VANETS BASED TRAFFIC SIGNALS CONTROLLING WITH ENHANCED SECURITY MODULE (ESM) IN SMART CITIES

Hariharasudhan V

School of Electronics Engineering (SENSE), VIT,
Chennai, TamilNadu 600127, India
hariharasudhan.v2014@vit.ac.in

Dr. P. Vetrivelan

School of Electronics Engineering (SENSE), VIT,
Chennai, TamilNadu 600127, India
vetrivelan.p@vit.ac.in

Abstract

VANET is an emerging platform that enables the inter-communication between the vehicles on-road to exchange control and data messages which can be used to take decisive actions to improve user applications such as congestion and traffic monitoring, secure messaging, and general-purpose Internet connectivity. It does not have a fixed infrastructure and uses wireless, multi-hop communication channels with nodes. The main bottlenecks in implementing a rigid security protocol in VANET applications are the absence of coordinated transmission and the fixed network topology in the VANET. The wireless medium requires various safety applications for the passengers. The availability of the pervasive computing infrastructure paves various paths for security vulnerability. Data security is a concern not only in the vehicular network but also in almost all networked systems, especially wireless networks. The network is vulnerable to compromising key pointers in the system such as confidentiality, integrity, authenticity, and privacy (CIAP). Compromising the CIAP parameters will provide access to any level of control over the network. The paper introduced a secure robust framework to establish the network and enable data communication in VANET using an enhanced RSA algorithm for ESM (Enhanced Security Module) model. The optimized LEACH cluster-based routing algorithm is also used to reduce energy consumption as well as to enhance the security of the data.

Keywords: **VANET Security; RSA algorithms; access control; cryptography; confidentiality; Enhanced Security Module (ESM)**

1. Introduction

VANET is not a future technology anymore. There has been enough research made in the field of VANET to make the Quality of Service and the user experience much better than in the last two decades. It evolved as an inevitable technology in the field of Intelligent Transport Systems and autonomous vehicles. As the trend for the network is scaled up, the risk of potential security attacks also increases. Because the data exchanged between the user and the infrastructures can risk exposing the user data to the potential attacker. If the attacker can tap into the data communication channel, he/she will not only be able to monitor the data but also can modify the data. This middleman attack can compromise the system and user safety. Data security is a vital element in any networked system, and this can be achieved with various technologies, based on the use case and the real time scenario. The network security technologies are developed and keep evolving day by day to prevent such network attacks and it is expected to keep the technologies. Developments in technologies like machine learning, data science, and Artificial intelligence require a lot of contextual data to be collected from the real time system to train and execute the system autonomously. This adds up to the risk of the data ending up in the wrong hands while collecting, transporting, and processing it.

As far as the network topology is concerned, there is no fixed topology for the VANET. Since the nodes in the VANET can move from one network to another network and one node needs several other nodes in the network to relay to or fetch the information to/from the intended node. Therefore, data security is a vital requirement in dynamic and wide networks such as VANET. The rapid wide spanning of the network requires a robust security architecture that should be immune to security threats and less to zero vulnerability. This ensures the confidentiality, integrity, and availability of data and the service when required. Improvising data and information

security is a multi step process. In this approach of designing the security architecture, the architect should take care of identifying the critical elements like entities, vulnerabilities, bugs, threat sources, potential impacts, and corresponding controls possible. The effectiveness of security robustness is then assessed. Another important aspect of data security is there should not be any compromise on user privacy. In the context of VANET, it includes information about the vehicle and the driver him/herself.

While designing the security mechanism, it must be taken care that only the essential information should be made available and also for legitimate use only. The Man in the Middle should not be able to look into or modify the data that is being exchanged.

There are two possible ways to interfere with network communication:

- Introducing a malicious node into the network
- Infect the existing node in the network

1.1 Attacks in VANETs

The security mechanism should be robust enough to detect both of these scenarios. Data security requires three major core concepts. They are Confidentiality, Integrity and Availability. This is also termed as “CIA Triad.” If any of these three elements are compromised, the others are also more likely to be compromised. The security mechanism must ensure to establish a robust framework to make the three elements tamper proof. Some of the sample attacks are discussed in figure 1.

On Vehicular networks, there are several sorts of cyberattacks that can be classified as follows: -

- Denial of Service (DoS) attacker: It prevents essential information from reaching its destination by seizing control of automobile capabilities or disrupting the Traffic related Network's communication link.
- Sybil assault: In this technique, the adversary requires a large number of pseudonymous to persuade automobiles to consider a better course and informs additional trucks about just the congestion by suggesting that there are more than 100 trucks beyond.
- Replay Assault: This attack confuses investigators and hinders vehicle recognition in blockbuster accidents by reproducing earlier data transmissions to take advantage of the statement's conditions and situations of distribution.
- Networking threat: By leveraging the vulnerabilities of network topology routing algorithms, this threat either disrupts the program's packet transmission or falls down data. The most prevalent routing vulnerabilities in VANETs are Black, Warm and Gray hole attacks.
- Timing attack: One of the most important needs of VANET is that security messages are transmitted to vehicles at the appropriate times. The timing attack contains many timeslots for the message, resulting in the message being received by a vehicle in an unintended place rather than a safe location.
- Confidentiality attack: The confidentiality methods ensure sensitive and proprietary data from misusing by parties without authorization.
- Integrity Attack: This involves capturing the data and modifying the actual content. This will induce the destination node to take the wrong decision.
- Availability attack: In this attack, the malicious node will try to increase the network traffic such that it will choke the network resources such as channel capacity and the processing power of the server. This results in a commonly known attack called Denial of Service.

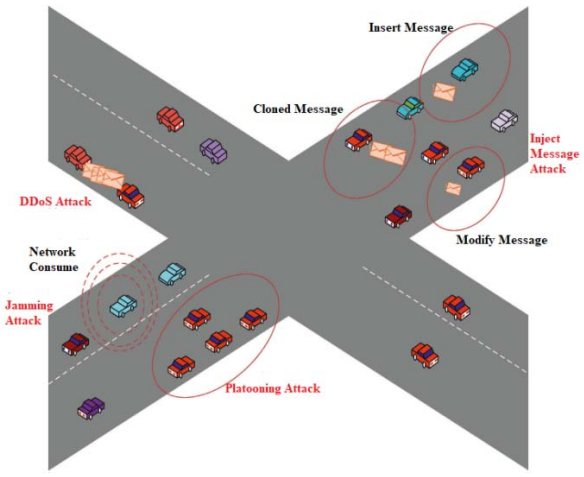

Fig. 1. The Attacks in the VANET.

2. Literature Survey

In this section, we are going to discuss the various security issues on the VANET.

The Manoj [1], introduced the novel method to secure the data using the LEACH protocol clustering along with a cryptography algorithm. They have used the NS2 simulation model to implement the concept in VANET. Their proposed data transmitted mechanism result is compared to traditional security approaches. In the future, a weighting grouping concept incorporating transportation autos will be used to improve the protection of information transfer and central control communication.

Deeksha et al [2], presented a summary of VANET design, as well as a complementary investigation on VANETs, with a focus on security considerations. Furthermore, the pattern of results suggests for those difficulties are taken, as well as a comparative analysis. According to the study, encoding and authenticating play an essential role in VANETs, and numerous scientific directions have been identified for further investigation.

Kabbur et al [3], presented a novel methodology regarding key creation and distribution in VANET. This method is then used with cryptographic technology to protect network packets.

Manickam et al [4], developed a lightweight cryptographic method along with a clustering mechanism to send data securely on VANET. At first, dividing the devices into groups and categorizing the networks by groups appears to be one of the greatest thorough and effective approaches. This technique provides a way to manage cyber-attacks on VANET infrastructure.

Afzal et al [5], covered numerous sorts of privacy difficulties, objectives, assaults, and perpetrators just on VANET, as well as some contemporary methods to overcome security vulnerabilities, as well as their benefits and drawbacks. The VANET attacks are discussed detailed in [6].

Kelarestaghi et al [7], they had explored malicious activity and responses on VANETs as just a mobile node, they initially synthesize the latest research. Furthermore, they examined the security vulnerabilities that arise as a result of the use of various VANET communication systems. They look into security methods to counter competitors' attempts to undermine cryptographic primitives to add to this topic. The VANET trust management tools and techniques are thoroughly described, highlighted by a comparison of cryptographic protocols and trust evaluation in relation to the various types of assaults. The optimization algorithms and VANET solutions were also discussed [8].

Nema et al [9], they have used MATLAB simulation for conducting an RSA cryptographic technique, as well as the implementation of boundaries including double RSU. In VANETs, quite an infrastructure can sometimes be employed to develop improved schemes have been proposed, dissemination techniques, and security mechanisms. MATLAB has the benefits of being readily accessible, often maintained, and having a larger influence.

Liang et al [10], presented a method for optimizing the scheduling algorithm. To limit the likelihood of an inappropriate cluster member dispersal, the adequate number of neighboring nodes is estimated based on comprehensive energy utilization in around. The results are represented in the form of a geometric schematic.

Javed et al [11], begin by looking at the international organization for standardization (ITS) network infrastructure. They further use an actual experiment to build Elliptic curve cryptography based digital certificates and encoding algorithms and complete a comprehensive benchmarks analysis to assess their reliability, which is dependent on aspects including packet sizes, clock speed, and data security.

Branquinho et al [12], recommended system is connected Road Side Units (RSUs), which have been updated us about the state of road intersections, with cars in redistributing intelligence about individuals in road intersections to automobiles. RSUs verify the warning messages that disseminate to discourage inaccurate information from spreading, and all cars may authenticate their identities. This necessitates stringent security procedures, including such non-repudiation of alarm communications, and also stringent real-time prerequisites, such as a threshold communication validating latency bring a target intersection.

Mohamed et al [13], reviewed a recent advancement of VANETs, which includes the structure and set of VANETs as well as the data protection concerns that must be addressed in addition to making those networking safe to use in operation. It analyses and summarizes all recognized security vulnerabilities in VANETs from a mathematical standpoint. It also gathers, investigates, and contrasts the numerous cryptography algorithms which have been offered individually for VANETs, assesses the efficacy of recommended techniques, and examines certain future events which might affect cryptographic techniques development for intelligent transportation.

Mejri et al [14], described the structure and set of VANETs and discussed the confidentiality issues that must be addressed for such networking to be feasible. It examines the different the various encryption strategies proposed for VANETs, as well as a few emerging developments which might influence authentication scheme experiments for connected vehicles.

Qin et al [15], introduced a lightweight decryption-based access control as well as an authentication method to share the data in a secure manner. In this method, they extend the elliptic-curve cryptography-based attribute-based encoding method. Additionally, they have applied token-based decryption in order to offer a lightweight access control mechanism for vehicular data.

Sookhak et al [16], introduced a new approach that relies on the parametric coupling to handle the metadata challenge and delegation of information systems to a Trusted Third Party (TPA). To do this, they employ cloud - based applications, which is the most popular platform in the convenience technologies and applications, to maintain enormous amounts of information and effectively complete the re-encryption processes.

Shen et al [17], developed a data-sharing mechanism that supports both efficient data updates as well as the stochastic nature of VANETs. To assure convenient and effective VANETs, the symmetrical imbalanced randomized complete block architecture (SBIBD) in computational mathematics is developed, while the notion of deindividuating concealment is used to promote appropriate encryption upgradation.

From these surveys, only a little research is done to enhance the data security using RSA. Hence, we are planning to propose a novel method to enhance the security of VANET data' using an enhanced RSA algorithm. In addition, for the selection of nodes, we are using an optimized LEACH clustering protocol to reduce energy usage and enhance the data security in a VANET environment.

3. Proposed Technique

In this section, we are going to secure the VANET communication in the WSN by implementing an enhanced RSA scheme of algorithms that will be clearly stated in Algorithm 1. The perpetrators are probably mentally captured to the genuine sensor cars in protection examinations, but the real automobiles do not have good protection, and therefore intruders effortlessly usurp the false terminals and gain access to all the information. Consequently, to separate the trustworthiness components, we used an optimization process called the Randomized Firefly (RFS) Strategy with Cluster formation in our improved cryptographic protocol. With the help of a trust-based frame, the packets relaying of the sensing devices are managed correctly and promptly, depending on the trustworthiness of nearby vehicles with remote communications.

The enhanced RSA scheme is used to discover the dependability components in the routing protocol and is used to encrypt downlink from a source to a recipient who is requesting it.

3.1 Clustering based routing

The clustering chiefs should choose an automobile node within every cluster during the cluster building procedure. The node sends a clear signal to the cluster head, though in a multi-hop configuration, all vehicle nodes relay respective data to the neighbor nodes. The cluster organization is critical to the cost reduction of a cluster-based sensor node, wherein cost refers to the expenditure of setting up and maintaining the network system. The routing algorithm is vitally important in this clustering concept, and we use the LEACH protocol in our research. Its purpose is to reduce energy usage by aggregating data and reducing transmission to a ground station.

Reduce the power consumption needs to create and maintain the Number Of clusters to extend the lifespan of WSN [18]. The LEACH platform's functioning is divided into several cycles, each of which has two phases: The set-up Process & Sustained Process. It employs the round with a unit, with every round consisting of a clustering set-up phase and sustained hoarding to save resources when forming a new clustering. The non-cluster anchor components are shown in Figure 2 as part of the LEACH-based clusters construction phase. Obtain the cluster head announcement and thereafter submit a proposal to the applications that belong to the cluster head members.

3.2 Reliability node selection

The RFF optimization technique is often used to optimize clustering nodes in order to improve node robustness [19]. The real issues are starting from either the generator node to the destination node and getting an improved path that can find the destination cluster. The number of sensor nodes that allow the regular station to rebroadcast the very last transmission should be kept within an acceptable distance. The optimum clustered nodes and their fundamental motivation are explained further down.

3.3 Randomization algorithm

In [20], they have presented a firefly technique that emphasizes the social behavior of dragonflies inside the tropical cloudless sky. Bioluminescence featuring varied flickering sequences is used by FFs to communicate, hunt for victims, and attract mates. The way FF acts in a broad sense throughout the early spring sky in tropical and tranquil places, the blinking beacon of dragonflies is a spectacular sight. There were around 2,000 species of fireflies, as well as the majority of them produce short, melodic flashing. Flashing lights are typically something for unique animal species. The spontaneous FF Randomization mechanism is used as a component of the attractiveness concept. In principle, the FF mechanism has many constraints, including as

(1) Because one firefly would be transformed into multiple fireflies with very little regard for its anatomy, FF is generally androgynous.
(2) The desirability is dependent on the wavelength, and it decreases as the distance between them grows. This will change its direction when there is nothing more remarkable than just an express firefly.

3.4 Objective function

The ideal approach determines the probability of failure again from the "i" number of vehicle units specified to tackle the objective function. The information is transported in an optimal way when something is acknowledged by the ideal nodes. Communication should have the fewest number of nodes possible. This capability is based on

$$R_{Network} = \sum_{i=1}^{X} Prob(FR). \quad (1)$$

Where,

$$Prob(FR) = \Pr(CN) * \Pr(IN). \quad (2)$$

The dependability is evaluated by using CN and IN as clustering subgroup clusters & inability subgroup clusters, respectively. The path to maintaining dependability with lowering time has been established. It is determined by intended and unintended trustworthiness values. Because the dependability of a WSN node is determined by the configuration of its components, if one of them fails, the complete network fails.

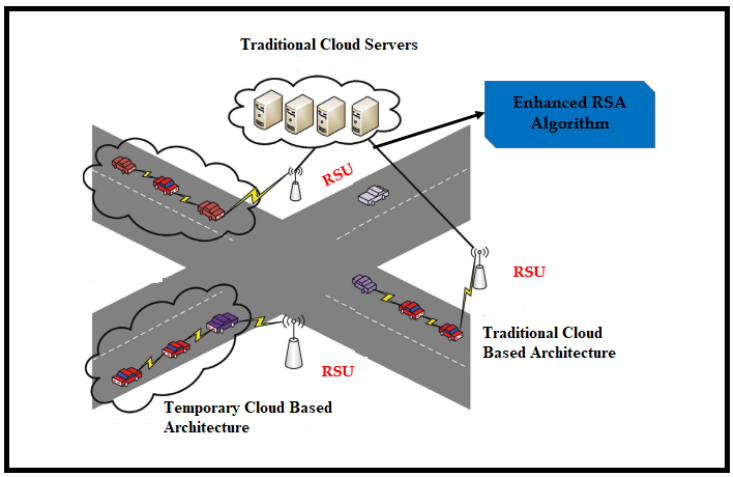

Fig. 2. The Proposed Architecture of the System.

3.5 Enhanced RSA algorithm

In this section, we'll tweak the classic RSA technique by putting one extra prime integer into the key creation procedure. For the suggested mechanism, p, q, and r are prime numbers, n is a generic module, E is a public key, D is a private key, and M appears to be the original message. n, which is dependent on the value of three prime numbers, is used in the E, D variable. E isn't directly measured, but E1 must be known before E can be discovered, which is dependent on two separate parameters, e1 and e2. The exact working flow of the RSA algorithm is explained in figure 3. This Enhanced Security Module provided better security and the security problems in the VANET can be addressed.
The Pseudocode of ERSA,

- **Vehicle Registration at RSU**
  V $\longrightarrow$ RSU: M = (M, ID_{RSU}, TimeStamp, C, X_{pos}, Y_{pos}, E(ID_V, P_{RSU}))
- **RSU Reply for a Registration**
  RSU $\longrightarrow$ V: E(M) = (M, ID_{RSU}, TimeStamp, C, X_{pos}, Y_{pos}, E(PID_V, PR_{RSU}))
- **RSU Broadcast a Message**
  RSU $\longrightarrow$ M, ID_{RSU}, TimeStamp, C, X_{pos}, Y_{pos}
- **Encode a Data using ERSA**
  V $\longrightarrow$ RSU: C = (M, ID_{RSU}, TimeStamp, C, X_{pos}, Y_{pos}, ERSA(DATA, P_{RSU}))
- **Decode a Data using ERSA**
  RSU $\longrightarrow$ V: D(C) = (M, ID_{RSU}, TimeStamp, C, X_{pos}, Y_{pos}, DRSA(C, PR_{RSU}))

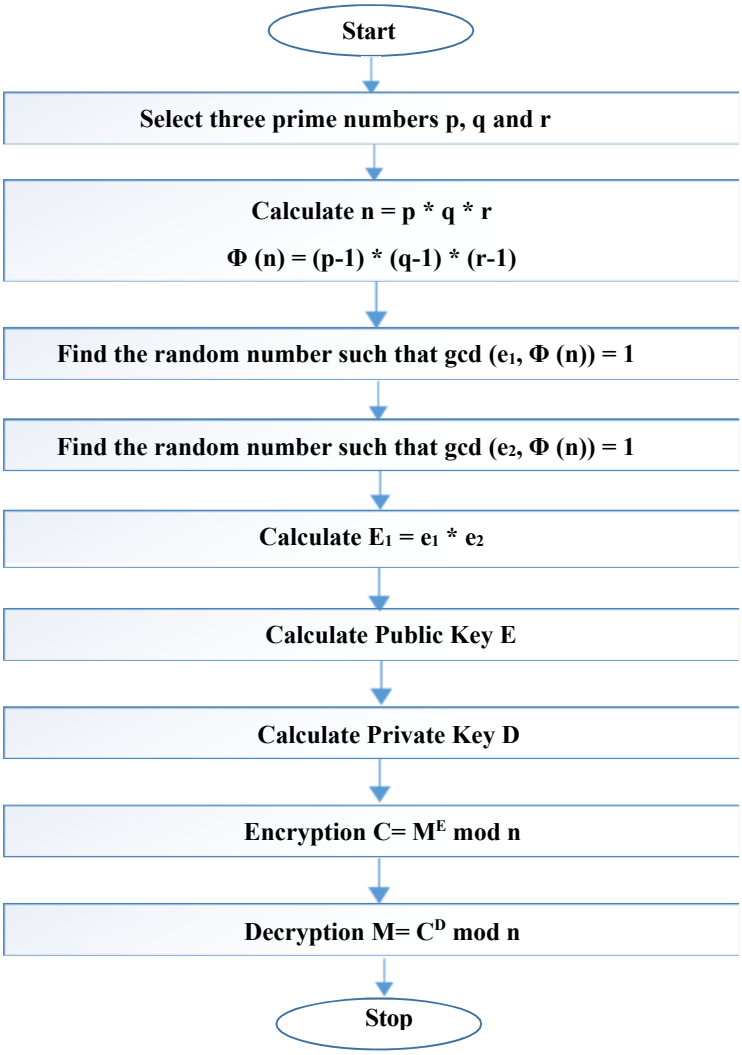

Fig. 3. The Process of enhanced RSA Algorithm.

This algorithm plays a very important role in the proposed method because all the vehicular data are encrypted before sending into the cloud.

4. Implementations

The issue addressed in this section is 'how VANET researchers will assess their proposed method'. Outdoor experimentation is the greatest assessment system; however, this option has several limitations. In real-world circumstances, having many vehicles is neither straightforward nor inexpensive, especially about community security procedures. Analyzing effectiveness in decentralized manner networks, such as VANETs, is challenging. It's ridiculous to evaluate different methodologies in almost the same circumstances. As a result, statistical models are the sole specific assessment instrument. Simulation software is made up of two parts: a network model and a routing algorithm. The routing algorithm is in charge of determining the telecommunication stack, which includes the wireless channel prototype, antennas framework, MAC layer, network layer, application layer, and other related concerns. VANET statistical models have used the same networking paradigm as MANET software systems [21].

Impediments in automobile maneuverability and the wireless channel should have been included in the experiment. Autonomous navigation patterns: Operators communicate with respective surroundings not just in terms of static obstacles, but as well as in response to variations obstacles like other vehicles and pedestrians. Human behaviors: Motorists are not machinery; they are humans. All operating simulations ought to be deterministic, with a threshold for inaccuracies, so that anticipated catastrophes can be avoided. Vehicle arrangement that isn't spontaneous: The initial placements of automobiles in the simulated region are not homogeneously dispersed, as can be seen in actual situations [21].

5. Results and Discussions

This section of the study discussed the effectiveness of the augmentation initiatives; some performance evaluations were used and compared to existing schemes. The suggested system was implemented in the Java programming language using JDK 1.9 on a Windows machine with the following configurations: Intel (R) Core i5 CPU, 2.6 GHz, 8 GB RAM, and Windows 10 as the OS.

Implementation Parameters:

Parameters	Values
Number of nodes	50/100/150/200
Area size	1000 m × 1000 m
Packet size	512 bytes
Network protocol	IPV4
Traffic source	CBR
Rate	60 kbps
Transmission range	250 m
Routing protocol	LEACH-RFF, LEACH, AODV-FF

Number of vehicles	PDR (%)	NLT(h)	Encryption time (s)	Decryption time (s)	Clustering level (%)	Security (%)
50	95.4	117	17.76	18.98	89.82	96.67
100	93	122	21.48	28.6	91.45	88.67
150	86.4	128	27.24	32.98	94.76	91.45
200	81.56	139	31.56	36.93	92.92	89.2

Table 1. VANET Security Measures

5.1. Reliability analysis

The validity and reliability for several node mobilities are shown in Figure 4. This research analyzes the suggested (LEACH-RFF) to the LEACH-FF and AODV-FF models. For the serviceability investigation, we use 50-200 vehicle clusters. In comparison to other methodologies, the suggested model (LEACH-RFF) determines the strongest serviceability clusters, according to the research.

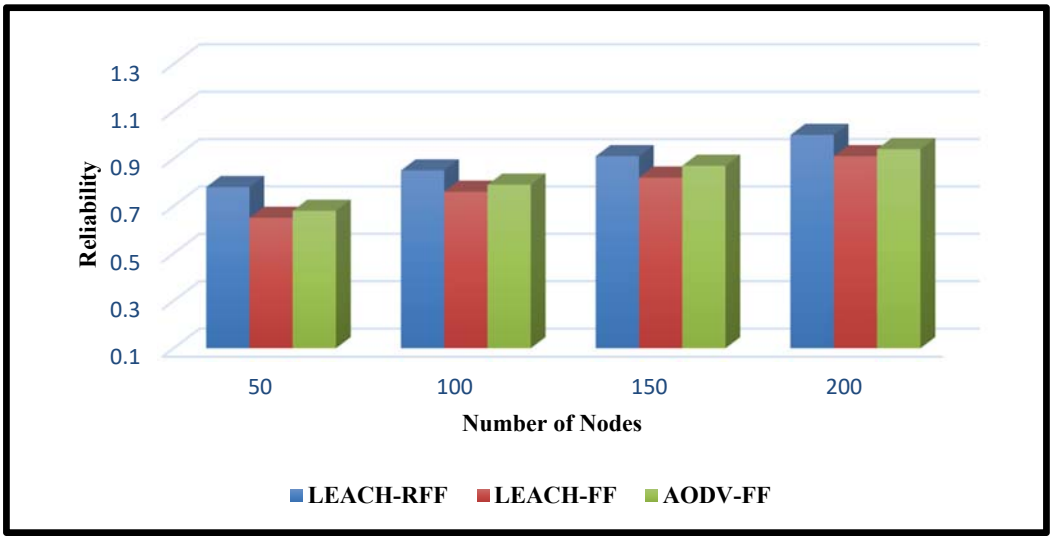

Fig. 4. The Reliability Analysis of the Proposed Method

Table 1 depicts the findings of evaluation metrics which include PDR and NLT for the proposed system depending on the number of automobiles. It contains encryption, decryption time, clustered level, and security accomplished in %. For a smaller number of motor vehicles, the encryption and decryption times are faster. Due to the general optimization technique, the decrypted level becomes optimal, and privacy also becomes optimal (high level) for each study. The vehicle nodes were grouped optimally using the LEACH technique, and the optimum dependability network analysis was discovered.

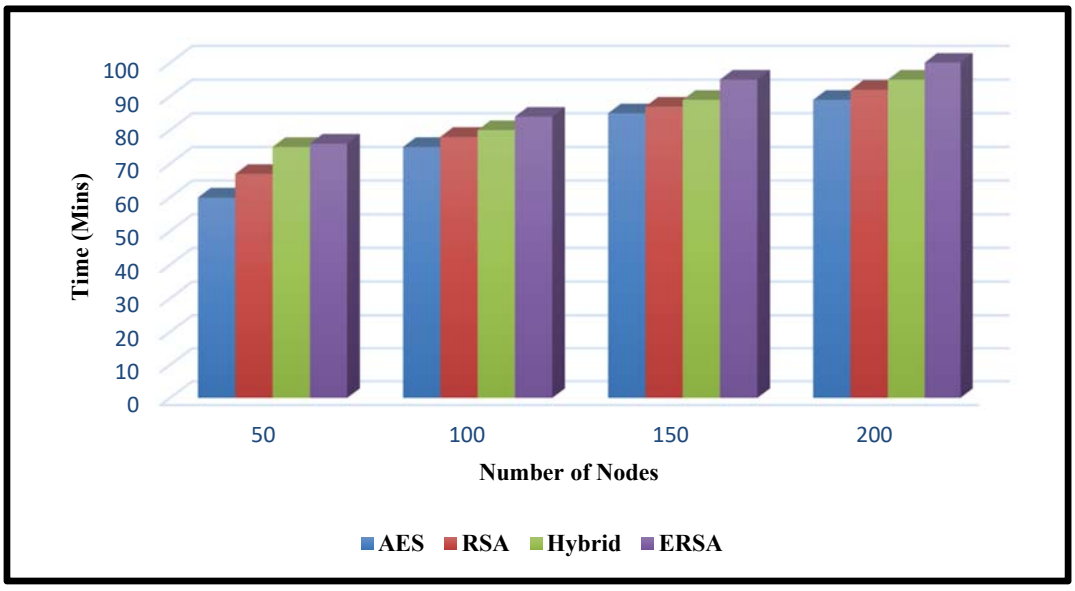

Fig. 5. Network Lifetime Analysis

The System Lifetime for quite a number of motor vehicles is depicted in figure 5. In comparison to AES, RSA and Hybrid [22], it shows that enhanced RSA algorithm with hashing algorithm performed best. Figures 6 and 7 depict the ideal ERSA-hash algorithm output (proposed). Furthermore, the research design ensures that VANET data is kept secure and that automotive routers are more reliable.

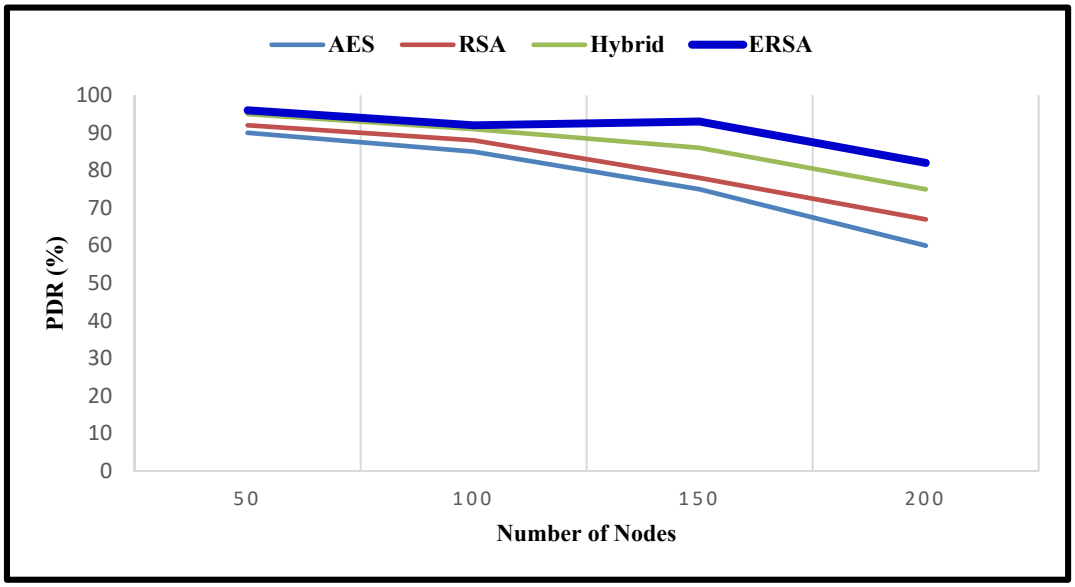

Fig. 6. The Packet Delivery Analysis

Figure 8 depicts the stability period depending on the attacks of a few different adversaries. If the number of sensor nodes grows, NET will want more for each adversary. It clearly states that the proposed method takes more time to attack the node depending on the number of adversaries.

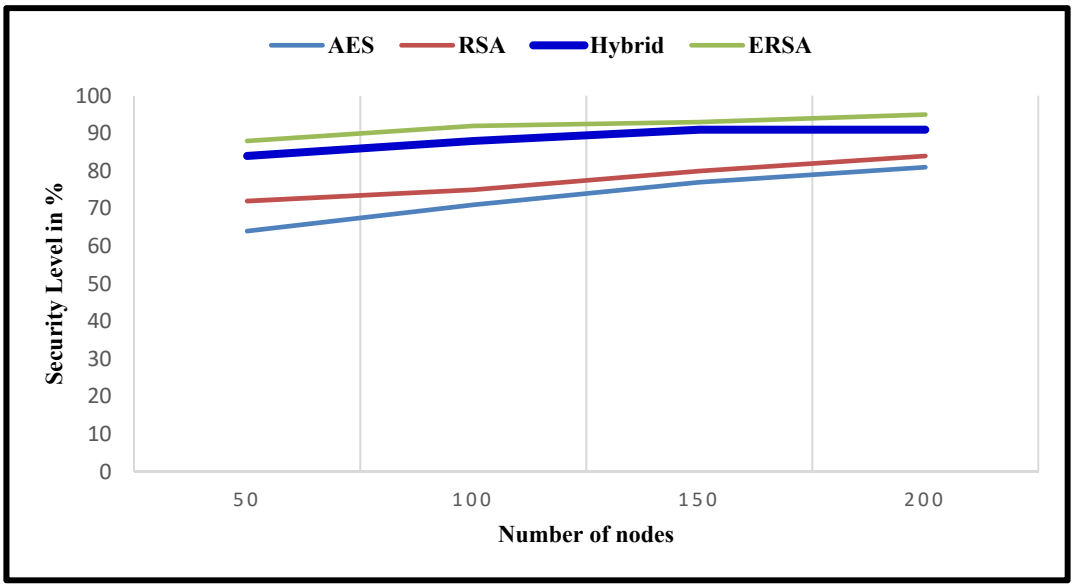

Fig. 7. Security Analysis of the Proposed Method

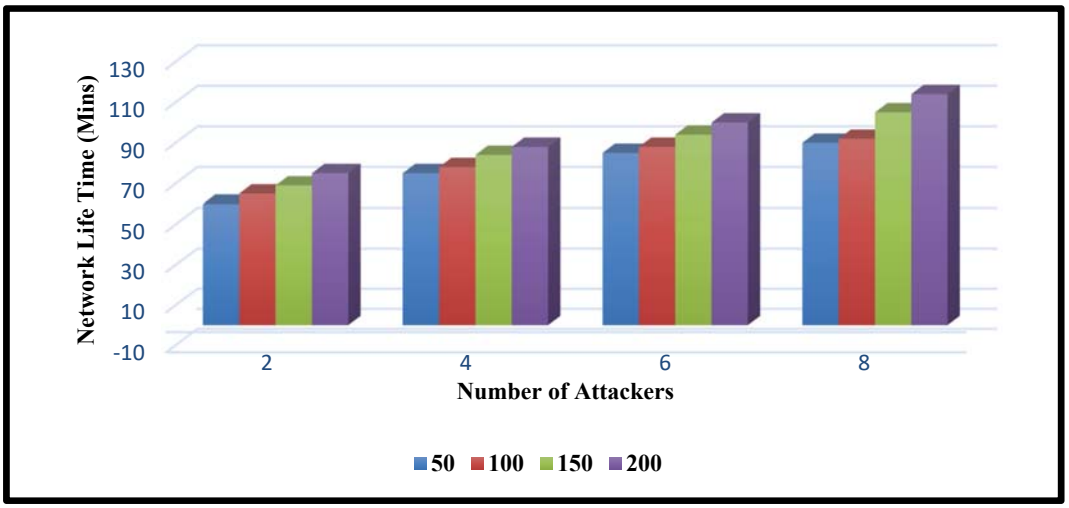

Fig. 8. Attack Analysis of the Proposed Method

6. Conclusion And Future Work

We investigated the Enhanced RSA Hash optimization method for enhancing the security of the VANET node in this article. The data that was safely delivered, as well as the misbehaviors, were both decisively detected. When a malicious or unauthorized station is detected on the networks, the data is routed to the next authorized nodes by disengaging the problematic node. To avoid this noxious component in the safe data transfer scheme, we used the optimized LEACH protocol to identify trustworthy vehicles. Our proposed approach is analyzed to AES, DES, and Hybrid techniques with some prerequisites including NLT, PDR, and security based on the working as intended.

In the future, a weight-based clustering model going to be inbuilt with the vehicles in order to improve the security of data transfer and traffic control systems and also implement a Digital certificate and Software Security module.

Conflicts of interest

"The authors have no conflicts of interest to declare"

References

[1] Manoj Priyatham, "Light Weight Cryptography for Secure Data Transmission", International Journal of Engineering Trends and Applications (IJETA) – Volume 7 Issue 5, Sep-Oct 2020
[2] Deeksha, Kumar, A., & Bansal, M. (2017). A review on VANET security attacks and their countermeasure. 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), 580-585.
[3] Kabbur, M.S., R, A., & Kumar V, A. (2021). MAR Security: Improved Security Mechanism for Emergency Messages of VANET using Group Key Management & Cryptography Schemes (GKMC). International journal of Computer Networks & Communications.
[4] Manickam, P., Shankar, K., Perumal, E., Ilayaraja, M., & Sathesh Kumar, K. (2019). Secure Data Transmission Through Reliable Vehicles in VANET Using Optimal Lightweight Cryptography. Advanced Sciences and Technologies for Security Applications.
[5] Zehra Afzal and Manoj Kumar 2020 J. Phys.: Conf. Ser. 1427 012015
[6] Arun Singh Kaurav and Sushama Rani Dutta 2021 J. Phys.: Conf. Ser. 2040 012017
[7] Kelarestaghi, K.B., Foruhandeh, M., Heaslip, K., & Gerdes, R.M. (2019). Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures. ArXiv, abs/1903.01541.
[8] Muhammad Sameer Sheikh, Jun Liang and Wensong Wang, Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey, Wireless Communications and Mobile Computing, 5129620, 2020, https://doi.org/10.1155/2020/5129620
[9] Nema M, S. Stalin and R. Tiwari, "RSA algorithm based encryption on secure intelligent traffic system for VANET using Wi-Fi IEEE 802.11p," 2015 International Conference on Computer, Communication and Control (IC4), 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375676.
[10] Liang, H., Yang, S., Li, L. et al. Research on routing optimization of WSNs based on improved LEACH protocol. J Wireless Com Network 2019, 194 (2019). https://doi.org/10.1186/s13638-019-1509-y
[11] Javed, M.A.; Ben Hamida, E.; Znaidi, W. Security in Intelligent Transport Systems for Smart Cities: From Theory to Practice. Sensors 2016, 16, 879. https://doi.org/10.3390/s16060879
[12] Branquinho, J.; Senna, C.; Súquete, A. An Efficient and Secure Alert System for VANETs to Improve Crosswalks' Security in Smart Cities. Sensors 2020, 20, 2473. https://doi.org/10.3390/s20092473
[13] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi, Survey on VANET security challenges and possible cryptographic solutions,Vehicular Communications, Volume 1, Issue 2, 2014, Pages 53-66, https://doi.org/10.1016/j.vehcom.2014.05.001.
[14] Mejri M.N and Hamdi M, "Recent advances in cryptographic solutions for vehicular networks," 2015 International Symposium on Networks, Computers and Communications (ISNCC), 2015, pp. 1-7, doi: 10.1109/ISNCC.2015.7238573.
[15] Qin, X., Huang, Y. & Li, X. An ECC-based access control scheme with lightweight decryption and conditional authentication for data sharing in vehicular networks. Soft Comput 24, 18881–18891 (2020). https://doi.org/10.1007/s00500-020-05117-x
[16] Sookhak, M., Yu, F.R., Tang, H. (2017). Secure Data Sharing for Vehicular Ad-hoc Networks Using Cloud Computing. In: Zhou, Y., Kunz, T. (eds) Ad Hoc Networks. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 184. Springer, Cham. https://doi.org/10.1007/978-3-319-51204-4_25
[17] Shen J, T. Zhou, J. Lai, P. Li and S. Moh, "Secure and Efficient Data Sharing in Dynamic Vehicular Networks," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8208-8217, Sept. 2020, doi: 10.1109/JIOT.2020.2985324.
[18] Manickam P et al (2015) A highly adaptive fault tolerant source routing protocol for energy constrained mobile ad hoc networks. Int J Appl Eng Res 10(7):16885–16897. ISSN 0973-4562
[19] Shankar K, Eswaran P (2015) ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm. Int J Appl Eng Res 10(5):1841–1845
[20] Wu W, Wu S, Zhang L, Zou J, Dong L (2013) LHash: a lightweight hash function (full version). IACR Cryptology ePrint Archive, 2013, p 867
[21] Hasrouny H, Samhat AE, Bassil C, Laouiti A. Trust model for secure group leader-based communications in VANET. Wirel Netw 1–23
[22] Chinnasamy, P., Deepalakshmi, P. HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. J Ambient Intell Human Comput 13, 1001–1019 (2022). https://doi.org/10.1007/s12652-021-02942-2

Authors Profile

Hariharasudhan V received a bachelor's degree in Electronics and Instrumentation Engineering from Bharathiar University, Coimbatore, and master's degree in Embedded Systems and Technology from SRM University, Chennai. Currently, he is working as a Principal Engineering Manager in Johnson Controls, Pune. He has 22 years of rich experience in end-to-end product design & development of embedded system controls in automotive domain & Building Automation Technology. His research interests are Wireless sensor networking, VANETs mobility, Embedded Controls, Cloud computing, Data Science and IoT.

Dr.Vetrivelan P, completed Bachelor of Engineering from the University of Madras, Chennai, and both Master of Engineering in Embedded Systems Technologies and Doctor of Philosophy in Information and Communication Engineering from Anna University, Chennai. He is working as a Professor in the School of Electronics Engineering & Assistant Controller of Examinations (ACOE) at Vellore Institute of Technology (VIT), Chennai, India. He has 18.3 years of teaching experience altogether in CSE and ECE Departments in both private Engineering Colleges in Chennai and Private Engineering University in Chennai, respectively. His research interests include Wireless Networks, Adhoc and Sensor Networks, VANETs, Embedded Systems, and the Internet of Things (IoT) with Machine Learning.