International Journal of Futuristic Research Evaluation in Engineering
Volume 2, Issue 6, December 2020, pp. 1~9

Performance Comparison of Various Techniques for Secure Data Communication in VANET

K. Nirmala[1]and Dr. S. Prasath[2]
1Ph.D Research Scholar(Part-Time)
1Department of computer Science, Nandha Arts and Science College, Erode, Tamilnadu, India[Email id: nirmalabuasc@gmail.com]
2Assistant professor & Research Supervisor
2Department of computer Science, Nandha Arts and Science College, Erode, Tamilnadu, India[Email id: softprasaths@gmail.com]

Article Info

Article history:
Received on : 08.10.2020
Revised on : 14.11.2020
Accepted on : 12.12.2020
Published on :14.12.2020

Keywords:
Communication
Authentication efficiency
Communication
Detection rate
privacy preservation rate
Security rate
VANET

Corresponding Author:
K. Nirmala,
Department of computer Science, Nandha Arts and Science College, Erode, Tamilnadu, India

ABSTRACT:

Vehicular Ad hoc Network (VANET) provides an efficient way of delivering information from one vehicle to another vehicle. One of the popular and dangerous attacks is impact attack where an attacker inserts a fake position in each class and therefore destroys the entire network performance. In general, VANET is an infrastructure-less network for data communication with any data access points. It is utilized in identifying and presenting the warning information safety threats and potential accidents. The safety information about vehicle is provided through vehicle direction, speed, acceleration, vehicle size. Based on node specification, data communication is carried out between two nodes in VANET. Security is the major challenging problem because of attacks nodes in network since conventional technique failed to attain better security due to the mobility of nodes, malicious nodes, lack of integrity, authentication and privacy rate. The conduction of simulation work on different proposed methods such as PMPC-IA scheme and MORABC-AD technique is carried out using NS-2 network simulator. The experimental work is conducted using a routing protocol. From vehicular network, the number of data packets ranging between 25 to 250 data is considered for experimental purpose. In addition, the number of vehicular nodes between 50 to 500 nodes is considered. From the simulation results, proposed PMPC-IA scheme shows higher authentication efficiency by 13% than other techniques..

1. INTRODUCTION

Vehicular ad-hoc network is an infrastructure-less network with a number of vehicle nodes that do not require any access points. In an intelligent transportation system, VANET is employed for identifying and providing the warning about the safety threats and potential accidents by exchanging the information (direction, speed, acceleration, vehicle size, etc.). When the communication takes place between two nodes in VANET, security is the challenging task due to the mobility of nodes, malicious nodes, lack of integrity, authentication and privacy. Hence, this proposed research work concentrates on providing communication security with the enhancement of authentication efficiency, attack detection and privacy by introducing three different techniques. Authentication is an essential process to provide secured communication by authenticating the vehicle nodes before data communication. Vehicle ad hoc network is a promising network to attain traffic safety and it includes components such as a Roadside Unit (RU) and Vehicular Nodes (VN). The VN and RU connect each other with a high speed Dedicated Short-Range Radio Signals (DSRS) to distribute information related to traffic. The data privacy, integrity, and authentication are the key problems to be addressed in VANET during information sharing between vehicular nodes. A lot of authentication techniques have been designed to increase security. However, the existing techniques failed to improve the authentication efficiency and also the communication overhead. Few research works have been designed in existing works to authenticate vehicular nodes in VANET before data communication. Still, the authentication efficiency of conventional techniques is poor. Fig.1.1 shows, secured communication of data packet based on vehicular network.

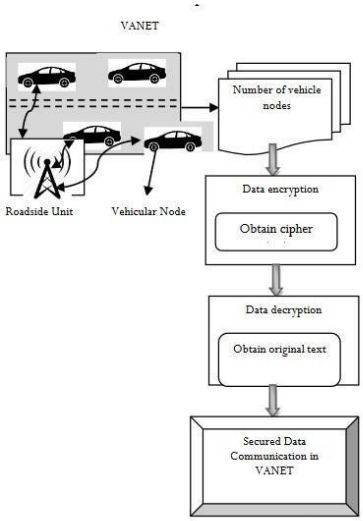

Fig.1.1 Secure data communication in VANET

Fig.1.1 Secure data communication in VANET

Fig.1.1 describes the communication of data packets on vehicle nodes by selecting authenticated nodes with minimum communication overhead and higher security rate. Therefore, three different proposed techniques are developed to achieve secured communication with vehicle node authentication. Firstly, in PMPC-IA technique malicious nodes are identified to improve security during the data communication between one vehicle to another vehicles.

2.RELATED WORK

A local identity-based anonymous message authentication protocol (LIAP) presented by Shibin Wang [1] for VANET. Every vehicle and road side unit (RSU) allocated long term certification from certificate authority (CA) in registration phase. RSU was employed for allocating the local master keys to each vehicle within communication range. When the vehicle addresses RSU, it authenticates each other through long

certificates. The valid vehicle gets the local master keys from RSU to create localized anonymous identity. The vehicle selected for the anonymous identity is verified by single authentication method to preserve the privacy but authentication accuracy did not improve using LIAP.

A Greedy Detection approach for Vehicular Ad hoc Network (VANET) Mohamed et al., [2] identified the greedy behavior attacks in VANET. The designed approach comprises of two phases namely suspicion phase and decision phase. The suspicion phase was depending on linear regression mathematical ideas while decision phase was depending on fuzzy logic decision scheme. A message authentication protocols problem addressed Siavash Mirzaee [3] in VANET because of transportation. An efficient and secure authentication scheme was with lesser computation cost for Vehicular Ad hoc Network (VANET) and an identity-based authentication scheme presented by Yong et al.,
[4] to guarantee reliability and integrity for conditional privacy-preservation. Though the computation cost was reduced, the authentication performance had no improvement.

An efficient CPPA scheme of Sunday et al., [5] for VANETs using elliptic curve cryptography was secure against selected message and identity attacks depending on elliptic curve discrete logarithm issues but the security level did not improved. Shiang et al., [6] suggested Identity-based Batch Verification (IBV) scheme to create and enhance the security and privacy of vehicles. Identity-based Batch Verification (IBV) scheme presented provable security in random oracle model. The batch verification required small constant number of pairing and point multiplication computations but the security level decreased while using Identity-based Batch Verification (IBV) scheme. An efficient anonymous authentication scheme suggested by Maria et al., [7] to avoid malicious vehicles entering into Vehicular Ad hoc network (VANET) and the designed scheme provided the conditional tracking mechanism to trace the vehicles. The scheme revoked privacy of misbehaving vehicles to present conditional privacy in efficient manner but the computational cost not get reduced.

SDN based Vehicular ad hoc Network (SDVN) architecture was constructed by Wafa et al., [8] for networking infrastructure design and advantages. The architecture is against security threats that violate the key security services like availability, privacy, authentication and data integrity. A comprehensive survey and security analysis on SDN based Vehicular ad hoc Network (SDVN) architectures was carried out to address the challenges in vehicular communication systems and enhance the future Intelligent Transportation Systems (ITS) but the complexity level was standard. A secure communication framework by Xiaoling et al., [9] with lightweight cryptography primitives. A point-to-point and broadcast communications for vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) were depending on symmetric cryptography. The key distribution and agreement protocols were introduced for two-party key and group key under different environments still, computational complexity was more in using secured communication framework.

3.METHODOLOGY

3.1 Local Identity-based anonymous message Authentication Protocol (LIAP)

Shibin Wang et al., [SHIB2017] designed a Local Identity-based anonymous message Authentication Protocol (LIAP) performed communication in VANET. LIAP designed with aid of PKI-based certificate and identity-based signature. PKI-based certificate is applied for discovering the authenticate node. An identity-based signature employed to meet the validity of safety-related message. The four different phases are registration phase, master key retrieval phase, signature verification phase, real identity tracking and revocation phase. In registration phase, every vehicle and road side unit is allocated with a unique long-term certification from certificate authority. In master key retrieval phase, Road Side Unit (RSU) is utilized to assign the local master keys to each vehicle within communication range. When vehicle enters the communication range of the (RSU), it validated other through long certificates. The valid vehicle gathers local master keys from existing Road Side Unit (RSU) for generating the localized anonymous identity. In signature verification phase, the vehicle selects the anonymous identity to sign the safety-related message and verifies with single or batch authentication for protecting the privacy. In real identity tracking and revocation phase, the mutual authentication process is used to ensure that only the valid vehicle attains key materials from unrevoked Road

Side Unit (RSU). Certificate Authority (CA) controls the revoked certificates with the RSU Certificate Revocation list and the Vehicle Certificate Revocation List (VCRL) respectively. When a vehicle is compromised, certificate authority (CA) is easily revoking its long-term certificate. The mutual authentication process avoids the message authentication of Vechicle-to-Vechicle (V2V) communication but the authentication accuracy could not be enhanced and the authentication overhead during data communication has not reduced using Local Identity-based Anonymous message Authentication Protocol (LIAP).

3.2Distributed Aggregate Privacy-Preserving Authentication(DAPPA)

Lei Zhang [LEI 2017] designed a Distributed Aggregate Privacy-Preserving Authentication (DAPPA) to secure data communications. The designed protocol based on the trusted authority with aggregate signature technique. By using the identity and signature process, traffic congestion is reduced. DAPPA is considered as the root Trusted Authority (TA) for many lower-level Trusted Authority (TAs) and users. Every lower-level TA is enrolled with the root Trusted Authority (TA) and the Distributed Aggregate Privacy Preserving Authentication (DAPPA) uses the rootTrusted Authority (TA) to create the system parameters and master secret. Every vehicle is pre-loaded by updatable (initial) secrets. When a vehicle meets the communication range of a Road Side Unit (RSU), it requests to share theRoad Side Units (RSU's) private key. The RSU transmits the shares of theRoad Side Units (RSU's) private key and authorizes period to the vehicle. When a vehicle authenticates dissimilar message, it minimizes the storage space required by vehicle but the security level remained minimum.

3.3Greedy Behavior Attack Detection Algorithm(GDVAN)

A novel Greedy Behavior Attack Detection Algorithm for VANETs (GDVAN) discussed to discover the greedy behavior attacks. The algorithm included two phases namely the suspicion phase and decision phase. The suspicion phase depending on linear regression equation while the decision phase depending on a fuzzy logic decision scheme. The algorithm not only discovered the greedy behavior but also employed three newly defined metrics. The suspicion phase used to measure the correlation coefficient among two random variables. The correlation coefficient values are -1 and 1. These values namely -1 and 1 are denoted as a strong correlation and the suspicion phase applied to compute the slope of the linear regression straight. The decision scheme has been used to identify greedy behavior suitable for VANET. The decision scheme applied to three newly defined metrics that best suits mobile networks through short monitoring periods. The algorithm examines the network traffic traces and verifies the existence of greedy nodes. The verification phase identified the responsible nodes. The time taken for detecting the attack node got minimized but the detection rate not improved.

3.4Probabilistic Mceliece Public-Key Cryptography based Identity Authentication (PMPC-IA)

The proposed PMPC-IA scheme is developed in VANET for attaining secured data communication among vehicles with minimum overhead. In VANET, vehicular node transmits the traffic information to roadside unit or other vehicles. Because of inherent nature of wireless channels, VN is vulnerable to various attacks. To prevent attacks from network, datasecurity is an important issue. This leads to avoid traffic accident and loss of human lives. A Local Identity-based anonymous message Authentication Protocol (LIAP) designed. The anonymous identity is generated to obtain communication with minimum overhead but authentication accuracy is not improved and the overhead involved during data communication could not be minimized.

The combination of Probabilistic McEliece Public key Cryptography and Identity Authentication, scheme is designed. With the asymmetric encryption algorithm. In this technique, identity authentication is applied for verifying the vehicular nodes to perform communication since it helps to achieve secured communication of roadside units with minimum complexity while cryptography performs of data encryption and decryption.

Based on hardness of decoding a general linear code, proposed scheme is designed. The error correcting code is selected for the generation of secret key for achieving a decoding process. By using secret key, error occurred during data communication is corrected and further, public key is formulated from secret key by concealing the selected code as a general linear code. For each vehicular node and roadside unit, public key and secret key is initialized and encryption and decryption process is carried out Probabilistic McEliece Cryptography. In McEliece data encryption process, data information is encrypted and it generates cipher text. The proposed PMPC-IA scheme resulted with higher communication security in VANET with minimum overhead.

The proposed PMPC-IA scheme developed a Probabilistic McEliece Data Encryption (PMDE) process after performing registration and key generation process. During encryption process, data are encrypted into cipher text by using produced public key. For each sender in Vehicular Nodes (VN) or Roadside Unit (RU), public key is utilized to encrypt the data. In encryption algorithm, randomness is used for encrypting any data. This supports encrypting same data several times using same public key and returns different cipher texts. Therefore, another vehicle in VANET cannot get original data by using the known cipher text results. An efficient anonymous authentication scheme to reduce communication overhead for efficient data integrity in VANET. To attain secured data transmission in VANET, each sender vehicular node or roadside unit performs encryption process. Initially, required number of data packets is considered that needs to be transmitted to receiver side. Next the data consider, each data packet is encoded into a number of binary strings and following these random data vectors are generated. Thus, Probabilistic McEliece Data Encryption (PMDE) algorithm creates random n-bit vectors and finally produces the cipher text.

Finally, McEliece Data Decryption process is performed in proposed PMPC-IA scheme for obtaining original data in VANET. It is a deterministic decryption algorithm. An Extended -Three Party Password-based Authenticated Key Exchange (E-3PAKE) to increase the security of value-added services with minimal transmission overhead but various security attacks during communication were not solved in VANET. Hence, McEliece Data Decryption process is carried out to decrypt data effectively with minimum overhead for secured data communication.

For efficient decryption process, trusted authority carries identity verification to ensure the receiver as authorized or unauthorized in network. With the identity verification process, data decryption is performed. If the identity of the receiver is valid, then data decryption is permitted. If the identity of receiver is not valid, data decryption cannot be performed. As a result, proposed PMPC-IA scheme achieves improved security for data communication between vehicular nodes with a minimal time in VANET.

4. Experimental Results and Analysis

The experimental evaluation of proposed Probabilistic McEliece Public-Key Cryptography based Identity Authentication (PMPC-IA) technique The proposed techniques are compared with three existing techniques are namely Local identity-based anonymous message authentication protocol (LIAP) by Shibin Wang and Nianmin Yao (2017), Greedy Behavior Attack Detection Algorithm for VANETs (GDVAN) by Mohamed NidhalMejri and Jalel Ben-Othman (2017) and Fast Confidentiality-Preserving Authentication (FCPA) by SiavashMirzaee and Letian Jiang (2019). The performance analysis of proposed techniques is elaborated in further section and the results are compared and analyzed with the help of given in table.

4.1 Impact of Authentication Efficiency

Authentication efficiency is defined as the ratio of vehicular node that is correctly authenticated to have secured communication according to the total number of vehicular nodes from network. It is measured in terms of percentage (%). When the authentication node has higher efficiency, the proposed technique is said to be more efficient.

Table 4.1 Tabulation for Authentication Efficiency

Number of Vehicular Nodes	Authentication Efficiency (%)			
	Existing DAPPA	Existing LIAP	Existing GDVAN	Proposed PMPC-IA
50	70	74	76	94
100	67	73	75	92
150	69	79	81	94
200	77	87	88	95
250	80	84	85	93
300	73	81	83	92
350	69	80	82	91
400	62	82	84	94
450	75	85	86	95
500	73	87	88	97

Table 4.1 demonstrates the experimental values of authentication efficiency with respect to different number of vehicular nodes presented in network and shows the comparison result of proposed techniques namely PMPC-IA technique with existing DAPPA, LIAP, GDVAN. To conduct the experimental work based on vehicular network scenario, various data packets are considered from different vehicular nodes in the range of 50 to 500. From the result, proposed PMPC-IA technique provides better result of enhanced authentication efficiency while compared with other techniques.

4.2 Impact of Detection Rate

The measure of correctly classified vehicle nodes among the number of vehicular nodes in a network is illustrated as detection rate. It is the ratio of correctly classified vehicle nodes as normal or attack nodes among total vehicle nodes in VANET. The detection rate is measured in percentage (%).

Table 4.2 Tabulation for Detection Rate

Number of Vehicular Nodes	Detection Rate (%)			
	Existing DAPPA	Existing LIAP	Existing GDVAN	Proposed PMPC-IA
50	66	70	72	84
100	69	73	75	91
150	73	75	77	87
200	71	78	79	90
250	74	79	80	91
300	78	81	83	89
350	70	75	78	86
400	72	80	81	90
450	75	78	80	88
500	78	80	82	90

Table 4.2 gives the comparison result of detection rate with respect to different number of vehicle nodes. Vehicle nodes in the range of 50 to 500 are considered during the experiment. From the values obtained, while increasing the number of nodes, detection of normal or attack nodes is getting varied in all other selected methods. Further, the table also provides the comparison of proposed PMPC-IA technique with existing techniques namely LIAP, GDVAN and DAPPA. Therefore, detection rate using PMPC-IA technique provides higher result than the existing techniques.

4.3 Impact of Privacy Preservation Rate

The privacy preserving rate is defined as the ratio of number of data packets that are correctly authenticated by the authorized vehicle nodes to the total number of data packets sent. The privacy preserving rate is measured in terms of percentages (%).When the number of data packets is increased, correspondingly privacy preserving rate is also getting increased.

Table 4.3 Tabulation for Privacy Preservation Rate

Number of Data Packets	Privacy Preservation Rate (%)			
	Existing DAPPA	Existing LIAP	Existing GDVAN	Proposed PMPC-IA
25	60	60	64	76
50	68	68	70	82
75	73	73	77	85
100	77	77	80	88
125	75	75	76	87
150	74	74	77	90
175	78	78	80	92
200	74	74	75	90
225	73	73	76	88
250	76	76	78	90

Table 4.3 demonstrate the experimental result of privacy preserving rate for proposed and existing techniques and shows the comparison of proposed PMPC-IA technique, with existing techniques namely DAPPA, LIAP, GDVAN. While carrying out the experiment, number of data packets in vehicular nodes is considered in the range of 25 to 250 from nodes. Various vehicle data is considered on node for communicating data in secured manner. From the resultant value, while increasing the number of node data packets, the privacy preserving rate also gets varied. When comparing with other techniques, PMPC-IA technique achieves maximum privacy preserving.

4.4 Impact of Communication Overhead

The quality of time consumed for transmitting the data packets from one vehicle node to another vehicle node is defined as communication overhead. It helps to communicate secured data in minimum time. Based on total number of vehicle nodes, time taken for data communication is presented. It is measured in milliseconds (ms).

Table 4.4 Tabulation for Communication Overhead

Number of Vehicular Nodes	Communication Overhead (ms)			
	Existing DAPPA	Existing LIAP	Existing GDVAN	Proposed PMPC-IA
50	45	51	49	41
100	46	54	51	47
150	57	62	57	51
200	61	68	62	54
250	70	78	70	59
300	79	85	76	66
350	73	91	84	72
400	91	96	89	78
450	87	98	93	83
500	95	103	97	87

The experimental result of communication overhead which is obtained using proposed and existing method is in table 4.4and the result provides the comparison of proposed and existing methods according to various numbers of vehicle nodes that need to communicate data packets with various sizes. For experimental purpose, number of vehicular nodes in the range of 50 to 500 is considered. From the values obtained, experimental result of proposed techniques namely PMPC-IA technique is presented after its comparison with other existing techniques such as DAPPA, LIAP, GDVAN. As a result, proposed PMPC-IA technique gives better communication overhead than other existing techniques.

4.5 Impact of Security Rate

The security rate is defined as the measure of number of data packets that are successfully transmitted to receiver node with respect to total number of data packets sent from vehicular nodes in network. Security rate is measured in percentage (%). When the data security data is more, then proposed technique can get more efficient result.

Table 4.5 Tabulation for Security Rate

Number of Data Packets	Security Rate (%)			
	Existing DAPPA	Existing LIAP	Existing GDVAN	Proposed PMPC-IA
25	64	64	68	80
50	70	70	74	84
75	75	75	79	88
100	79	79	81	89
125	76	76	78	90
150	76	76	79	91
175	79	79	81	93
200	75	75	77	91
225	74	74	76	88
250	76	76	79	91

Table 4.5 presents the result of security rate for the transmission of different data packets with respect to various sizes. To analyse a secured communication in VANET, the data packets in the range of 25 to 250 are selected. The table shows the comparison of proposed PMPC-IA with existing techniques named as DAPPA, LIAP, GDVAN. When the security rate during data communication between nodes is higher, then the method is said to be more efficient and from the obtained value, it is proved that security rate using PMPC-IA technique enhanced when compared to other techniques.

5. Conclusion

The proposed PMPC-IA technique theoretical analysis and experimental result show that the proposed methods are designed for providing secured data communication on VANET. The main purpose of developing proposed technique is to improve security rate with minimum overhead. Further, PMPC-IA technique is designed to identify the attacks with higher performance during secured communication. The main purpose is performing secured communication with higher privacy preservation with a lower overhead. Therefore, three different existing techniques is compared to attain higher data security rate during communication with minimum communication overhead.

REFERENCES

[1] Shibin Wang and Nianmin Yao, "LIAP: A local identity-based anonymous message authentication protocol in VANETs", Computer Communications, Elsevier, Volume 112, Pges 154–164, 2017
[2] Mohamed NidhalMejri and Jalel Ben-Othman, "GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs", IEEE Transaction on Mobile Computing, Volume 16, Issue 3, March 2017, Pages 759 –771
[3] SiavashMirzaee, Letian Jiang, "Fast Confidentiality-Preserving Authentication for Vehicular Ad Hoc Networks", Journal of Shanghai Jiaotong University (Science), Springer, Volume 24, Issue 1, Pages 31–40, February 2019
[4] Yong Xie, LiBing Wu, Jian Shen, AbdulhameedAlelaiwi, "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs", Telecommunication Systems, Springer, Volume 65, Issue 2, Pages 229–240, June 2017
[5] Sunday OyinlolaOgundoyin, "An autonomous lightweight conditional privacypreserving authentication scheme with provable security for vehicular ad-hoc networks", International Journal of Computers and Applications, Pages 516 –526, March 2017
[6] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhmmad Khurram Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", IEEE Transactions on Vehicular Technology, Volume 66, Issue 4, Pages 3235 –3248, April 2017
[7] Maria Azees, Pandi Vijayakumar, and Lazarus JegathaDeboarh, "EAAP: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks", IEEE Transactions on Intelligent Transportation Systems, Pages 1-10, 2017
[8] Wafa Ben Jaballah, Mauro Conti and Chhagan Lal, "Security and Design Requirements for Software-Defined VANETs", Computer Networks, Elsevier, Volume 169, March 2020, Pages 1-31
[9] XiaolingZhua, Yang Lua, XiaojuanZhua&ShuweiQiua, "Lightweight and scalable secure communication in VANET", International Journal of Electronics, Taylor and Francis, Pages 1-18, 2014
[10] Yang Ming and Hongliang Cheng, "Efficient Certificateless Conditional Privacy-Preserving Authentication Scheme in VANETs", Mobile Information Systems, Hindawi, Volume 2019, Article ID 7593138, Pages 1-19, 2019
[11] Yousheng Zhou, Xingwang Long, Lvjun Chen and Zheng Yang, "Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs", Journal of Information Security and Applications, Elsevier, Volume 47, 2019, Pages 295–301
[12] XiaolingZhua, Yang Lua, XiaojuanZhua&ShuweiQiua, "Lightweight and scalable secure communication in VANET", International Journal of Electronics, Taylor and Francis, Pages 1-18, 2014
[13] Wenjia Li and Houbing Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", IEEE Transactions on Intelligent Transportation Systems, Volume 17, Issue 4, 2016, Pages 960 –969
[14] Wafa Ben Jaballah, Mauro Conti and Chhagan Lal, "Security and Design Requirements for Software-Defined VANETs", Computer Networks, Elsevier, Volume 169, March 2020, Pages 1-31
[15] Ubaidullah Rajput, Fizza Abbas, HasooEun, Heekuck Oh, "A Hybrid Approach for Efficient Privacy-Preserving Authentication in VANET", IEEE Access, Volume 5, Pages 12014 –12030, 2017.
[16] S.Prasath,K.Nirmala,"A Performance Comparison of Authentication and Privacy Preserving Techniques for Secured Communication in VANET",International Journal of Innovative Technology and Creative Engineering(ISSN:2045-8711),Vol.9, No.2,Pp.625-635 ,2019.
[17]S.Prasath, K.Nirmala, "Adaptive Boosting Classifier Based Attack Detection for Secured Communication in Vanet", International Journal of Advanced Science and Technology(ISSN:2005-4238), Vol.28, No.17,Pp.No.168-177,2019. (Scopus Indexed Journal Sl.No.16260)
[18]S.Prasath, K. Nirmala, "Probabilistic Mceliece Public-Key Cryptography Based Identity Authentication for Secured Communication in Vanet", Solid State Technology Vol.63 Iss.6, Pages 10167-10182.