Multi Encryption Approach for Privacy Preserving Authentication over VANETs

Pooja Verma, Prof. Rohit Rathore

M.Tech Scholar, Dept. of ECE., Lakshmi Narain College of Technology Excellence, Bhopal, India,

Assistant Professor, Dept. of ECE., Lakshmi Narain College of Technology Excellence, Bhopal, India.

Abstract : Encryption and decryption is the key technique to secure data or information during communication. Multi encryption is the process of encrypting an already encrypted message one or more times, either using the same or a different algorithm. It is also known as multiple encryptions. Data encryption standard (DES), Advance Encryption standard (AES), RSA etc. are common security algorithm. With such algorithm, applying encryption twice even with the same key or different key may make it more secure. A Vehicular Ad-Hoc Network or VANET is a sub form of Mobile Ad-Hoc Network or MANET. VANET can also support other non-safety applications that require a Quality of Service (QoS) guarantee. This paper proposed multi encryption approach for data encryption and decryption sp that Vehicle can perform secure communication. In this work implement security algorithm based on Advance Encryption standard and RSA algorithm and estimate performances.

IndexTerms **– DES, AES, RSA, MANET, VANET, QoS, Security.**

I. INTRODUCTION

In the VANET systems, the leakage of some sensitive data or communication information will cause heavy losses for life and property. Then, a higher security level is required in the VANET systems. Meanwhile, fast computation powers are needed by devices with limited computing resources. Thus, a secure and lightweight privacy-preserving protocol for VANETs is urgent. VANET research is very emerging area for researchers now days. Recent years have witnessed that the new mobility Intelligent Transportation System is booming, especially the development of Vehicular Ad Hoc Networks (VANETs). It brings convenience and a good experience for drivers. Unfortunately, VANETs are suffering from potential security and privacy issues due to the inherent openness of VANETs. In the past few years, to address security and privacy-preserving problems, many identity-based privacy-preserving authentication schemes have been proposed by researchers. However, it is found that these schemes fail to meet the requirements of user privacy protection and are vulnerable to attacks or have high computational complexity. Hence, it is focus on enhancing privacy-preserving via authentication and achieving better performance. Many issues arise when efforts are gathered towards running vehicular ad hoc networks in an attempt to provide an improvement to driver behavior, with the aim of reducing the number of Fatalities caused by automobile accidents. The main important challenges in VANET and the key challenges from the Technical perspectives are as follows:

Signal fading: Objects placed as obstacles between two communicating vehicles are one of the challenges that can affect the efficiency of VANET. These obstacles can be other vehicles or buildings distributed along roads especially in the cities Bandwidth limitations. Another key issue in the VANET is the absence of a central coordinator that controls the communications between nodes, and which has the responsibility of managing the bandwidth and contention operation.

Connectivity: Owing to the high mobility and rapid changes of topology, which lead to a frequent fragmentation in networks, the time duration required to elongate the life of the link communication should be as long as possible. This task can be accomplished by increasing the transmission power; however, that may lead to throughput degradation. Accordingly, connectivity is considered to be an important issue in VANET, Owing to the small effective network diameter of a VANET that lead to a weak connectivity in the communication between nodes.

Security and privacy: Keeping a reasonable balance between the security and privacy is one of the main challenges in VANET. The receipt of trustworthy information from its source is Important for the receiver.

Routing protocol: Because of the high mobility of nodes and rapid changes of topology, designing an efficient routing protocol that can deliver a packet in a minimum period of time with few dropped packets is considered to be a critical challenge in VANETs.

II. BACKGROUND

D. Zheng et al., [2019] The vehicular ad-hoc networks (VANETs) is one of the most promising application in the communications of smart vehicles and the smart transportation systems. However, authentication and privacy of users are still two vital issues in VANETs. Moreover, in the traditional mode, the transactional data storage provides no distributed and decentralized security, so that the third party initiates the dishonest behaviors possibly. In this work, based on blockchain technique, it is propose a traceable and decentralized the Internet of Vehicle system framework for communication among smart vehicles by employing of a secure access authentication scheme between vehicles and RoadSide Units (RSUs). On the one hand, this scheme allows that vehicles employ pseudonyms for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications anonymously in the non-fully trusted environment. [1]

Z. Wei, et al., [2019] propose an identity-based signature that achieves unforgeability against chosen-message attack without random oracle. In order to reduce the computational cost, it is design two secure and efficient outsourcing algorithms for the exponential operations, where a homomorphic mapping based on matrices conjugate operation is used to achieve the security of both exponent and base numbers. Furthermore, it is construct a privacy-preserving protocol for VANETs by using outsourcing computing and the proposed IBS, where a proxy re-signature scheme is presented for authentications. In the VANET privacy-preserving protocol, TA authorizes RSU to act as an agent and RUS converts OBU's signature into TA's signature, which effectively hides the real identity of vehicle OBU. Meanwhile, TA has access to trace the real identity of OBU using its secret key

when malicious messages are found. Then, the protocol provides anonymity, traceability, and privacy. In addition, with respect to the efficiency, our scheme does not need pairing operations and exponential operations. Thus, the calculation burdens for the VANET system can be significantly reduced.[2]

L. Wu et al., [2019] In this work, first, it is describe the vulnerabilities of the previous scheme. Furthermore, to enhance privacy protection and achieve better performance, it is propose an efficient privacy-preserving mutual authentication protocol for secure V2V communication in VANETs. Through security analysis and comparison, it is formally demonstrate that our scheme can accomplish security goals under dynamic topographical scenario compared with the previous scheme. Finally, the efficiency of the scheme is showed by performance evaluation. The results of our proposed scheme are computationally efficient compared with the previously proposed privacy-preserving authentication scheme.[3]

H. Tan, et al., [2018] In this work, it is address the above issues by developing a secure and efficient authentication scheme with unsupervised anomaly detection. In our design, certificateless authentication technique is deployed for conditional privacy preserving, along with the Chinese remainder theorem for efficient group key distribution and dynamic updating. Subsequently, the corresponding unsupervised anomaly detection method is illustrated, which applies dynamic time warping for distance measurement. The proposed method could remarkably alleviate unnecessary authentication burden in vehicle side. DoS attack can also be prevented in this way. Furthermore, anomaly detection method is conducted by the involving road side units (RSUs), while the contents of the processing traffic flows are kept secret to RSUs during the entire process. Security analysis shows that our scheme can achieve desired security properties. Additionally, performance analysis demonstrates that our design is efficient compared with state-of-the-art.[4]

Z. Lu, et al., [2018] propose a blockchain-based anonymous reputation system (BARS) to establish a privacy-preserving trust model for VANETs. The certificate and revocation transparency is implemented efficiently with the proofs of presence and absence based on the extended blockchain technology. The public keys are used as pseudonyms in communications without any information about real identities for conditional anonymity. In order to prevent the distribution of forged messages, a reputation evaluation algorithm is presented relying on both direct historical interactions and indirect opinions about vehicles. A set of experiments is conducted to evaluate BARS in terms of security, validity, and performance, and the results show that BARS is able to establish a trust model with transparency, conditional anonymity, efficiency, and robustness for VANETs.[5]

A. Deshpande, et al., [2018] present the work which is performed in divided into two stages. In the first stage data is normalized using mean normalization. In second stage genetic algorithm is used to reduce number of features and further multilevel ensemble classifier is used for classification of data into different attack groups. From result analysis it is analysed that with reduced feature intrusion can be classified more efficiently.[6]

C. Sun, et al., [2017] propose a conditional privacy-preserving mutual authentication framework with denial-of-service attack resistance called MADAR. The authentication framework combines different identity-based signature schemes and distinguishes inner-region and cross-region authentications to increase efficiency. Beyond the privacy preservation and non-repudiation achieved by the existing framework, our authentication framework provides asymmetric inter-vehicle mutual authentication and strength-alterable computational DoS-attack resistance. it is have formally proved the privacy preservation, unlinkability, mutual authenticity, and correctness of pseudonym with ProVerif, and analyzed other security objectives. The performance evaluations are conducted and the results demonstrate that our framework can achieve these security objectives with moderate computation and communication overheads.[7]

K. Shim, et al., [2017] A WAVE-based cross-layer anonymous authentication scheme based on a variant of ECDSA (Biswas and Misic "A Cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," IEEE Trans. Veh. Technol., vol. 62, no. 5, pp. 2182-2192, Jun. 2013.) was published for authenticity of vehicular safety application messages. Our result shows that, contrary to what is claimed, the scheme is entirely broken due to the insecurity of their underlying signature scheme: Their modification of ECDSA is insecure against secret key recovery attacks where anyone can recover OBUs' or mobile nodes' private keys from transmitted signed messages just eavesdropping.[8]

U. Rajput et al., [2017] hybrid approach combines the useful features of both the pseudonym-based approaches and the group signature-based approaches to preclude their respective drawbacks. The proposed approach neither requires a vehicle to manage a certificate revocation list, nor indulges vehicles in any group management. The proposed approach utilizes efficient and lightweight pseudonyms that are not only used for message authentication, but also serve as a trapdoor in order to provide conditional anonymity. It is present various attack scenarios that show the resilience of the proposed approach against various security and privacy threats.[9]

H. Zhong et al., [2016] Vehicle Ad hoc NETworks (VANET) can enhance traffic safety and improve traffic efficiency through cooperative communication among vehicles, roadside infrastructure, and traffic management centers. To guarantee secure service provision in VANET, message authentication is important. Moreover, a vehicle user's private information can also be leaked during service provision. A protection mechanism is needed to prevent such leakage. Therefore, it is propose a conditional privacy-preserving and authentication scheme for secure service provision in VANETs. The proposed scheme not only satisfies the security requirements of VANETs, but also optimizes the calculation process of signature generation and verification. it is carry out a detailed comparative analysis. The result shows that the proposed scheme is more efficient than existing schemes in terms of communication overhead and computational cost. Therefore, our scheme is suitable for secure service provision in VANETs.[10]

III. PROPOSED METHODOLOGY

A. Collection of Data

The data will be collected from primary as well as secondary sources. The primary sources of data would be collected through personal observation, discussions questioner and interview with the personnel working at various levels of the organization i.e. from top to operational level officers.

The secondary data sources would be collected from books, articles published in various journals, booklets, annual reports, magazines, web sites etc.

B. Coding and Tabulation

After the interview, the information in the questioner will be edited and after editing the information, each information will be assigning the number. This is known as Code Manual. After the codification of data, the data will be presented in the form of tables depending upon the type of information and requirement of the testing of hypotheses.

C. Analysis and Interpretation of data

Analysis work after tabulation is generally based on the computation of various percentages, coefficients, chi-square test etc., by applying various well defined statistical formulae. In the process of analysis, relationships or differences supporting or conflicting with original or new hypotheses should be subjected to tests of significance to determine with what validity data can be said to indicate any conclusion(s).

D. RSA

RSA is based on one important mathematical phenomenon: the difficulty of factoring large numbers. RSA is a member of the asymmetric encryption algorithms. The public and private keys are derived from a pair of large (min. 200 digits) prime numbers, p and q. Keys are generated as follows:

1. Compute n = pq and z = (p-1)(q-1).
2. Randomly choose the encryption key e, such that e and z are relatively prime.
3. Choose a decryption key d, such that ed mod z = 1. In general, d is calculated with help of the Euclidean algorithm.

Key generation is now completed. The public key is defined as <e, n> and the private key as <d, n>. The two prime numbers p and q are not longer needed and should be discarded. To encrypt a message m, compute c = me mod n. For decryption use m = cd mod n.

E. AES

AES is a variant of Rijndael with a fixed block size. AES ciphers use a 128-bit block and 128, 192 or 256-bit keys. The larger block size helps resist birthday attacks while the large key size prevents brute force attacks. It is efficient in both software and hardware.

The main features of AES are-

- AES does not use network. It uses 10, 12, or 14 rounds.
- 128-bit input/output data block size
- 128, 192, and 256-bits key sizes. The key size depends on the number of rounds.
- AES uses one S-box which takes in 8 bits and outputs 8 bits.

IV. SIMULATIONS RESULTS

The simulation is performed using the MATLAB 8.3 software. Various functions and command are available in MATLAB library.

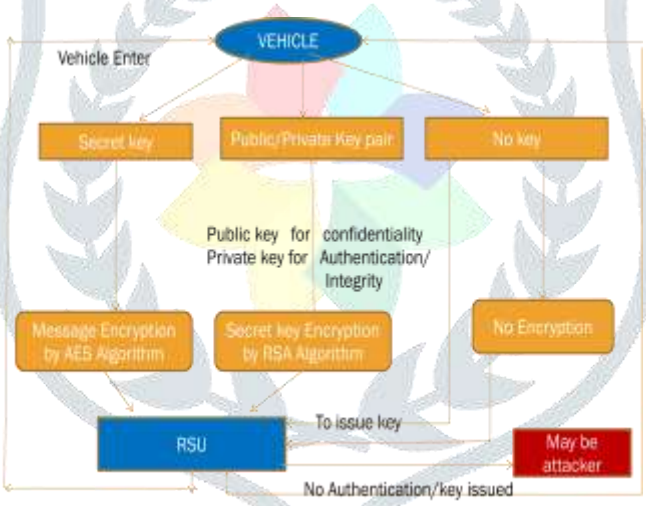


Figure 1: Flow chart of Security Model

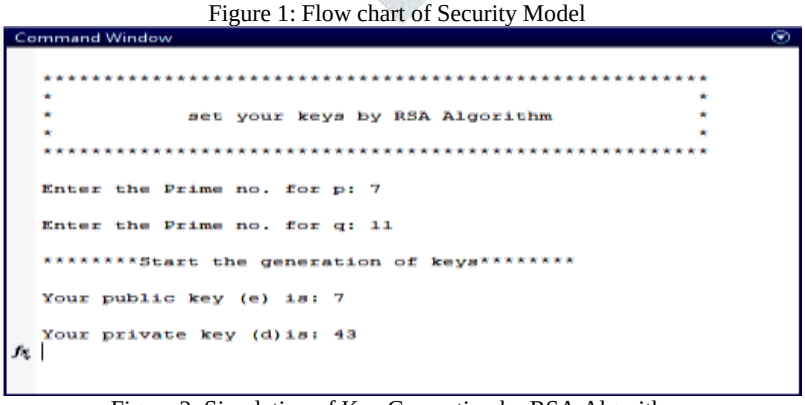


Figure 2: Simulation of Key Generation by RSA Algorithm

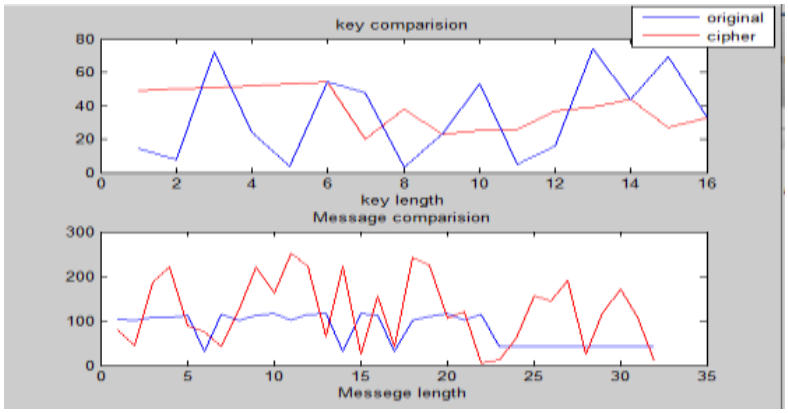


Figure 3: Graph of Original key Vs Cipher key

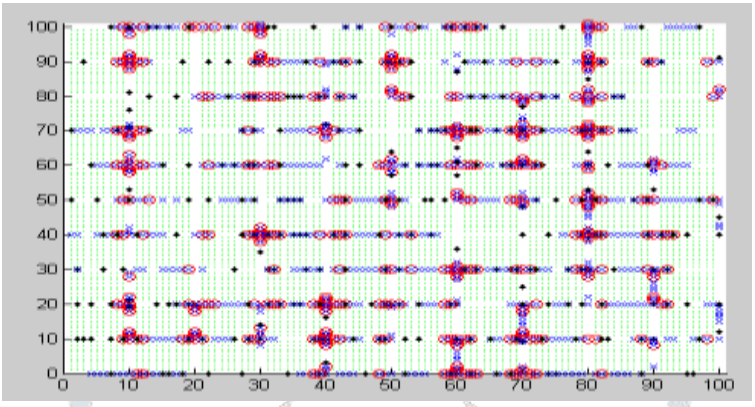
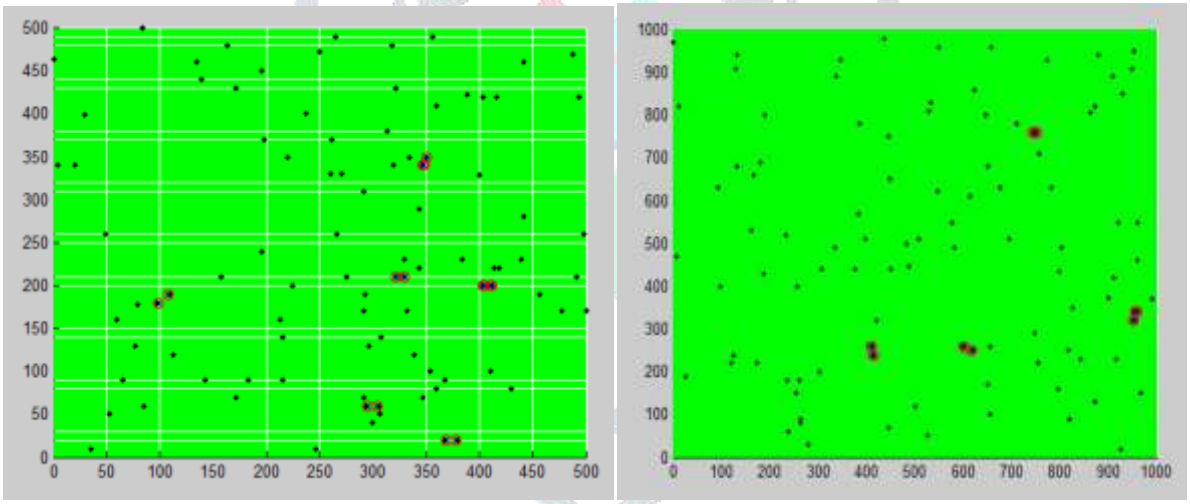


Figure 4: Simulation of VANET (100meter x 100meter area)



(a) (b)

Figure 5: Simulation of VANET

Table 1: Simulation Parameter

Simulator	MATLAB 8.0.3.532
Simulation time	20(s)
MAC layer protocol	802.11
Number of mobile nodes	2
Topology	Mesh
Traffic loading speed	1 CBR packet/s
Routing protocol	AODV
Maximum bandwidth	27 mbps
Traffic	Constant bit rate
Maximum speed	2-10m/s
Packet size	512 bytes
Simulation area	100 m x 100m

Table 2: Comparative execution time (in seconds) and buffer size of encryption algorithms

Input data(bytes)	Method	Computation Time(seconds)		Buffer Size (Bytes)
		Encryption	Decryption	
128	DES	0.5416	0.2007	4096
	AES	0.0424	0.063	6232
	RSA	0.0771	0.0735	448
256	DES	0.8795	0.5232	4324
	AES	0.0303	0.0425	6648
	RSA	0.1474	0.1427	904
512	DES	1.3868	1.1493	6580
	AES	0.0254	0.0474	7480
	RSA	0.3117	0.3451	1736

Table 3: Comparative result analysis of all algorithms with proposed method

Input Size(bytes)	Method	Simulation Time(seconds)		Throughput	
		Encryption	Decryption	(Encryption)	(Decryption)
512	DES	2.8079	1.8732	319.1	478.3
512	AES	0.0981	0.1531	9133.5	5852.4
512	RSA	0.5362	0.5613	1671.1	1596.3
512	Proposed Method	0.1146	0.1144	7818.5	7859.7

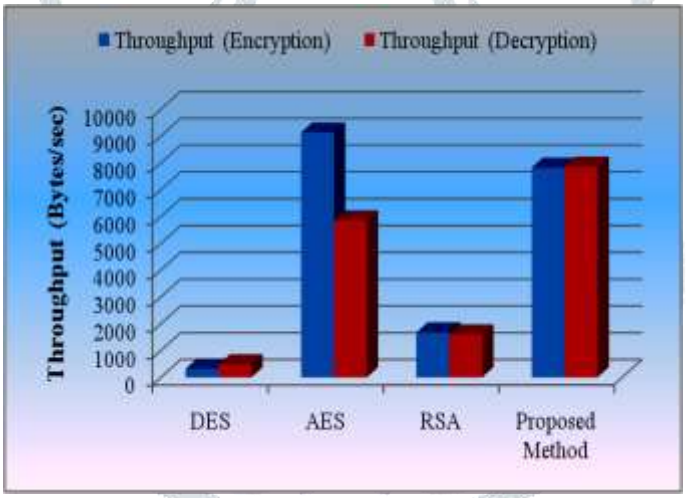


Figure 6: Comparative throughput analyses of all algorithms with proposed method

After seen simulation graph and result it is clear that proposed method gives better result than existing approaches.

V. CONCLUSION

In this paper, security algorithm for VANETs is studied and implemented multi encryption algorithm. Choosing the correct security algorithm providing with appropriate simulation will improve the performance security algorithm in VANETs. MATLAB 8.3 software is using to simulate proposed approach. Simulated results shows that the proposed algorithm gives better performance than previous methods in terms of simulation time, buffer size, security level etc.

REFERENCES

1. Ali, Y. Yang, X. Zeng and Y. Xu, "Periods on the Cascade Connection of an LFSR and an NFSR," in *Chinese Journal of Electronics*, vol. 28, no. 2, pp. 301-308, 3 2019.
2. H. Zhong, L. Pan, Q. Zhang and J. Cui, "A New Message Authentication Scheme for Multiple Devices in Intelligent Connected Vehicles Based on Edge Computing," in *IEEE Access*, vol. 7, pp. 108211-108222, 2019.
3. H. Wang, D. Guo, Q. Wen and H. Zhang, "A Robust Authentication Scheme for Multiple Servers Architecture," in *IEEE Access*, vol. 7, pp. 111222-111231, 2019.
4. T. Zhou, X. Yang, L. Liu, W. Zhang and N. Li, "Faster Bootstrapping With Multiple Addends," in *IEEE Access*, vol. 6, pp. 49868-49876, 2018.

5. X. Jia, D. Wang, D. Nie and C. Zhang, "Collaborative Visual Cryptography Schemes," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 5, pp. 1056-1070, May 2018.
6. A. Deshpande and R. Sharma, "Anomaly Detection using Optimized Features using Genetic Algorithm and MultiEnsemble Classifier", IJOSTHE, vol. 5, no. 6, p. 7, Dec. 2018. https://doi.org/10.24113/ojssports.v5i6.79
7. H. Taha and E. Alsusa, "Secret key establishment technique using channel state information driven phase randomisation in multiple-input multiple-output orthogonal frequency division multiplexing," in *IET Information Security*, vol. 11, no. 1, pp. 1-7, 1 2017.
8. Y. Chen, "Fully Incrementing Visual Cryptography From a Succinct Non-Monotonic Structure," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 5, pp. 1082-1091, May 2017.
9. S. Li, J. Li and D. Wang, "Region Incrementing Visual Cryptography Scheme with Same Contrast," in *Chinese Journal of Electronics*, vol. 25, no. 4, pp. 621-624, 7 2016.
10. M. A. M. Abdullah, S. S. Dlay, W. L. Woo and J. A. Chambers, "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography," in *IEEE Access*, vol. 4, pp. 10180-10193, 2016.
11. M. Poolakkaparambil, J. Mathew, A. M. Jabir and D. K. Pradhan, "A Low-Complexity Multiple Error Correcting Architecture Using Novel Cross Parity Codes Over GF(2^{m})," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 8, pp. 1448-1458, Aug. 2015.
12. T. T. Mapoka, S. J. Shepherd and R. A. Abd-Alhameed, "A New Multiple Service Key Management Scheme for Secure Wireless Mobile Multicast," in *IEEE Transactions on Mobile Computing*, vol. 14, no. 8, pp. 1545-1559, 1 Aug. 2015.
doi: 10.1109/TMC.2014.2362760
13. S. Liu, Y. Hong and E. Viterbo, "Unshared Secret Key Cryptography," in *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 6670-6683, Dec. 2014.
14. J. Xu, L. Hu, S. Sun and Y. Xie, "Cryptanalysis of countermeasures against multiple transmission attacks on NTRU," in *IET Communications*, vol. 8, no. 12, pp. 2142-2146, 14 August 2014.
15. M. Nema, 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), Indore, 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375676.
16. S. N. Premnath *et al*., "Secret Key Extraction from Wireless Signal Strength in Real Environments," in *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917-930, May 2013.