

Improving the detection of intrusion in vehicular ad-hoc networks with modified identity-based cryptosystem

Zachaeus K. Adeyemo¹, Emmanuel B. Ajulo², Damilare O. Akande¹, Hammed O. Lasisi³, Samson I. Ojo¹

¹Department of Electronic and Electrical Engineering, Faculty of Engineering and Technology, Ladoko Akintola University of Technology, Ogbomoso, Nigeria

²Department of Computer Science and Mathematics, College of Basic and Applied Sciences, Mountain Top University, Ibafo, Ogun State, Nigeria

³Department of Electrical and Electronics Engineering, College of Science, Engineering and Technology, Osun State University, Osogbo, Osun State, Nigeria

Article Info

Article history:

Received Nov 10, 2021

Revised Mar 21, 2023

Accepted Apr 30, 2023

Keywords:

Identity-based cryptosystem

Intrusion

On-board unit

Road side unit

VANET

ABSTRACT

Vehicular ad-hoc networks (VANETs) are wireless-equipped vehicles that form networks along the road. The security of this network has been a major challenge. The identity-based cryptosystem (IBC) previously used to secure the networks suffers from membership authentication security features. This paper focuses on improving the detection of intruders in VANETs with a modified identity-based cryptosystem (MIBC). The MIBC is developed using a non-singular elliptic curve with Lagrange interpolation. The public key of vehicles and roadside units on the network are derived from number plates and location identification numbers, respectively. Pseudo-identities are used to mask the real identity of users to preserve their privacy. The membership authentication mechanism ensures that only valid and authenticated members of the network are allowed to join the network. The performance of the MIBC is evaluated using intrusion detection ratio (IDR) and computation time (CT) and then validated with the existing IBC. The result obtained shows that the MIBC recorded an IDR of 99.3% against 94.3% obtained for the existing identity-based cryptosystem (EIBC) for 140 unregistered vehicles attempting to intrude on the network. The MIBC shows lower CT values of 1.17 ms against 1.70 ms for EIBC. The MIBC can be used to improve the security of VANETs.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Damilare O. Akande

Department of Electronic and Electrical Engineering, Faculty of Engineering and Technology

Ladoko Akintola University of Technology, PMB 4000, Ogbomoso, Oyo State, Nigeria

Email: doakande@lautech.edu.ng

1. INTRODUCTION

The vehicular ad-hoc network (VANET) is an infrastructure-less network created as a result of developments in wireless communications and networking technologies [1]. This new technology provides ubiquitous connectivity to vehicles while in motion thereby creating efficient vehicular communications that enable intelligent transportation systems (ITS) [2]. In VANET, there are two forms of communication, namely: vehicle-to-vehicle (V2V) communication, in which vehicles fitted with an on-board unit (OBU) wireless communication system communicate with other road vehicles, and vehicle-to-infrastructure (V2I) communication, in which vehicles use their OBU to communicate with roadside units (RSUs) [3]. Improving road safety and quality is the primary essence of this technology [2]. In VANET, the OBU of the vehicle acts as an independent router, generates independent data, and periodically transmits information to other nearby vehicles and RSUs on their current states, such as location, direction, speed, current time, and traffic events [4].

In communicating with vehicles beyond the wireless range; intermediate vehicles or RSUs forward messages to the intended destination over multiple hops. Thus, many initiatives in academic and standardization societies have been inspired by this new model of communication [5]. Seven 10 MHz channels in the 5.9 GHz dedicated short-range communication (DSRC) band have recently been allocated by the Federal Communications Commission (FCC) of the United States of America (USA) to increase the protection and efficiency of the transport system [5], [6]. Six 10 MHz channels are dedicated to comfort applications (internet facility, information on the nearest restaurant, car park, filling station) in the new DSRC standard, and one channel is to safety applications.

Given the tremendous benefits expected from vehicular communications, just like any other wireless communication network, security has been a major challenge. Intruders can easily intercept, modify, and replay messages transmitted on the network or even impersonate other vehicles to broadcast incorrect information [6], [7]. Besides, the privacy of users on the network is also a challenge. The ideal is that the travelling route of drivers should not be traceable by intruders through the message(s) sent or received by the vehicles on the network [8], [9]. Consequent to these security challenges in VANETs, it has received due attention from researchers, and the use of identity-based cryptosystem (IBC) to provide this security [10]-[12]. The uniqueness of IBC compare to other forms of security protocol is that the identity and pre-configuring key of users is derived from an arbitrary string that uniquely identifies them [13]-[15]. Nonetheless, the existing identity-based cryptosystem (EIBC) used to solve this problem lack membership authentication security feature thereby allowing intruders to invade the network [10]. This informs the purpose of this work to develop a modified identity-based cryptosystem (MIBC) to prevent and detect intrusion in VANETs. In this paper, the MIBC was simulated using MATLAB R2018a. The performance of the MIBC was evaluated using intrusion detection ratio (IDR) and computation time (CT) as performance metrics, and compared with EIBC.

2. OVERVIEW OF VEHICULAR AD-HOC NETWORKS (VANETS) AND IDENTITY-BASED CRYPTOSYSTEM

Improving the detection of intruders in VANETs with a MIBC forms the basis for this study. Therefore, the need to discuss the technology of VANETs and the fundamental of an identity-based cryptosystem cannot be sidelined. The overview of VANETs technology and the IBC used for this work is thus explained.

2.1. Vehicular ad-hoc networks

A sub-class of the wireless ad-hoc network (WANET) and the mobile ad-hoc network (MANET) extension is the VANET. In VANET, nodes consist of self-organized vehicles and road-side infrastructure that communicate with each other through wireless devices and function independently of any infrastructure in a peer-to-peer mode. Each node operates and produces independent data as an independent router [16]-[19]. Network management and fault detection become distributed and hence more difficult to handle [20]. Nodes in VANETs are mobile which causes frequent changes to the network topology and makes it unpredictable. It cannot be assumed that VANETs would always be under the protection of their owners because of the ubiquitous existence of mobile nodes; nodes may be stolen or tampered with. For both legitimate and unauthorized network users, the shared wireless medium is available [21]. While driving along the road, these wireless-equipped vehicles spontaneously form networks. The key idea is to provide vehicle nodes with ubiquitous connectivity while on the move and to establish effective vehicle-to-vehicle communications that allow ITS. The ultimate objective of VANETs is to enhance the driving experience, improve traffic safety and improve the performance of drivers [22]-[24].

2.2. Identity-based cryptosystem

Pre-configured vehicle keying materials and RSUs are created from their identities in identity-based cryptosystems in such a way that the public and private keys of the vehicles and RSUs are bound to their respective identities, thus avoiding certificate verification [25]. The cost of computing in this cryptosystem is therefore small. Also, because in identity-based cryptosystems, the vehicle and the RSU do not need to exchange certificates, the message length is reduced, and IBC is much more effective. IBC consists of two mechanisms in basic form, namely identity-based encryption (IBE) and identity-based signature (IBS), with four steps each. Setup/initialization, private key extraction, encryption, and decryption are the IBE process steps while the IBS mechanism includes four steps include setup/initialization, private key extraction, signature, and verification [25]-[27]. Both mechanisms follow the same process for setup/initialization and private key extraction. These mechanisms are combined to achieve desired identity-based cryptosystems.

3. RESEARCH METHOD

The MIBC consists of four entities, namely: the trusted authority (TA), the network control unit (NCU), the RSUs, and the vehicles. The TA is a trusted third party responsible for the system setup, registration, configuration, and issuing of private keys to the NCU, RSUs, and vehicles on the network. The NCU is responsible for the authentication of users on the network. The RSUs are static smart devices on the road such as traffic sensors or pedestrian sensors mounted on the road, while the vehicles are mobile entities with a transceiver known as OBU installed in them to enable communication. The cryptographic process involves four phases. The first is the key and pseudo-identity generating phase which is solely carried out by the TA. The second is the vehicle authentication phase where valid users of the network are allowed to join the network, the third is the data transmission phase comprising message signing, and the fourth is the message verification phase.

3.1. Development of a secure communication system

The development of secure communication begins at this stage. The system was developed on a non-singular elliptic curve as expressed in the (1) and Lagrange interpolation was used to define and interpolates points on the curve. The use of Lagrange interpolation eliminates the need for point pairing which may increase the cryptographic headcount.

$$y^2 = x^3 + ax + b \text{ mod } p \quad (1)$$

The registration and setup of vehicles, RSUs, and NCU which are entities on the network were carried out by the TA. The TA creates a group G defined by a non-singular elliptic curve as expressed in (1) and selects a generator $P \in G$. The TA then randomly generates a master private $s \in Z_q^*$ for the system and computes the system public key P_{pub} as in (2).

$$P_{pub} = s.P \quad (2)$$

Where: 's' is the master private key of the system, and it is an integer within the order q , P is the generator of the element in the group, and Z^* is a set of integers other than zero. The pseudo-identity of entities (participants) on the network was generated using (3).

$$PID = \gamma_i.P || RID \oplus H(\gamma_i.P_{pub}). \quad (3)$$

Where: PID is the pseudo-identity of entities (participants) on the network, γ_i is a set of integers randomly generated in $\gamma_i \in Z_q^*$, RID is the real identity of the entity on the network, P_{pub} is the master public key of the system as derived in (2), and P is the generator of the group as already defined. In order to generate the private key of any entity on the network.

$$sk_i = \gamma_i + \theta_i.s \text{ mod } q. \quad (4)$$

Where: γ_i is a set of integers randomly generated in $\gamma_i \in Z_q^*$, ' θ_i ' is a hashed value of pseudo-identity concatenated with a timestamp T_i , 's' is the master private key of the system, and $\text{mod } q$ is a modular arithmetic operation in prime q .

3.2. Development of vehicle authentication system

The TA selects randomly a live session code $S_{LC} \in Z_q^*$ and then generates vehicle membership authentication code to the vehicle using (5), and the control authentication key for the NCU using (6) respectively. However, the live session code S_{LC} is not given to the vehicle(s) directly, but to the NCU for vehicle(s) validation and authentication whenever it has to join the network for communication.

$$M_k = H(C_k || ID_{NCU}) \oplus RID_v \quad (5)$$

$$C_k = s.H(ID_{TA} || RID_v || S_{LC}) \quad (6)$$

Where: M_k is the membership authentication code for participants on the network, C_k is the control authentication key for the NCU, ID_{TA} is the identity of the TA, RID_v is the real identity of the vehicle, ID_{NCU} is the identity of NCU, 's' is the master secret key, γ_i is a set of integer randomly generated in $\gamma_i \in Z_q^*$, H is the hash function, $||$ is the concatenation operation and \oplus is the exclusive-OR operation. The NCU checks for the validity of the request using (7), and further checks the revocation list which contains the real identities of revoked vehicles received securely from the TA to ascertain the authenticity of the vehicles' membership.

$$RID_v \stackrel{\Delta}{=} M_k \oplus H(C_k || ID_{NCU}) \quad (7)$$

The correctness of this authentication is proven as recall from (5) that:

$$M_k = H(C_k || ID_{NCU}) \oplus RID_v$$

Then,

$$RID_v = H(C_k || ID_{NCU}) \oplus RID_v \oplus H(C_k || ID_{NCU})$$

$$RID_v = RID_v$$

3.3. Message signing

The vehicle signs messages to be transmitted on the network via the OBU device by generating a random number $\mu_i \in Z_q^*$ and computes (8), (9), and (10). This is to ensure non-repudiation and to ensure high-security protection because any computation towards breaking the scheme by any intruder requires simultaneous extraction of two unknown secrets.

$$R_i = \mu_i \cdot P \quad (8)$$

$$\beta_i = H(PID || T_i || R_i || M_i) \quad (9)$$

$$\sigma_i = sk_v + \beta_i \cdot \mu_i \text{ mod } q \quad (10)$$

The signed message $M = \{M_i, PID_i, T_i, R_i, \sigma_i\}$. Then, the vehicle broadcasts the message M to the nearby RSUs and vehicles, which are the receivers.

3.4. Message verification

The verifier which may be an RSU or a vehicle checks the validity of the message received using (11). The verifier checks the freshness of timestamp T_i ; if $\Delta T \geq T_{Now} - T_i$, where: ΔT is the predefined endurable transmission delay, T_{Now} is the recent message received, and $i = 1, 2, 3, \dots, n$; otherwise, the verifier rejects the message.

$$\sigma_i \cdot P = PID_v + \theta_i \cdot P_{pub} + \beta_i \cdot R_i. \quad (11)$$

Where: θ_i is the hashed value of pseudo-identity concatenated with a timestamp T_i . If it does, the message is approved by the verifier; otherwise, the message is rejected by the verifier.

3.5. System simulation and procedures

The MIBC was simulated using MATLAB R2018a. The simulation was conducted on a Windows 8 computer system with Intel® Core™ i3 processor, 4 GB RAM. The simulation was considered for the V2V and vehicle-to-roadside unit (V2R) communications, and the frequency of operation is 5.9 GHz. The driving scenario designer (DSD) Application on the MATLAB R2018a Environment was used as a mobility generation tool; and the transmission rate used is 0.3 seconds. The graphical users interface (GUI) as shown in Figure 1 was created to aid simulation and analysis of the system. The membership authentication panel on the GUI checks the validity of the vehicle when a request to join the network is sent; such a request is either valid or not valid. The key generating panel generates on the GUI generates the entire usable key for the vehicles on the network.

3.6. System evaluation performance metrics

The performance evaluation of the system was done using IDR and cryptographic computation time. The IDR which is the ratio of the detected number of vehicles trying to break into the network to vehicles not detected was analysed. The simulation analyses the efficiency of the NCU in preventing invalid and unregistered vehicles into the network. For an efficient system, the detection ratio is expected to be high, and the percentage detection rate is expressed as in (12).

$$IDR = \frac{\text{Number of incidents successfully detected}}{\text{Total number of incidents}} \times 100\% \quad (12)$$

In the same vein, the computation time which is the time required for computing the cryptographic operations was also analyzed. In this paper, the computation time was carried out using the 'tit-tot' function of the MATLAB R2018a for both the developed and existing systems. The percentage of performance improvement analysis of the developed system was achieved using the (13).

$$I_{per} = \frac{(T_{exist} - T_{developed})}{T_{exist}} \% \quad (13)$$

Where I_{per} refers to the improvement percentage, T_{exist} refers to the time costs of the existing scheme, and $T_{developed}$ refers to the time costs of the developed scheme. Consequently, the developed system (MIBC) was compared with the existing system, (EIBC), and the percentage performance improvement analysis was carried out using the (14).

$$I_{per} = \frac{(T_{exist} - T_{developed})}{T_{exist}} 100\% \quad (14)$$

Where I_{per} refers to the improved percentage, T_{exist} refers to the value of the existing scheme, and $T_{developed}$ refers to the value of the developed scheme.

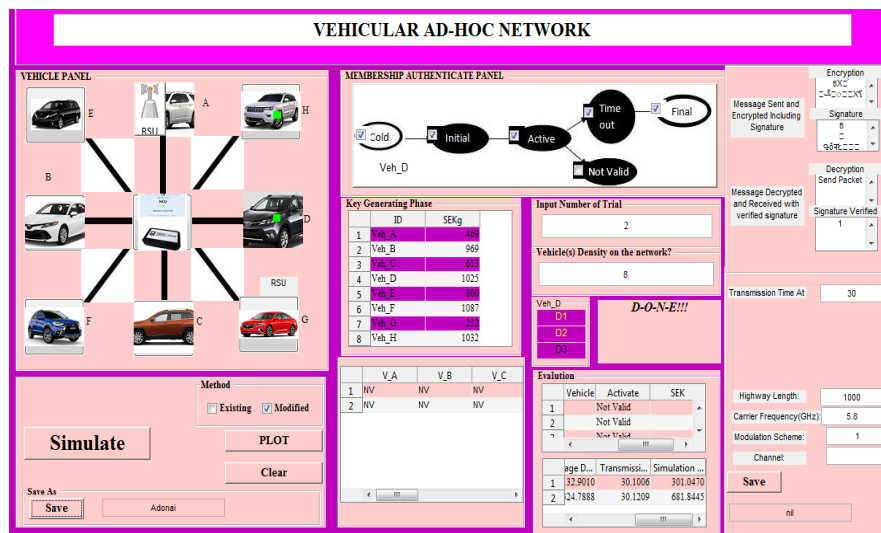


Figure 1. Simulation interface for the modified identity-based cryptosystem

4. RESULTS AND DISCUSSION

The IDR which is the ratio of the detected number of vehicles trying to break into the network to vehicles not detected was analysed. The simulated vehicles were divided into two parts, 70% of the vehicles were unregistered and invalid vehicles and made to intrude into the network, while the remaining 30% were registered and valid members of the network. From the simulation, it was observed that all attempts made by the intruding vehicles were rejected by the NCU. The result is shown in Table 1, and the percentage intrusion detection rate for the number of incidents (vehicles) is shown in Figure 2.

In the same vein, the CT of the cryptographic process of the MIBC obtained is 1.17 ms. This is an average result of running the cryptographic algorithm for an average of 1000 times. Also, the MIBC was compared with the EIBC. In terms of CT, the CT for MIBC is 1.17 ms while that of EIBC is 1.70 ms. The result shows that the MIBC has a lower computation time compared to the EIBC. Consequently, the percentage improvement of the computation time of MIBC over the EIBC, shows that the MIBC has 31.18% improvements over the EIBC. The IDR result for the MIBC and EIBC for different vehicles were compared. The values are as shown in Table 2, and illustrated in Figure 3.

The overall average percentage of performance improvement analysis of intrusion detection rate in the MIBC and EIBC is presented in Figure 4. The result shows that the MIBC has a total average of 98.5% intrusion detection rate compare to the EIBC which has a 93.2% intrusion detection rate. This is a 5.4% performance improvement over EIBC. The results presented show that the performance of MIBC gets better even with an increase in the number of vehicles released into the network which is a great improvement compared to EIBC.

Table 1. Intrusion detection ratios

No. of vehicle	Total no. of incidents	No. of incidents successfully detected	% IDR
50	35	33	94.3
100	70	69	98.6
150	105	103	99.1
200	140	139	99.3

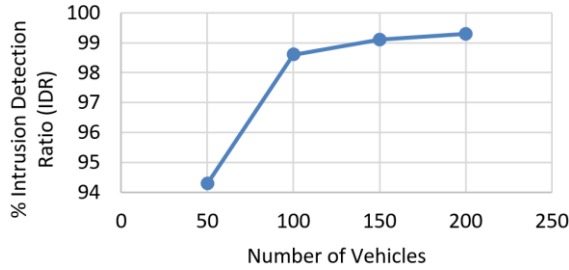


Figure 2. Intrusion detection rate for the number of incidents (vehicles)

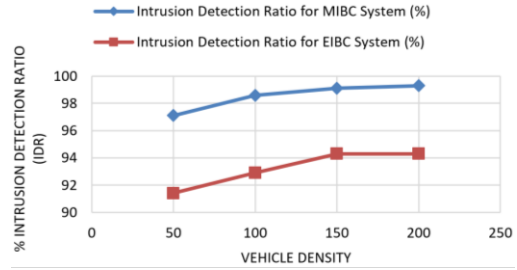


Figure 3. Comparison of intrusion detection rate in the MIBC and EIBC

Table 2. Intrusion detection ratio for the MIBC and EIBC

Vehicle density	Intrusion detection ratio for MIBC system (%)	Intrusion detection ratio for EIBC system (%)
50	97.1	91.4
100	98.6	92.9
150	99.1	94.3
200	99.3	94.3

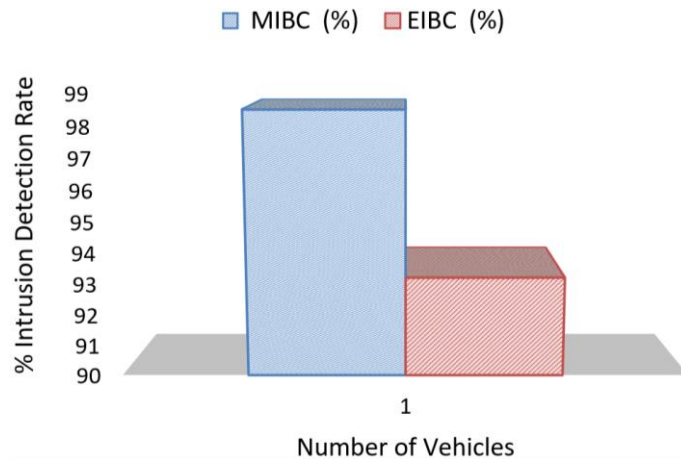


Figure 4. Overall average intrusion detection analysis

5. CONCLUSION

In this paper, a variant IBC that ensures secure communication and prevention of intruders in VANET was developed. An authentication system for users' validation on the network was incorporated into the system. The validation is done via the NCU in a handshake with the TA of the system to securely prevent intrusion and ensures that only valid members of the network are allowed to join the network. The NCU of the system securely prevents intrusion and ensures that only valid members of the network are allowed to join the network. The result shows that the proposed MIBC outperforms the EIBC in IDR and CT performance and shows the superiority of the security features in terms of users' membership authentication.

ACKNOWLEDGEMENTS





Our sincere appreciation goes to the Department of Electronic and Electrical Engineering, Ladoko Akintola University of Technology, Ogbomosho, Nigeria, for the provision of the conducive environment upon which this research was conducted.

REFERENCES





- [1] D. A. J. Al-Khaffaf and M. G. Al-Hamiri, "Performance evaluation of campus network involving VLAN and broadband multimedia wireless networks using OPNET modeler," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 19, no. 5, pp. 1490-1497, 2021, doi: 10.12928/TELKOMNIKA.v19i5.18531.
- [2] Girish and Phaneendra H. D., "Identity-based cryptography and comparison with traditional public-key encryption: A survey," *International Journal of Computer Science and Information Technologies (IJCSIT)*, vol. 5, no. 4, pp. 5521-5525, 2014. [Online]. Available: <https://www.ijcsit.com/docs/Volume%205/vol5issue04/ijcsit20140504155.pdf>
- [3] J. Jenefa and E. A. M. Anita, "Secure vehicular communication using identity-based signature scheme," *Wireless Personal Communication*, vol. 98, pp. 1383-1411, 2018, doi: 10.1007/s11277-017-4923-7.
- [4] J. Cui, W. Xu, H. Zhong, J. Zhang, Y. Xu, and L. Liu, "Privacy-preserving authentication using a double pseudonym for the internet of vehicles," *Sensors*, vol. 18, no. 5, 2018, doi: 10.3390/s18051453.
- [5] H. Peng, L. Liang, X. Shen, and G. Y. Li, "Vehicular communications: a network layer perspective," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 2, pp. 1064-1078, 2019, doi: 10.1109/TVT.2018.2833427.
- [6] E. B. Ajulo, R. O. Akinyede, and O. S. Adewale, "Security threats and privacy issues in vehicular ad-hoc network (VANET): survey and perspective," *Journal of Information*, vol. 4, no. 1, 2018, doi: 10.18488/journal.104.2018.41.1.9.
- [7] Y. Huang, X. Ma, Y. Liu, and Z. Yang, "Effective capacity maximization in beyond 5G vehicular networks: a hybrid deep transfer learning method," *Wireless Communications and Mobile Computing*, vol. 2021, 2021, doi: 10.1155/2021/8899094.
- [8] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S. Al-Rimy, A. Alsaeedi, and W. Boulila, "Ensemble-based hybrid context-aware misbehavior detection model for vehicular ad hoc network," *Remote Sensing*, vol. 11, no. 23, 2019, doi: 10.3390/rs11232852.
- [9] E. B. Ajulo, R. O. Akinyede, and O. S. Adewale, "Modeling of situation response time in vehicular ad-hoc network," *MATICS: Jurnal Ilmu Komputer dan Teknologi Informasi*, vol. 10, no. 1, pp. 1-7, 2018, doi: 10.18860/mat.v10i1.4785.
- [10] H. F. Jassim, M. A. Tawfeeq, and S. M. Mahmoud, "Overlapped hierarchical clusters routing protocol for improving quality of service," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 19, no. 3, pp. 705-715, 2021, doi: 10.12928/TELKOMNIKA.v19i3.18354.
- [11] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANETs)," *Vehicular Communications*, vol. 25, 2020, doi: 10.1016/j.vehcom.2020.100247.
- [12] F. A. Ghaleb *et al.*, "Misbehavior-aware on-demand collaborative intrusion detection system using distributed ensemble learning for VANET," *Electronics*, vol. 9, no. 9, 2020, doi: 10.3390/electronics9091411.
- [13] B. A. S. Al-Rimy *et al.*, "A pseudo feedback-based annotated TF-IDF technique for dynamic crypto-ransomware pre-encryption boundary delineation and features extraction," *IEEE Access*, vol. 8, pp. 140586-140598, 2020, doi: 10.1109/ACCESS.2020.3012674.
- [14] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in VANETs and VANET cloud," *Vehicular Communication*, vol. 12, pp. 138-164, 2018, doi: 10.1016/j.vehcom.2018.04.005.
- [15] J. Liang, J. Chen, Y. Zhu, and R. Yu, "A novel intrusion detection system for vehicular ad hoc networks (VANETs) based on differences of traffic flow and position," *Application Soft Computing*, vol. 75, pp. 712-727, 2019, doi: 10.1016/j.asoc.2018.12.001.
- [16] Y. Zhou, S. Liu, M. Xiao, S. Deng, and X. Wang, "An efficient V2I authentication scheme for VANETs," *Mobile Information Systems*, 2018, doi: 10.1155/2018/4070283.
- [17] S. Zeng, Y. Huang, and X. Liu, "Privacy-preserving communication for VANETs with conditionally anonymous ring signature," *International Journal Network Security*, vol. 17, no. 2, pp. 135-141, 2015. [Online]. Available: <http://ijns.jalaxy.com.tw/contents/ijns-v17-n2/ijns-v17-n2.pdf#page=37>
- [18] C. Wan and J. Zhang, "Efficient identity-based transmission for VANET," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, pp. 1861-1871, 2018, doi: 10.1007/s12652-017-0650-x.
- [19] F. A. Ghaleb, M. A. Maarof, A. Zainal, B. A. S. Al-Rimy, F. Saeed, and T. Al-Hadhrani, "Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network," *IEEE Access*, vol. 7, pp. 159119-159140, 2019, doi: 10.1109/ACCESS.2019.2950805.
- [20] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Vehicular Communications*, vol. 28, 2021, doi: 10.1016/j.vehcom.2020.100310.
- [21] S. Zhang, Y. Liu, Y. Xiao, and R. He, "A trust based adaptive privacy preserving authentication scheme for VANETs," *Vehicular Communication*, vol. 37, 2022, doi: 10.1016/j.vehcom.2022.100516.
- [22] A. F. Abbas, U. U. Sheikh, F. T. Al-Dhief, and M. N. H. Mohd, "A comprehensive review of vehicle detection using computer vision," *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, vol. 19, no. 3, pp. 838-850, 2021, doi: 10.12928/TELKOMNIKA.v19i3.12880.
- [23] V. H. La and A. Cavalli, "Security attacks and solutions in vehicular ad-hoc networks: A survey," *International Journal on AdHoc Networking Systems (IJANS)*, vol. 4, no. 2, pp. 1-20, 2014, doi: 10.5121/ijans.2014.4201.
- [24] B. Ji *et al.*, "Survey on the internet of vehicles: network architectures and applications," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 34-41, 2020, doi: 10.1109/MCOMSTD.001.1900053.
- [25] F. Mezrag, S. Bitam, and A. Mellouk, "An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks," *Journal of Network and Computer Applications*, vol. 200, 2022, doi: 10.1016/j.jnca.2021.103282.
- [26] Y. Chen, Y. Wang, M. Liu, J. Zhang, and L. Jiao, "Network slicing enabled resource management for service-oriented ultra-reliable and low-latency vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7847-7862, 2020, doi: 10.1109/TVT.2020.2991723.
- [27] B. A. S. Al-Rimy, M. A. Maarof, and S. Z. M. Shaid, "Crypto-ransomware early detection model using novel incremental bagging with enhanced semi-random subspace selection," *Future Generation Computer Systems*, vol. 101, pp. 476-491, 2019, doi: 10.1016/j.future.2019.06.005.

BIOGRAPHIES OF AUTHORS







Zachaeus K. Adeyemo     received his B.Eng., M.Eng. degrees in Electrical Engineering from University of Ilorin, Ilorin, Nigeria in 1994 and 2002, respectively, and Ph.D. in Electronic and Electrical Engineering (Communication Engineering) from Ladok Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria in 2009. He joined the services of Ladok Akintola University of Technology (LAUTECH) Ogbomoso in 1995 as a Graduate Assistant in the department of Electronic and Electrical Engineering and rose from this lowest level of the academic cadre through all the ranks until he was promoted to a full-fledged Professor. His current research interests are wireless communications, signal processing in communication systems, development of a path-loss prediction model using adaptive neuro-fuzzy inference system, spectrum detection in a cognitive radio network. Prof. Adeyemo is a corporate member, Nigerian Society of Engineers (MNSE), Registered member of Council for the Regulation of Engineering in Nigeria (R. COREN) and Member, Africa Engineering Education Association (AEEA). He can be contacted at email: zkadeyemo@lautech.edu.ng.







Emmanuel B. Ajulo     received his B.Tech and M.Tech degrees in Electronic and Electrical Engineering from Ladok Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria; and M.Tech and Ph.D degrees in Computer Science from the Federal University of Technology, Akure, Nigeria in 2015 and 2020 respectively. He's reputable for developing I.T architectures and security frameworks to drive communication systems. He is a member of Nigeria Society of Engineers, member of Nigeria Computing Society, and a registered engineer with the Council for the Regulation of Engineering in Nigeria (COREN). His research interest is on computational cryptography, signal processing, machine learning, and artificial intelligence. He can be contacted at email: emmanuelajulo@gmail.com.







Damilare O. Akande     obtained his B. Tech and M. Tech degrees in Electronic and Electrical Engineering from Ladok Akintola University of Technology (LAUTECH), Ogbomoso and the Federal University of Technology, Akure, Nigeria in 2008 and 2012 respectively. He obtained his Ph. D degree from University Sans Malaysia, Malaysia in 2019. He is a member of Nigeria Society of Engineers and a registered member of COREN. His research interest is on signal processing, cooperative communications and MAC layer design. He can be contacted at email: doakande@lautech.edu.ng.



Hammed O. Lasisi     is a senior lecturer and researcher in the Department of Electrical and Electronics Engineering, Osun State University, Osogbo, Nigeria. He holds doctorate (Ph.D) and master's degrees in Elecctrical and Electronics Engineering from University of Ilorin, Nigeria. His area of specialization is telecommunication and telegraphic engineering. He is a registered member of the Council for the Regulation of Engineering (COREN) in Nigeria. He can be contacted at email: hammed.lasisi@uniosun.edu.ng.



Samson I. Ojo     received his B. Tech and M. Tech degrees in Electronic and Electrical Engineering in 2011 and 2018, respectively, from Ladok Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria. He is a registered member of Council for the Regulation of Engineering in Nigeria (COREN). He obtained his Ph.D. in mobile communication in the year 2021. His research interest is on signal processing, diversity and cognitive radio. He can be contacted at email: siojo83@lautech.edu.ng.