# A PERFORMANCE COMPARISON OF AUTHENTICATION AND PRIVACY PRESERVING TECHNIQUES FOR SECURED COMMUNICATION IN VANET

**K . Nirmala**
Ph.D Research Scholar (Part-Time),
Department of Computer Science, Nandha Arts & Science College, Erode, Tamil Nadu, India
E-mail ID: nirmalabuasc@gmail.com
**Dr.S.Prasath**
Assistant Professor & Research Supervisor,
Department of Computer Science, Nandha Arts & Science College, Erode, Tamil Nadu, India
E-mail ID: softprasaths@gmail.com

**Abstract- Vehicle adhoc network (VANET) is vital role in communication which is used for enhancing the traffic efficiency and safety through communicating one vehicle with other vehicles. Security is the key problems in VANETs and trust is an essential one that avoid the generic attacks on network. A misuse of information leads to the traffic accident and loss of human lives. Vehicle authentication is need for improving the security level in VANET. In the authentication, vehicle data like identity and location information are kept private. Privacy is an important one during communication in VANETs. The vehicle privacy information like current position, license number, drivers identity and travel route are maintained as confidential one for long time period. Many techniques were developed for secured communication in VANET. But the existing techniques have some drawbacks, there is a need to improve the authentication accuracy and privacy performance during communication in VANET. To improve the security level during communication, machine learning and cryptographic techniques is used.**

**Keywords: Vehicle ad hoc network, security, trust, vehicle authentication, privacy, communication.**

## 1. INTRODUCTION

Vehicular Ad-Hoc Network technology selected moving vehicles as nodes in network to create the mobile network. The movement of vehicles is limited by roads and traffic regulations use fixed infrastructure at critical locations. VANET presents road safety rules where the information concerning vehicle current speed and location coordinates is provided with or without exploitation. When vehicles goes beyond the signal range and drop out of the network, additional vehicles join, link the vehicles to another where the mobile internet are generated.

Vehicle authentication is requirement for improving the security level in VANET. The authentication includes the identity authentication and message integrity to guarantee the security of VANETs. When identity authentication is not satisfied, malicious vehicle imitate as legal vehicle to broadcast messages for receiving the illegal benefits. The message integrity is not guaranteed and malicious vehicle broadcast the falsified messages to disrupt the traffic for surrounding vehicles without being caught.

This paper is structured as follows: Section 2 explains authentication and privacy preservation techniques for secured communication in VANET. Section 3 shows the analysis of the existing authentication and privacy preservation techniques for secured communication in VANET. Section 4 identifies the possible comparison between the techniques of VANET. Section 5 presents the discussion and limitations of authentication and privacy preserving techniques. Section 6 concludes the paper to improve the security level during communication in VANET.

## 2. RELATED WORKS

A local identity-based anonymous message authentication protocol (LIAP) proposed in [1] for VANETs where every vehicle and Road Side Unit (RSU) assigned long term certification from Certificate Authority (CA). Vehicle selected anonymous identity to sign safety message verified by single authentication technique. But, authentication overhead is not reduced using LIAP. A new detection approach called Greedy Detection for VANETs (GDVAN) is developed in [2] for greedy behavior attacks. The design of algorithm identified greedy behavior and established list of compromised nodes through defined metrics. However, reaction method against the greedy attack not considers the GDVAN approach to eliminate serious problems.

A Novel and Efficient Conditional Privacy-Preserving Authentication (NECPPA) scheme developed in [3] for secure communications in VANET. The hacking single On-Board Unit (OBU) failed to threaten the network in Tamper Proof Device Based (TPDB) scheme that create whole vehicles to re-register and change secret keys. However, the privacy preserving rate is not improved using NECPPA. An anonymous authentication protocol designed [4] depending on the cooperative authentication method. A two-layer pseudo-identity generation method built key update tree for efficient revocation. But, self-healing functionality is not used to protect the success of group key update when the vehicles miss update messages.

An efficient randomized authentication protocol carried out the homomorphic encryption [5] to permit every individual vehicle for self-generating the number of authenticated identities to attain the anonymity in VANETs. However, authentication time is not minimized using efficient randomized authentication protocol. Event Based Reputation System (EBRS) proposed in [6] for dynamic reputation and trusted value. Every event reduces the spread of false messages. In automatic mode, trust relationship among the participant vehicles is not identified. An analytical framework developed [7] message dissemination process in vehicular network with malicious vehicles distributed in network. The probability with destination vehicle at fixed distance collected the message correctly from source vehicle. However, security level is not enhanced by analytical framework.

PassWord-based Conditional Privacy Preserving Authentication and Group-Key generAtion (PW-CPPA-GKA) protocol proposed [8] for VANETs. The design of protocol is lightweight during the computation and communication without the bilinear-pairing and elliptic curve. But, random oracle model not used for security. A vehicular authentication protocol called distributed aggregate privacy-preserving authentication designed in [9]. The protocol depends on multiple trusted authority one-time identity-based aggregate signature method. However, DAPPA failed to improve the security level through privacy-preserving authentication.

## 3. AUTHENTICATION AND PRIVACY PRESERVATION TECHNIQUES FOR SECURED COMMUNICATION IN VANET

In huge development of wireless communication, adhoc networking, automotive and transportation industry, vehicular adhoc networks have attracted large attention from government, industry and academia because of potential to provide enhanced driving experience and road safety. It is essential to meet critical security needs of VANETs like data integrity, reputation management, privacy protection, etc. The methods without protection of security and privacy methods resulted in bad user experience results.

### 3.1 Local Identity-based anonymous message Authentication Protocol in VANETs

Vehicle communicates with the additional nodes through open wireless channel that increases the safety issues. The Public Key Infrastructure (PKI) and identity based authentication protocols addressed the security and privacy requirements of VANETs. The receiver verifies the Certificate Revocation List (CRL) before certificate and signature verification in PKI-base methods. CRL checking minimized the authentication efficiency. In identity-based schemes, every vehicle maintains the valid identities to preserve the privacy. The authentication technique is developed on the public key infrastructure and identity-based encryption technology. In PKI based systems, certificate authority allocated pseudonym certificates and public/private key pairs for each registered vehicle that are preloaded into storage unit. When vehicle transmits the safety-related message, it chooses the private key to generate signature and matching certificate is embedded in message. When vehicle is revoked, CA adds all of pseudonym certificates into certificate revocation list. With increase of revoked vehicle, size of CRL not scalable that leads to high computational complexity and communication overhead.

A Local Identity-based anonymous message Authentication Protocol (LIAP) for VANETs utilized the efficient revocation of PKI and authentication efficiency of identity. Every node attain unique long term certificate from CA in system initialization phase. When the vehicle entered the communication range of new RSU, it requested local master keys with its certificate. The validity of communication message between vehicle and vehicle are guaranteed through mutual authentication process. After collecting the valid master keys, vehicle created the localized anonymous identity to mark safety-related message. When node is cooperated, CA invalidated their unique certificate. The safety-related message is verified by single or batch manner to enhance the authentication efficiency. In Expedite Message Authentication Protocol (EMAP) and Anonymous Batch AutHentication (ABAH), certificate used to verify the validity of safety-related message. For every received message, it computed the Hash Message Authentication Code (HMAC) and authenticate certificate. The certificate selected to authenticate validity of the nodes. CRL checking and certificate verification were implemented on mutual authentication between RSU and vehicle. The validity of safety-related message is verified by identity-based signature. Vehicle created the pseudonym after collecting the master keys from RSU. EMAP and ABAH pseudonym allocated by the CA. RSU allocates and modernizes their local master keys separately in LIAP and ABAH.

**\\Local Identity-based anonymous message Authentication Algorithm\\**

Vehicle $V_i$ authenticates hello message $M_h$
**Require:** Receive a hello message

```
Step 1: Check $T_e$
Step 2: If $T_e$ is valid then
          Check $PK_{RI}$ whether $R_i$ is a new RSU
Step 3: If $PK_{RI} = New$ then
          Check $Cert_{Ri}$ against the RCRL
Step 4: If $Cert_{Ri} \notin RCRL$ then
          Verify $Cert_{Ri}$ and $\sigma_{Ri}$
Step 5: If $Cert_{Ri} = true$ and $\sigma_{Ri} = true$ then
Step 6: Store $(RPK_i^1, RPK_i^2)$
Step 7: Store $(RPD_{i-1}^1, RPD_{i-1}^2, RPD_{i+1}^1, RPD_{i+1}^2)$
Step 8: Send a request message $M_r$ to $R_i$
          End if
          End if
          End if
          End if
```

The above algorithm explains the algorithmic process of local identity-based anonymous message authentication algorithm. A hybrid authentication protocol proposed on PKI and identity-based signature that meet the needs of security and conditional privacy in VANETs. Every node comprises long term PKI-based certificate to authenticate the node validity. For safety-related message, vehicle creates the localized anonymous identity to mark it. The mutual authentication between the RSU and vehicle guarantee that vehicle communicates with the unrevoked RSU and valid vehicle gathers the local master keys. For increasing the authentication efficiency, node verify safety-related message by single or batch authentication manner. CA manages revoked certificates by the RSU Certificate Revocation List (RCRL) and the Vehicle Certificate Revocation List (VCRL). When the node gets compromised, CA revokes their certificate. The time-consuming CRL checking is executed in mutual authentication process avoided in message authentication of V2V communication.

### 3.2 A New Greedy Behavior Attack Detection Algorithm for VANETs

Vehicular Ad hoc Networks is used to provide the road safety and enhance the driving conditions. VANET were exposed to many types of attacks like Denial of Service (DoS) attacks that affect the availability of given services for legitimate users. A new detection approach termed Greedy Detection for VANETs (GDVAN) developed for greedy behavior attacks in VANETs. The detection approach comprises two phases termed suspicion phase and the decision phase. The suspicion phase based on linear regression mathematical ideas while decision phase depending on fuzzy logic decision scheme. The designed algorithm identified the existence of greedy behavior and established list of compromised nodes by newly defined metrics.

GDVAN used three defined metrics for greedy detection in high mobile environment like VANET. The connection is short and nodes not have sufficient amount of time to execute the adaptive manipulation of backoff parameters. It comprised both suspicion and decision phases to enhance linear regression and fuzzy logic ideas. In through monitoring the network traffic traces, the algorithm affirms the existence. In affirmative case, it identified the dependable nodes. GDVAN are passive, non-resource-intensive and failed to need variations in MAC layer. It is transparent to the users and it executed by any node of the network.

```
\\ Greedy Detection Algorithm\\
INPUT: T= Monitoring speed,
       State_Greedy=False
OUTPUT: Annonce_Greedy(State_Greedy)
Begin
Repeat
  Step 1: Collect traffic traces during T
  Step 2: Calculate correlation coefficient '$\rho$'
  Step 3: If $\rho$ is close to 1 then
            Goto (8)
            Else
            Goto (13)
            end
    Step 4: Calculate slope of the linear regression
            straight
    Step 5: If the slope is close to 1 then
            State_Greedy= FALSE
          else run (13)
          end
    Step 6: Greedy behavior is suspected: Return and run
           watchdog supervision tool
    Step 7: Return; Annonce_Greedy(State_Greedy)
    Step 8: until no existing communication
            End
```

The above algorithm describes the greedy detection process in VANET. A new decision scheme developed for identifying the greedy behavior for VANETs. The designed scheme identified the nodes to violate the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol rules to increase their bandwidth at expense of the well-behaving nodes. The newly defined metrics are convenient to high mobile networks and employed during the short monitoring periods. In watchdog detection software, three newly defined metrics for each node in VANET used are:

- Number of connection attempts
- Average of connection duration
- Average of waiting times between connection

From the fuzzy logic, existence of greedy behavior from certain value of parameter is imagined. In between two threshold values, suspicion is slow. The idea is depending on use of tools presented by fuzzy logic theory.

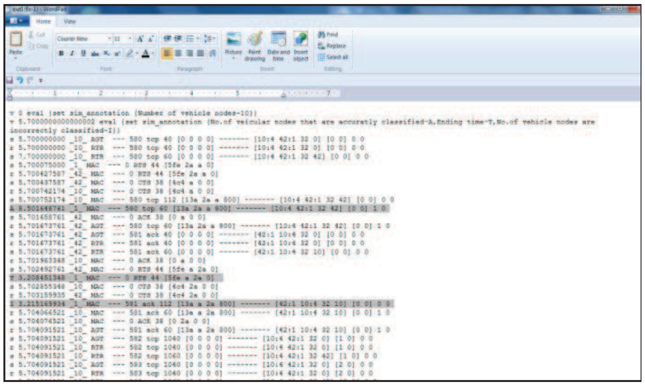
### 3.3 A Novel and Efficient Conditional Privacy- Preserving Authentication scheme for VANET (NECPPA)

Vehicular Ad-hoc Networks are developing one in recent years for providing real-time communication between vehicles safer and more comfortable driving. The key objective of VANET is to broadcast the ad-hoc messages like traffic incidents and emergency events. VANETs are safe and commercialized. It connects the central stations or internet through VANETs to exchange the data. VANETs are one of the key components of intelligent transportation systems. The main objective of direct communication is vehicle safety and traffic minimization. VANETs are unique type of MANETs where the vehicles in VANET represent the nodes. Vehicles detect the additional vehicles to form the network by connecting them and perform suitable communications. The node movement is selected property of networks that allows them to vary their pattern immediately.

A Novel Efficient Conditional Privacy Preserving Authentication (NECPPA) scheme developed for VANETs which is mixture of Tamper Proof Device Based (TPDB) and Road Side Unit Based (RSUB) techniques. In this scheme, authentication of vehicles carried out without the group signature. The signature verification of this scheme not increases linearly with number of revoked vehicles. The revocation process scheme is efficient than anonymous certificate schemes when the revocation of vehicles not increases CRL suddenly. The verifier not verifies the CRL for every signature. The sensitive information and master key of Trusted Authority (TA) were not in tamper proof device of vehicles but they were stored in RSU tamper proof devices. RSUs include the direct, fast and secure communicational link with TA that make easier and faster to modernize the system parameters and revoke vehicles. The compromise of single vehicle failed to imply varying parameters of whole network and re-registration of all vehicles. The vehicles require contacting the RSUs when they enter area covered by them. The signature verification is carried out by vehicles without any online RSUs.

## 4. COMPARISON OF AUTHENTICATION AND PRIVACY PRESERVING TECHNIQUES FOR SECURED COMMUNICATION

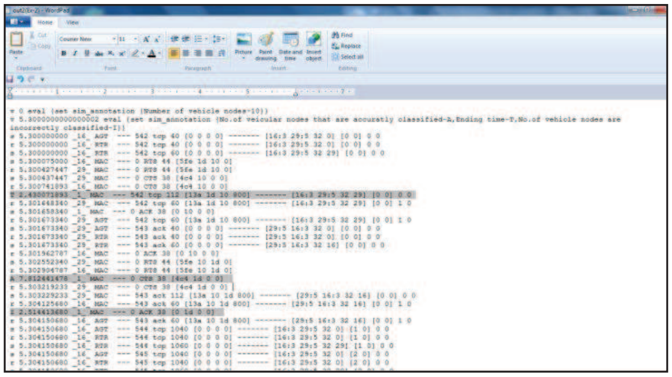
In order to compare the authentication and privacy preserving techniques for secured communication in VANET, number of vehicular nodes is considered to perform the experiment. Various parameters are used in authentication and privacy preserving techniques for secured communication in VANET. The coding output screenshots of LIAP, GDVAN and NECPPA scheme is described in fig.1.1, fig. 1.2 and fig. 1.3 respectively.



```
v 0 eval (set sim_annotation (Number of vehicle nodes-10))
v 5.7000000000000002 eval (set sim_annotation (No.of veicular nodes that are accuratly classified-A,Ending time-T,No.of vehicle nodes are
incorrectly classified-I))
s 5.700000000 _10_ AGT  --- 580 tcp 40 [0 0 0 0] ------- [10:4 42:1 32 0] [0 0] 0 0
r 5.700000000 _10_ RTR  --- 580 tcp 40 [0 0 0 0] ------- [10:4 42:1 32 0] [0 0] 0 0
s 7.700000000 _10_ RTR  --- 580 tcp 60 [0 0 0 0] ------- [10:4 42:1 32 42] [0 0] 0 0
s 5.700075000 _1_ MAC  --- 0 RTS 44 [5fe 2a a 0]
r 5.700427587 _42_ MAC  --- 0 RTS 44 [5fe 2a a 0]
s 5.700437587 _42_ MAC  --- 0 CTS 38 [4c4 a 0 0]
r 5.700742174 _10_ MAC  --- 0 CTS 38 [4c4 a 0 0]
s 5.700752174 _10_ MAC  --- 580 tcp 112 [13a 2a a 800] ------- [10:4 42:1 32 42] [0 0] 0 0
A 8.501648761 _1_ MAC  --- 580 tcp 60 [13a 2a a 800] ------- [10:4 42:1 32 42] [0 0] 1 0
s 5.701658761 _42_ MAC  --- 0 ACK 38 [0 a 0 0]
r 5.701673761 _42_ AGT  --- 580 tcp 60 [13a 2a a 800] ------- [10:4 42:1 32 42] [0 0] 1 0
s 5.701673761 _42_ AGT  --- 581 ack 40 [0 0 0 0] ------- [42:1 10:4 32 0] [0 0] 0 0
r 5.701673761 _42_ RTR  --- 581 ack 40 [0 0 0 0] ------- [42:1 10:4 32 0] [0 0] 0 0
s 5.701673761 _42_ RTR  --- 581 ack 60 [0 0 0 0] ------- [42:1 10:4 32 10] [0 0] 0 0
r 5.701963348 _10_ MAC  --- 0 ACK 38 [0 a 0 0]
s 5.702492761 _42_ MAC  --- 0 RTS 44 [5fe a 2a 0]
T 3.208451348 _1_ MAC  --- 0 RTS 44 [5fe a 2a 0]
s 5.702855348 _10_ MAC  --- 0 CTS 38 [4c4 2a 0 0]
r 5.703159935 _42_ MAC  --- 0 CTS 38 [4c4 2a 0 0]
I 3.215169934 _1_ MAC  --- 581 ack 112 [13a a 2a 800] ------- [42:1 10:4 32 10] [0 0] 0 0
r 5.704066521 _10_ MAC  --- 581 ack 60 [13a a 2a 800] ------- [42:1 10:4 32 10] [0 0] 1 0
s 5.704076521 _10_ MAC  --- 0 ACK 38 [0 2a 0 0]
r 5.704091521 _10_ AGT  --- 581 ack 60 [13a a 2a 800] ------- [42:1 10:4 32 10] [0 0] 1 0
s 5.704091521 _10_ AGT  --- 582 tcp 1040 [0 0 0 0] ------- [10:4 42:1 32 0] [1 0] 0 0
r 5.704091521 _10_ RTR  --- 582 tcp 1040 [0 0 0 0] ------- [10:4 42:1 32 0] [1 0] 0 0
s 5.704091521 _10_ RTR  --- 582 tcp 1060 [0 0 0 0] ------- [10:4 42:1 32 42] [1 0] 0 0
s 5.704091521 _10_ AGT  --- 583 tcp 1040 [0 0 0 0] ------- [10:6 42:1 32 0] [2 0] 0 0
r 5.704091521 _10_ RTR  --- 583 tcp 1040 [0 0 0 0] ------- [10:4 42:1 32 0] [2 0] 0 0
```

**Fig. 1.1 Output Screenshot for LIAP**

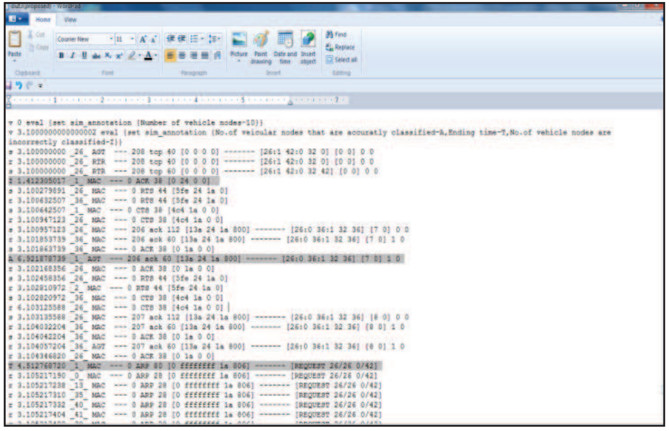
In fig. 1.1, the output for LIAP is given. The number of nodes that are accurately classified, ending time and number of nodes that are incorrectly classified values are obtained for LIAP in the simulation outputs. These values are substituted in equ. (1), (2) and (3) to obtain the authentication accuracy, authentication time and false positive rate of LIAP. In fig. 1.2, the coding result of GDVAN is illustrated.



```
v 0 eval (set sim_annotation (Number of vehicle nodes-10))
v 5.3000000000000002 eval (set sim_annotation (No.of veicular nodes that are accuratly classified-A,Ending time-T,No.of vehicle nodes are
incorrectly classified-I))
s 5.300000000 _16_ AGT  --- 542 tcp 40 [0 0 0 0] ------- [16:3 29:5 32 0] [0 0] 0 0
r 5.300000000 _16_ RTR  --- 542 tcp 40 [0 0 0 0] ------- [16:3 29:5 32 0] [0 0] 0 0
s 5.300000000 _16_ RTR  --- 542 tcp 60 [0 0 0 0] ------- [16:3 29:5 32 29] [0 0] 0 0
s 5.300075000 _16_ MAC  --- 0 RTS 44 [5fe 1d 10 0]
r 5.300427447 _29_ MAC  --- 0 RTS 44 [5fe 1d 10 0]
s 5.300437447 _29_ MAC  --- 0 CTS 38 [4c4 10 0 0]
r 5.300741893 _16_ MAC  --- 0 CTS 38 [4c4 10 0 0]
T 2.430071893 _1_ MAC  --- 542 tcp 112 [13a 1d 10 800] ------- [16:3 29:5 32 29] [0 0] 0 0
r 5.301648340 _29_ MAC  --- 542 tcp 60 [13a 1d 10 800] ------- [16:3 29:5 32 29] [0 0] 1 0
s 5.301658340 _1_ MAC  --- 0 ACK 38 [0 10 0 0]
r 5.301673340 _29_ AGT  --- 542 tcp 60 [13a 1d 10 800] ------- [16:3 29:5 32 29] [0 0] 1 0
s 5.301673340 _29_ AGT  --- 543 ack 40 [0 0 0 0] ------- [29:5 16:3 32 0] [0 0] 0 0
r 5.301673340 _29_ RTR  --- 543 ack 40 [0 0 0 0] ------- [29:5 16:3 32 0] [0 0] 0 0
s 5.301673340 _29_ RTR  --- 543 ack 60 [0 0 0 0] ------- [29:5 16:3 32 16] [0 0] 0 0
r 5.301962787 _16_ MAC  --- 0 ACK 38 [0 10 0 0]
s 5.302552340 _29_ MAC  --- 0 RTS 44 [5fe 10 1d 0]
r 5.302904787 _16_ MAC  --- 0 RTS 44 [5fe 10 1d 0]
A 7.812441478 _1_ MAC  --- 0 CTS 38 [4c4 1d 0 0]
r 5.303219233 _29_ MAC  --- 0 CTS 38 [4c4 1d 0 0]
s 5.303229233 _29_ MAC  --- 543 ack 112 [13a 10 1d 800] ------- [29:5 16:3 32 16] [0 0] 0 0
r 5.304125680 _16_ MAC  --- 543 ack 60 [13a 10 1d 800] ------- [29:5 16:3 32 16] [0 0] 1 0
I 2.514413680 _1_ MAC  --- 0 ACK 38 [0 1d 0 0]
r 5.304150680 _16_ AGT  --- 543 ack 60 [13a 10 1d 800] ------- [29:5 16:3 32 16] [0 0] 1 0
s 5.304150680 _16_ AGT  --- 544 tcp 1040 [0 0 0 0] ------- [16:3 29:5 32 0] [1 0] 0 0
r 5.304150680 _16_ RTR  --- 544 tcp 1040 [0 0 0 0] ------- [16:3 29:5 32 0] [1 0] 0 0
s 5.304150680 _16_ RTR  --- 544 tcp 1060 [0 0 0 0] ------- [16:3 29:5 32 29] [1 0] 0 0
s 5.304150680 _16_ AGT  --- 545 tcp 1040 [0 0 0 0] ------- [16:3 29:5 32 0] [2 0] 0 0
r 5.304150680 _16_ RTR  --- 545 tcp 1040 [0 0 0 0] ------- [16:3 29:5 32 0] [2 0] 0 0
```

**Fig. 1.2 Output Screenshot for GDVAN**

In fig. 1.2, the output for the GDVAN is given. The number of nodes that are accurately classified, ending time and number of nodes that are incorrectly classified values are obtained for GDVAN in the simulation outputs. These values are substituted in equ. (1), (2) and (3) to obtain the authentication accuracy, authentication time and false positive rate of GDVAN. In fig. 1.3, the coding result of NECPPA scheme is provided.



```
v 0 eval (set sim_annotation (Number of vehicle nodes-10))
v 3.1000000000000002 eval (set sim_annotation (No.of veicular nodes that are accuratly classified-A,Ending time-T,No.of vehicle nodes are
incorrectly classified-I))
s 3.100000000 _26_ AGT  --- 208 tcp 40 [0 0 0 0] ------- [26:1 42:0 32 0] [0 0] 0 0
r 3.100000000 _26_ RTR  --- 208 tcp 40 [0 0 0 0] ------- [26:1 42:0 32 0] [0 0] 0 0
s 3.100000000 _26_ RTR  --- 208 tcp 60 [0 0 0 0] ------- [26:1 42:0 32 42] [0 0] 0 0
I 1.412305017 _1_ MAC  --- 0 ACK 38 [0 24 0 0]
s 3.100279891 _26_ MAC  --- 0 RTS 44 [5fe 24 1a 0]
r 3.100632507 _36_ MAC  --- 0 RTS 44 [5fe 24 1a 0]
s 3.100642507 _1_ MAC  --- 0 CTS 38 [4c4 1a 0 0]
r 3.100947123 _26_ MAC  --- 0 CTS 38 [4c4 1a 0 0]
s 3.100957123 _26_ MAC  --- 206 ack 112 [13a 24 1a 800] ------- [26:0 36:1 32 36] [7 0] 0 0
r 3.101853739 _36_ MAC  --- 206 ack 60 [13a 24 1a 800] ------- [26:0 36:1 32 36] [7 0] 1 0
s 3.101863739 _36_ MAC  --- 0 ACK 38 [0 1a 0 0]
A 6.921878739 _1_ AGT  --- 206 ack 60 [13a 24 1a 800] ------- [26:0 36:1 32 36] [7 0] 1 0
r 3.102168356 _26_ MAC  --- 0 ACK 38 [0 1a 0 0]
s 3.102458356 _26_ MAC  --- 0 RTS 44 [5fe 24 1a 0]
r 3.102810972 _2_ MAC  --- 0 RTS 44 [5fe 24 1a 0]
s 3.102820972 _36_ MAC  --- 0 CTS 38 [4c4 1a 0 0]
r 6.103125588 _26_ MAC  --- 0 CTS 38 [4c4 1a 0 0]
s 3.103135588 _26_ MAC  --- 207 ack 112 [13a 24 1a 800] ------- [26:0 36:1 32 36] [8 0] 0 0
r 3.104032204 _36_ MAC  --- 207 ack 60 [13a 24 1a 800] ------- [26:0 36:1 32 36] [8 0] 1 0
s 3.104042204 _36_ MAC  --- 0 ACK 38 [0 1a 0 0]
r 3.104057204 _36_ AGT  --- 207 ack 60 [13a 24 1a 800] ------- [26:0 36:1 32 36] [8 0] 1 0
r 3.104346820 _26_ MAC  --- 0 ACK 38 [0 1a 0 0]
T 4.512768720 _1_ MAC  --- 0 ARP 80 [0 ffffffff 1a 806] ------- [REQUEST 26/26 0/42]
r 3.105217190 _0_ MAC  --- 0 ARP 28 [0 ffffffff 1a 806] ------- [REQUEST 26/26 0/42]
r 3.105217238 _13_ MAC  --- 0 ARP 28 [0 ffffffff 1a 806] ------- [REQUEST 26/26 0/42]
r 3.105217310 _35_ MAC  --- 0 ARP 28 [0 ffffffff 1a 806] ------- [REQUEST 26/26 0/42]
r 3.105217332 _40_ MAC  --- 0 ARP 28 [0 ffffffff 1a 806] ------- [REQUEST 26/26 0/42]
r 3.105217404 _41_ MAC  --- 0 ARP 28 [0 ffffffff 1a 806] ------- [REQUEST 26/26 0/42]
```

**Fig. 1.3 Output Screenshot for NECPPA scheme**

In fig. 1.3, the output for NECPPA scheme is described. The number of nodes that are accurately classified, ending time and number of nodes that are incorrectly classified values are obtained in simulation outputs for NECPPA scheme. These values are substituted in equ. (1), (2) and (3) to obtain the authentication accuracy, authentication time and false positive rate of GDVAN. In fig. 1.3, the coding result of NECPPA scheme is provided. Based on the values obtained, the table values are given in table 1.1, table 1.2 and table 1.3.

## 4.1 Authentication Accuracy

Authentication accuracy is defined as the ratio of number of vehicular nodes that are accurately authenticated to the total number of vehicular nodes. It is measured in terms of percentage (%) using the equ. (1).

$$Authentication\ accuracy = \frac{Number\ of\ vehicular\ nodes\ that\ are\ accurately\ authenticated}{Total\ number\ of\ vehicular\ nodes} * 100 \text{ equ...} \qquad (1)$$

From the equ.(1), the authentication accuracy is calculated. When the authentication accuracy is higher, that method is more efficient.

**Table. 1.1 Comparison of Authentication Accuracy**

| Number of Vehicular Nodes (Number) | Authentication Accuracy (%) | | |
|---|---|---|---|
| | LIAP | GDVAN | NECPP A Scheme |
| 10 | 85 | 78 | 69 |
| 20 | 87 | 80 | 71 |
| 30 | 88 | 82 | 73 |
| 40 | 91 | 79 | 77 |
| 50 | 89 | 77 | 75 |
| 60 | 86 | 75 | 70 |
| 70 | 88 | 78 | 72 |
| 80 | 90 | 81 | 74 |
| 90 | 93 | 83 | 76 |
| 100 | 95 | 85 | 78 |

From the table. 1.1 describes the authentication accuracy with respect to number of vehicular nodes ranging from 10 to 100. Authentication accuracy compares with local identity-based anonymous message authentication protocol, Greedy Detection for VANETs and novel efficient conditional privacy preserving authentication scheme. From the table 1.1, it is observed that the authentication accuracy using local identity-based anonymous message authentication protocol is higher when compared to Greedy Detection for VANETs and novel efficient conditional privacy preserving authentication scheme. The graphical representation of authentication accuracy as shown in fig. 1.4.

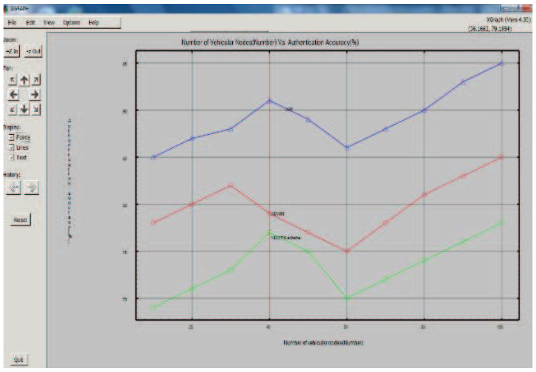

XGRAPH
File Edit View Options Help
XGraph (Vers 4.30)
(36.1663, 79.1954)
Zoom:
Pan:
Display:
Points
Lines
Text
History:
Reset
Quit
Number of Vehicular Nodes(Number) Vs. Authentication Accuracy(%)
Authentication accuracy(%)
LIAP
GDVAN
NECPPA scheme
Number of vehicular nodes(Number)
20
40
60
80
100

**Fig. 1.4 Measure of Authentication Accuracy**

From the fig. 1.4, authentication accuracy based on different number of vehicular node is explained. From the fig. 1.4, it is observed that the authentication accuracy using local identity-based anonymous message authentication protocol is higher when compared to Greedy Detection approach for VANETs and novel efficient conditional privacy preserving authentication scheme. Hybrid authentication protocol based on PKI and identity-based signature meet requirements of security and conditional privacy in VANETs. Every node includes the long term PKI-based certificate to authenticate node validity. For safety-related message, vehicle creates localized anonymous identity to mark it. This local identity-based anonymous message authentication protocol provides 12% higher authentication accuracy than GDVAN approach and consumes 21% higher authentication accuracy than novel efficient conditional privacy preserving authentication scheme.

## 4.2Authentication Time

Authentication time is defined as amount of time taken to perform the authentication for secured communication in VANET. The difference of starting time and ending time during the authentication for secured communication is called authentication time. It is measured in terms of milliseconds (ms) using the equ. (2).

$$Authentication\ Time = Ending\ time - starting\ time\ of\ node\ authentication \quad equ\ldots..(2)$$

From the equ. (2) authentication time is calculated. When the authentication time is low, the method is more efficient.

**Table 1.2 Comparison of Authentication Time**

| Number of Vehicular Nodes (Number) | Authentication Time (ms) | | |
|---|---|---|---|
| | LIAP | GDVAN | NECPPA scheme |
| 10 | 32 | 24 | 45 |
| 20 | 35 | 27 | 47 |
| 30 | 38 | 30 | 51 |
| 40 | 42 | 33 | 53 |
| 50 | 46 | 36 | 57 |
| 60 | 43 | 34 | 55 |
| 70 | 40 | 31 | 52 |
| 80 | 44 | 35 | 56 |
| 90 | 47 | 38 | 60 |
| 100 | 50 | 41 | 64 |

Table 1.2 discusses the authentication time with respect to number of vehicular nodes in the range 10 to 100. The authentication time compared with local identity-based anonymous message authentication protocol, Greedy Detection for VANETs and Conditional privacy preserving authentication scheme. From the table 1.2, it shows the authentication time using Greedy Detection for VANETs is less when compared to local identity-based anonymous message authentication protocol and novel efficient conditional privacy preserving authentication scheme. The graphical representation of authentication time is illustrated in fig. 1.5.

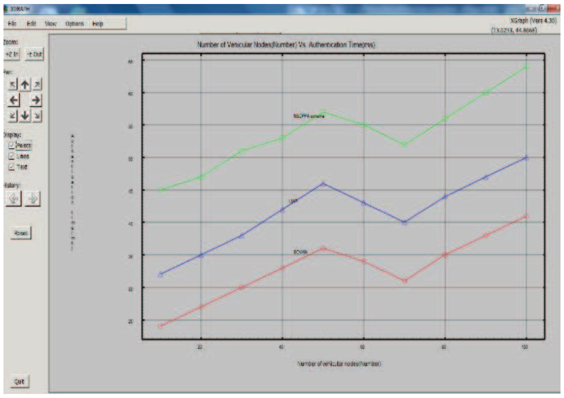


**Fig. 1.5 Measure of Authentication Time**

In fig. 1.5, authentication time based on different number of vehicular node is described. From the fig. 1.5, authentication time using Greedy Detection approach for VANETs is less when compared to local identity-based anonymous message authentication protocol and novel efficient conditional privacy preserving authentication (NECPPA) scheme. Because, GDVAN have suspicion phase and decision phase. Suspicion phase depend on linear regression mathematical ideas while decision phase depend on fuzzy logic decision scheme. The algorithm is identified the existence of greedy behavior and established list of compromised nodes through newly defined metrics. GDVAN approach consumes 21% low authentication time than local identity-based anonymous message authentication protocol and consumes 39% less authentication time than novel efficient conditional privacy preserving authentication scheme.

### 4.3 False Positive Rate

False positive rate is defined as ratio of number of vehicular nodes that are incorrectly classified to the total number of vehicular nodes. It is measured in terms of percentage (%) using the equ. (3).

$$False\ positive\ Rate = \frac{Number\ of\ vehicular\ nodes\ that\ are\ incorrectly\ classified}{Total\ number\ of\ vehicular\ nodes} * 100 \quad equ\ldots..(3)$$

From the equ. (3), the false positive rate is calculated. When the false positive rate is low, the method is more efficient.

**Table 1.3 Comparison of False Positive Rate**

| Number of Vehicular Nodes (Number) | False Positive Rate (%) | | |
|---|---|---|---|
| | LIAP | GDVAN | NECPPA scheme |
| 10 | 32 | 25 | 14 |
| 20 | 35 | 27 | 16 |
| 30 | 37 | 30 | 19 |
| 40 | 41 | 32 | 22 |
| 50 | 43 | 35 | 26 |
| 60 | 39 | 31 | 23 |
| 70 | 42 | 34 | 25 |
| 80 | 45 | 36 | 28 |
| 90 | 47 | 39 | 31 |
| 100 | 50 | 42 | 34 |

Table 1.3 shows the false positive rate with number of vehicular nodes varies from 10 to 100. False positive rate comparison takes place on local identity-based anonymous message authentication protocol, Greedy Detection for VANETs and novel efficient conditional privacy preserving authentication scheme. The graphical representation of false positive rate is shown in fig. 1.6.

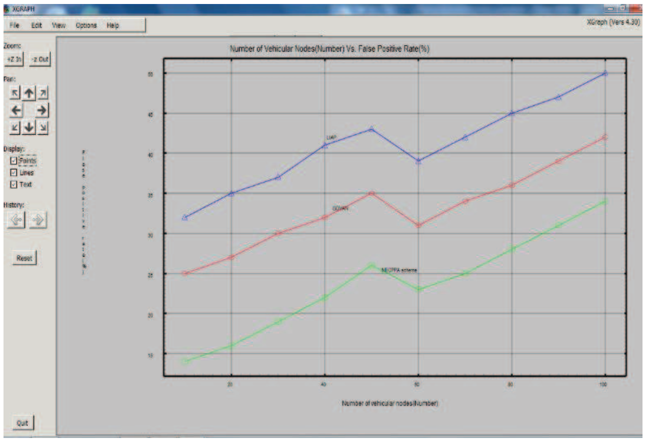


Fig. 1.6 Measure of False Positive Rate

From the fig.1.6, false positive rate based on different number of vehicular node is explained. From the fig. 1.6, it describes the false positive rate using novel efficient conditional privacy preserving authentication scheme is less when compared to local identity-based anonymous message authentication protocol and Greedy Detection for VANETs. Because of authentication vehicles are carried out without group or ring signature. The signature verification of designed scheme not increases linearly with number of revoked vehicles. The revocation process of design the scheme efficient than anonymous certificate schemes when revocation of vehicles not enhances CRL suddenly. A novel efficient conditional privacy preserving authentication scheme has 43% low false positive rate than local identity-based anonymous message authentication protocol and consumes 29% low false positive rate than Greedy Detection for VANETs.

## 5. DISCUSSION ON LIMITATION OF AUTHENTICATION AND PRIVACY PRESERVING TECHNIQUES FOR SECURED COMMUNICATION

LIAP was developed for VANETs where every vehicle and Road Side Unit (RSU) assigned with distinctive long term certification. Hybrid authentication protocol depending on PKI and identity-based signature enhances the security level and conditional privacy level in VANETs. The valid vehicle collected local master keys from RSU to produce the localized anonymous identity. Node authenticates the safety-related message through single authentication manner for increasing the authentication efficiency. But, the authentication overhead is not reduced using LIAP. Greedy Detection for VANETs developed for identifying the greedy behavior attacks in VANETs. The algorithm identified the existence of greedy behavior and established list of compromised nodes. GDVAN are passive, non-resource-intensive and failed to need variations in Medium Access Control (MAC) layer. The designed approach executed by any node of network and failed to require any modification of IEEE 802.11p standard. But, the reaction method against the greedy attacks not used in GDVAN approach to eliminate serious impacts.

NECPPA employed the keys and essential parameters of system in Tamper Proof Device (TPD) of Road Side Units (RSUs). A secure and fast communicational link between TA and RSU insert TPD in RSU is efficient. The designed scheme for cost efficient than other online RSUB scheme it failed to need establishment of on-line RSUs in whole roads. The privacy preserving rate not improved using NECPPA.

## 6. CONCLUSION

The comparison of different existing authentication and privacy preserving techniques for secured communication in VANET is studied. From the study, it is observed that existing techniques failed to reduce the authentication overhead using LIAP. The existing reaction method against the greedy attacks was not used in GDVAN approach to eliminate serious impacts. Further, the privacy preserving rate not improved using NECPPA. The wide range of experiments on existing methods computes the performance of many authentication and privacy preserving techniques for secured communication in VANET with limitations. In this research, work can be carried out using machine learning and cryptographic techniques for enhancing authentication and privacy preservation performance during communication in VANET.

## REFERENCES

[1] Shibin Wang and Nianmin Yao, “LIAP: A local identity-based anonymous message authentication protocol in VANETs”, Computer Communications, Elsevier, Vol. 112, Pp. no.154–164, 2017.

[2] Mohamed Nidhal Mejri and Jalel Ben-Othman, “GDVAN: A New Greedy Behavior Attack Detection Algorithm for VANETs”, Journal of IEEE Transaction on Mobile Computing, Vol. 16, Iss.3, Pp. no 759–771, 2017.

[3] Seyed Morteza Pournaghi, Behnam Zahednejad, Majid Bayat and Yaghoub Farjami “NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET”, Computer Networks, Springer, Vol. 134, Pp. no. 78–92, 2018.

[4] Hyo Jin Jo, In Seok Kim and Dong Hoon Lee “Reliable Cooperative Authentication for Vehicular Networks” IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Intelligent Transportation Systems, Vol. 19, Iss. 4, Pp. no. 1065–1079, 2018.

[5] Jian Kang, Dan Lin, Wei Jiang and Elisa Bertino, “Highly efficient randomized authentication in VANETs”, Pervasive and Mobile Computing, Elsevier, Vol. 44, Pp. no 31–44, 2018.

[6] Xia Feng, Chun-yan Li, De-xin Chen and Jin Tang, “A method for defensing against multi-source Sybil attacks in VANET”, Peer-to-Peer Networking and Applications, Springer, Vol. 10, Iss. 2, Pp. no. 305–314, 2017

[7] Jieqiong Chen and Guoqiang Mao “On the security of warning message dissemination in vehicular Ad hoc networks”, Journal of Communications and Information Networks, Springer, Vol. 2, Iss. 2, Pp. no. 46–58, 2017

[8] SK Hafizul Islam, Mohammad S. Obaidat, Pandi Vijayakumarc, Enas Abdulhayd, Fagen Lie, M Krishna Chaitanya Reddyf, “A Robust and Efficient Password-based Conditional Privacy Preserving Authentication and Group-Key Agreement Protocol for VANETs”, Future Generation Computer Systems, Elsevier, Vol. 84, Pp. no. 216-227, 2018

[9] Lei Zhang, QianhongWu, Josep Domingo-Ferrer, Bo Qin, and Chuanyan Hu, “Distributed Aggregate Privacy-Preserving Authentication in VANETs”, IEEE Transactions on Intelligent Transportation Systems, Vol. 18, Iss. 3, Pp. no. 516 – 526, 2017