication protocols. By using authentication processes, the VANET can operate more efficiently and will prevent the imposition of illegal content between OBUs and RSUs.

The following are prerequisites for the VANET authentication protocols.

- First and foremost, methods of authentication must possess strong cryptography without the need for encryption. By enforcing this requirement, telecommunication modules (OBU) and base stations (RSU) may be able to implement authentication without requiring the delivery of private and public keys.
- Second, RSUs shouldn't gather data about the car and the driver during the authentication procedure. The confidentiality and anonymity of the vehicle's owners will be violated if this requirement is not met, as the RSU will be able to determine the route of any vehicle.
- Thirdly, a rule allowing the protocol parameters to be adjusted based on the intensity of vehicle traffic must be included in the authentication protocol. In situations where traffic volume is high, RSU devices must shorten the time needed for vehicle identification. The cryptographic strength of the protocol can be altered to accomplish this goal.

Fourth, the protocol should enable service providers to connect with automobile owners by providing them with access to the VANET network's vehicle registration sites (VRS). One needs to submit a service delivery request in order to receive services. That being said, the vehicle ID and the required services cannot be transmitted over an open channel because of the potential for message interception or modification. As a result, the algorithm used in the OBU-VRS authentication protocol needs to enable the VRS to decrypt the vehicle's public key. Next, the VRS confirms its credentials and offers the necessary service using the computed public key. [7].

Our contribution is as follows.

- Based on zero-knowledge proof, an adaptive authentication protocol was created with consideration for the requirements for authentication in the VANET. When completing OBU-RSU, RSU-OBU, and OBU-OBU authentication without the use of encryption techniques, this protocol offers a high degree of anonymity. In this scenario, the information obtained by RSUs or OBUs during the authentication procedure will prevent the trusted authorities from tracking the vehicle's route. In addition, this protocol saves a lot of time when it comes to vehicle authentication. By reducing the number of execution stages in comparison to previously established challenge-response protocols, this can be accomplished.

- A plan that enables the parameters of the protocol to be adjusted based on the volume of vehicle traffic. In situations where traffic volume is low, the OBU opts for a high level of confidentiality, specifically level 3. The user can reduce the secrecy level (to level 2) as traffic congestion increases. The amount of time needed for vehicle authentication will decrease as this level falls. The least amount of time spent on vehicle authentication is ensured by a further reduction in secrecy to the first level. It makes it possible for RSUs to function well in situations with heavy traffic [5].

- A procedure for confirming the car owner's legitimacy to provide requested services. The VRS calculates the vehicle's public key without the need for encryption as a result of this protocol's implementation, and it also offers the required services.

C. Implementing components that can verify the identification by keeping track of the number of requests –

In this study, we primarily concentrate on deploying two essential elements to strengthen the security of vehicular ad hoc networks (VANETs). The first part is identity verification, in which users' authorized status is determined by means of a strong hash value method. White-listing, the second element, is used to safely enroll new users into the VANET system.

➢ *Identity Verification* -

First, we acquire and prepare the necessary data by gathering real-world information or modeling VANET scenarios, such as vehicle identification and interaction requests. After that, preprocessing is done on the data to make sure it is arranged and anonymous to safeguard user privacy. We put in place a reliable system for hash value generation for identity verification that makes use of both device IDs and serial keys. Together with the matching vehicle identification and authorization status, these distinct hashes are kept in a database. Relying upon those hash values, a verification algorithm is created to validate incoming inquiries. We also develop a request monitoring system at the same time, keeping track of a query counter for any vehicle in the database of vehicles. The maximum amount of authorized identity queries in a certain period of time is determined by a threshold value.

We constantly track the request counter in real-time. We design an anomaly detection method that can detect anomalies and attempts at illegal access. Depending on how serious the abnormality is, this mechanism sets off the proper reactions, which can include suspending access temporarily, notifying network administrators, or taking other required action. Testing and evaluation come next, during which we put the implemented components to the test in a virtual or actual VANET environment. Identification verification and request tracking components are assessed for efficacy using performance indicators including false positives, false negatives, detection accuracy, and response time [5].

The completed components are then incorporated into the wider VANET system, guaranteeing smooth functioning with further safety and telecommunication modules. To be able to accommodate different network sizes and data quantities, flexibility and efficiency are considered. The validation procedure is done to ensure that the system functions correctly and according to plan. A great deal of paperwork is kept up to date during this procedure in order to document implementation specifics, conclusions, and outcomes [9].

- *White Listing*

White-listing pertains to a distinct facet of VANET security. We start a thorough white-listing procedure the moment a user logs into the system for the first time. We specify precise requirements for user authorization in this manner. User identities are rigorously verified through the production of digital signatures, authentication certificates, and the validation of vehicle registration details. The purpose of an access control mechanism is to limit network access to just those authorized users who are on the white-list [8]. Because this process is real-time, authorized users can be onboarded right away, while unauthorized entities cannot access the system. Then, new authorizations are added and expired ones are removed from the white-listed user database through routine updates and maintenance.

D. Facial Movement Detection On the VANET System

Designing a Facial Movement Detection System for Vehicular Ad Hoc Networks (VANETs) involves several key steps and considerations. Here we created this for Protect the Drivers from Accidents and sleeping wile driving. For this objective we have some prefixed devices in the Vehicle. A face detection system within VANETs can have applications in surveillance, driver monitoring, and passenger safety. Here's a methodology for implementing a Facial Movement Detection in VANET

- *Camera mounted inside the vehicle and capture the faces of drivers.*

This unit processes the video feed from the cameras, performs face detection, tracks faces, and analyzes facial movements. It can be implemented using onboard vehicle computing resources or connected to the VANET infrastructure. To enable real-time communication with other vehicles and the VANET infrastructure, a communication module is integrated. This module allows for the exchange of information related to detected facial movements and potential safety warnings. Face detection and tracking algorithms are essential for identifying and following faces within the video feed. Here we used predesigned libraries and command s to detect facial detections. These algorithms analyze the facial movements of drivers. They can detect various movements such as blinking, yawning, nodding, and other gestures that indicate driver drowsiness or distraction [12] [13].

- *Face Detection*

The system's face detection algorithm identifies and localizes faces within the video frames. The system's tracking algorithm follows the identified faces, even as they move within the frame or if multiple faces are present. Facial movement analysis algorithms monitor the tracked faces for specific movements indicative of drowsiness, distraction, or other safety concerns. he system may send alerts and relevant data to other vehicles in the vicinity via the VANET network, potentially warning nearby drivers about the driver's condition or potential hazards [14].

III. RESULTS AND DISCUSSION

We explain and share the findings from our research study in this section, which addressed the vital problem of security in vehicular ad hoc networks (VANETs). We are aware that security breaches on VANETs may have unfavorable effects, including accidents and fatalities [15]. Owing to the distinct qualities of VANETs, including their large network size, high mobility, and geographic relevance, our study sought to create a communication system that would allow cars to exchange information regarding upcoming accidents and traffic patterns. We provide our research findings below and go over their consequences [16] [17].

The outcomes of our study show that a VANET communication system for exchanging data regarding incidents and traffic conditions was successfully developed and put into operation. Vehicles on the network receive real-time updates from this system, which warns drivers of possible dangers and traffic. We discovered that the system successfully notifies linked vehicles of important information, such as accident alerts and traffic congestion warnings, after conducting thorough testing in both simulated and real-world VANET scenarios [18]. According to our tests, the system successfully disseminated information with a high degree of accuracy and above 95% success rate. Updates were regularly delivered with lightning speed, guaranteeing that cars got current and useful information. With the use of device IDs and serial keys, the privilege of Sybil attack malicious node detection technique creates unique hashes that are successfully verified, allowing us to check for authentic connections and verify the position of VANET cars. We ran experiments in simulated VANET scenarios to evaluate this component's efficacy [19] [20].

Socket-based real-time traffic condition update system has shown to be a very effective technology. It was successful in giving VANET users real-time updates. Users were guaranteed to obtain crucial information regarding traffic conditions and incidents because to the rapid and precise updates [21]. The reciprocal authentication system for privacy protection in secure vehicle-to-vehicle (V2V) communication performed exceptionally well. With an average response time of 15 milliseconds and an authentication accuracy of 97.5%, it defeated the drawbacks of conventional V2V authentication techniques. Through the use of sockets, our real-time traffic condition updating system allows cars to communicate with one another and exchange vital information about impending accidents and traffic. A variety of simulated and real-world tests were used to assess this system's efficacy [22].

An effective mutual authentication mechanism for privacy protection was created by us to facilitate secure vehicle-to-vehicle (V2V) communication and improve security in VANETs. The correctness of the authentication process and response times were assessed for this protocol [19]. With a success percentage of 97.2%, the correctness of the authentication. An average reaction time of 15 milliseconds is the response time distribution. We put in place a feature that counts the amount of queries to confirm users' identities. The tracking methodology was assessed in terms of response times and detection accuracy. The detection accuracy is displayed with a remarkable rate of 96.8%. The response time distribution is shown the average reaction time is 25 milliseconds [23].

IV. CONCLUSION

To sum up, our research project has addressed the urgent problem of security in vehicular ad hoc networks (VANETs) with significant progress. We started working on the development of a VANET communication system to improve traffic management and road safety because we were aware of the possible negative effects of security breaches, which could lead to accidents and fatalities [24].

Our study has produced observable outcomes that show how well the VANET communication platform has been implemented. Through extensive testing, which included both simulated and real-world VANET scenarios, we have proven that the system is capable of providing linked vehicles with accurate and timely information. With a knowledge dissemination success rate of over 95% and quick response times, the system offers critical alerts and traffic updates, enabling cars to drive safely and sensibly [25]. Our research emphasizes how important communication and security are in the particular setting of VANETs. Because of the network's great mobility, vast size, and geographic significance, creative solutions are needed to reduce risks and improve safety. The system that we have created is a major advancement in tackling these problems. Our findings have implications for the larger field of vehicular communication and security, even outside the immediate scope of our study [26]. As VANETs develop further and become more essential to contemporary transportation networks, our research emphasizes the critical role that cutting-edge solutions play in saving lives and maximizing the effectiveness of our roads [27].

Essentially, our study not only tackles the initial investigation's problem but also emphasizes how crucial reliable and flexible networks of communication are to guarantee the safety of all users of the road. The project's advancement is evidence of the possibility of creative approaches to promote a more effective and safe driving environment in VANETs and elsewhere [7].

REFERENCES

[1] S. A. Asra. [Online]. Available: https://www.researchgate.net/publication/361798203. [Accessed 12 03 2023].

[2] F. A. K. A. I. Muhammad Imran, "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks," 06 2014. [Online]. Available: https://www.researchgate.net/publication/269876048. [Accessed 02 04 2023].

[3] P. G. Sujithra Muthuswamy, "IOT Security Challenges and Issues," 02 2016. [Online]. Available: https://www.researchgate.net/publication/301887203. [Accessed 23 05 2023].

[4] S. G. A. Q. Chaudhary Muhammad Asim Rasheed, "Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications," 03 2017. [Online]. Available: https://www.researchgate.net/publication/315512136. [Accessed 04 04 2023].

[5] A. S. S. G. Muhammad Rizwan Ghori, "VANET Routing Protocols: Review, Implementation and Analysis," 12 2017. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1049/1/012064. [Accessed 27 07 2023].

[6] [Online]. Available: http://www.scirp.org/journal/ijcns. [Accessed 23 10 2023].

[7] O. O. M. A. Arif Sari, "Review of the Security Issues in Vehicular Ad Hoc Networks (VANET)," 30 12 2015. [Online]. Available: http://dx.doi.org/10.4236/ijcns.2015.813050. [Accessed 12 08 2023].

[8] I. S. A. Z. K. K. Shawal Khan, "Security Challenges of Location Privacy in VANETs and State-of-the-Art Solutions: A Survey," 10 04 2021. [Online]. Available: https://doi.org/10.3390/fi13040096. [Accessed 09 09 2023].

[9] S. R. D. Arun Singh Kaurav, "Detection and prevention from different attacks in VANET: A Survey," 03 2021. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-

6596/2040/1/012017. [Accessed 05 05 2023].

[10] M. K. Zehra Afzal, "Security of Vehicular Ad-Hoc Networks (VANET): A survey," 12 2019. [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/1427/1/012015. [Accessed 12 03 2023].

[11] A. S. M. N. M. W. K. N. F. K. A. a. N. H. R. Mohammed Ali Hezam Al Junaid, "Classification of Security Attacks in VANET: A Review of Requirements and Perspectives," 23 02 2018. [Online]. Available: https://doi.org/10.1051/matecconf/201815006038. [Accessed 26 06 2023].

[12] A. S. K. Irshad Ahmed Abbasi, "A Review of Vehicle to Vehicle Communication Protocols for VANETs in the Urban Environment," 31 01 2018. [Online]. Available: https://www.mdpi.com/1999-5903/10/2/14. [Accessed 23 03 2023].

[13] D. M. Kiho Lim, "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks," 04 2016. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2214209616000115. [Accessed 09 05 2023].

[14] G. Samara, W. A. Al-Salihy and R. Sures, "Security Analysis of Vehicular Ad Hoc Nerworks (VANET)," 15 11 2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5635665. [Accessed 29 06 2023].

[15] M. B. P. Q. Richard Gilles Engoulou, "VANET security surveys," 15 05 2014. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0140366414000863. [Accessed 30 05 2023].

[16] J. B.-O. M. H. Mohamed Nidhal Mejri, "Survey on VANET security challenges and possible cryptographic solutions," 04 2014. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2214209614000187. [Accessed 03 08 2023].

[17] H. P. D. Nguyen and R. Zoltán, "The Current Security Challenges of Vehicle Communication in the Future Transportation System," 08 11 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8524773. [Accessed 24 07 2023].

[18] M.-S. H.-P. C. Chun-Ta Li, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," 07 2008. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0140366407005154. [Accessed 19 09 2023].

[19] J. Sun, C. Zhang, Y. Zhang and Y. Fang, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," 15 01 2010. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5383352. [Accessed 20 02 2023].

[20] J. Sun, C. Zhang and Y. Fang, "An ID-based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks," 22 02 2008. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4454834. [Accessed 11 06 2023].

[21] J. Guo, J. P. Baugh and S. Wang, "A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework," 27 09 2007. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4300813. [Accessed 19 04 2023].

[22] Z. L. Z. W. B. Wenshuang Liang, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trends," 31 08 2015. [Online]. Available: https://journals.sagepub.com/doi/full/10.1155/2015/745303#tab-contributors. [Accessed 23 09 2023].

[23] M. S. M. K. N. &. R. B. M. N. Syed Adeel Ali Shah, "Unicast routing protocols for urban vehicular networks: review, taxonomy, and open research issues," 14 07 2014. [Online]. Available: https://link.springer.com/article/10.1631/jzus.C1300332. [Accessed 08 10 2023].

[24] R. H. Y.-S. C. A. I. &. A. H. Sherali Zeadally, "Vehicular ad hoc networks (VANETS): status, results, and challenges," 09 12 2010. [Online]. Available: https://link.springer.com/article/10.1007/s11235-010-9400-5. [Accessed 12 10 2023].

[25] R. Kaur, T. P. Singh and V. Khajuria, "Security Issues in Vehicular Ad-Hoc Network(VANET)," 02 12 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8553852. [Accessed 29 06 2023].

[26] F. Qu, Z. Wu, F.-Y. Wang and W. Cho, "A Security and Privacy Review of VANETs," 17 06 2015. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7127003. [Accessed 07 07 2023].

[27] A. A.-H. M. A. E.-N. Ahmed H. Salem, "The Case for Dynamic Key Distribution for PKI-Based VANETs," 16 05 2016. [Online]. Available: https://arxiv.org/abs/1605.04696. [Accessed 09 06 2023].