International Journal of Engineering &Technology, 7 (3.12) (2018) 1102 -1111

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Broadcast Message Authentication Mechanism to Detect Clone and Sybil attacks in VANET's based on ID-Based Signature Scheme

Kareemulla Shaik[1*], Md. Ali Hussain[2]

[1]Research Scholar, Department of Computer science and Engineering, KLEF Guntur
[2]Professor, Department of Computer science and Engineering, KLEF Guntur
**Corresponding Author E-mail: [1]kareem.mtech@gmail.com , [2]alihussain.phd@gmail.com*

Abstract

Broadcast Communication is crucial in VANET communication, to send and receive safety messages within network. Securing these beacon message is a challenge, since they are very prone to clone and Sybil attacks. Many works have been proposed to address this problem but they failed to address how to detect and protect these messages from clone attacks and also limited to static networks with limited data sizes. To achieve this a secure authentication and attack detection mechanism can be designed. In this paper we propose a secure broadcast message authentication and attack detection mechanism with Identity – Based Signatures. Experimental results proved that it can be used in both V2V and V2RSU c communications. Our scheme shown best performance compared to existing schemes in terms of packet delivery ration, detection rate and detection time.

***Keywords**: Authentication protocol, integrity verification, clone attacks, Sybil attack ID-Based Signatures.*

1. Introduction

VANET (Vehicular Ad-hoc Network) is a wireless network which provides communication between vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) in a static and dynamic way. VANET applications are based on vehicles' onboard units and roadside units to broadcast necessary messages throughout the process of communication. Hence, there is still necessity of an advanced and effective authentication and verification approach. There has been extensive amount of research works carried out in order to develop an advanced an effective authentication and verification scheme for VANET. Nowadays, vehicles are manufactured with integration of embedded processors. Such vehicles can communicate among themselves with the help of wireless broadcast system. These vehicles are known as smart vehicles. The prime objective of this technique is to enhance the safety of driving. Let us consider an example to prevent accidents, to request urgent help, report crashes, etc.

Co-operative driving is an efficient driving mechanism in which it helps to use roads in an efficient way. Traffic optimization process is used for prevention of traffic jams. Additional services are included for smart vehicles, those are: - payment of tolls, automatic re-fueling and infotainment. Vehicles are required to be communicated among themselves. The safety messages transmitted by vehicles are categorized into three groups and those are described below: -

1. Periodic Messages: - These types of messages are sent at a interval. This interval is usually 10-100ms. This type of message usually includes general traffic information. Messages are sent to other vehicles or other infrastructures.

2. General Safety Messages: - Such kind of messages are generally used during the process of co-operative driving. Prevention of accidents is the prime objective of such type of messages.

3. Liability Messages: - These messages are meant for liability-related incidents such as, reporting crash. Such messages are only broadcasted by vehicles. No node-to-node communication is allowed here. Confidentiality is not considered as a vital factor here.

In order to prevent both insider and outsider attacks, every individual vehicle is required to authenticate itself. Data integrity must be maintained in order to prevent active attacks such as addition of bogus information and replay attack.

Let us consider an example of Cooperative Collision Warning (CCW) application where vehicles usually interchange its location and speed in order to prevent accidents. This technique considers periodic beacon messages for its working. The Congested Road Notification (CRN) application can inform other approaching vehicles about the status of a traffic jam. VANET applications completely depend upon vehicles' onboard units to broadcast necessary messages.

Non-repudiation is necessary to prevent vehicles from rejecting the creation of sent messages. In traditional system, both broadcast authentication and non-repudiation can be achieved with the help of Elliptic Curve Digital Signature Algorithm (ECDSA). It has the responsibility to check each and every signature. It results huge computational overhead on OBU hardware. A standard and traditional processor needs 20 milliseconds in order to check a single signature.

In most of the cases signature flooding can happen, hence this is the major limitation of the traditional techniques. In some cases, vehicle that receives huge signed messages within a very short time period is incapable to verify all of them.

In the traditional VANET security models, the signature flooding is usually mitigated through broadcast authentication techniques.

In this case the overhead is almost equal to the entropy of broadcast messages. In order to overcome the mentioned problem of flooding, two different flooding-resilient broadcast authentication techniques are proposed, those are: - FastAuth and SelAuth. Both of these approaches depend upon the concepts of digital signature. Hence, non-repudiation can be achieved easily. No research work on lightweight broadcast authentication supports non-repudiation feature. Traditional approaches are not efficient in case of dynamic VANET applications.

1.Fast Authentication Algorithm (FastAuth):- This is basically a real-time and lightweight authentication technique. It considers the predictability of future beacon messages. Here, if there is lesser entropy of future beacon message, then the beacon message is smaller. By implementing the mentioned algorithm, a new structure is constructed which is known as chained Huffman hash trees. It involves an advanced one-time signature algorithm. The verification is 50 times faster and generation is 20 times faster as compared to ECDSA. Additionally, this technique decreases the communication overhead to 50%.

2.Selective Authentication Algorithm (SelAuth):-This algorithm is faster in terms of isolation of malicious senders. All of the unauthenticated signatures are restricted within a small area. This algorithm results very less convergence time as vehicles verify all signed messages and after that it forwards.

Security Issues of VANET:

It is very much important to detect the objectives of VANET security protocols. These security issues are necessary to find the objectives of security techniques. There are total five numbers of attributes for secure communication of VANET, those are described below:-

1.Authentication: - It is compulsory for every individual vehicle to authenticate itself, before initiation of the communication process. Unauthenticated vehicles are not permitted to transmit messages throughout the network.

2.Integrity: - The message transmitted by a vehicle can’t be modified without knowledge of the receiver.

3.Privacy/anonymity: - Usually, the identity of a vehicle is interlinked with the identity of driver. A driver never wants to show his identity to other entities. The security protocol must enforce constraints to restrict further information leakage.

4.Unlinkability: - Multiple messages transmitted by a particular vehicle must not be related with each other.

5.Traceability/ Non-Repudiation:- A sender must not refuse to send a message. This feature is basically included under the category of liability-related messages. Only higher authorities are allowed to overrule the privacy policies of a sender.

Challenges of VANET:

There are several challenges that differentiate VANET from conventional MANET.

1.Contradictory security requirements: - By enforcing authentication constraints, complete privacy can’t be achieved. Privacy and unlinkability create conflicts with traceability. In case of VANET, all the security requirements must be considered in order to develop more efficient security system.

2.Resource-constrained computing: - Every modern vehicle contains embedded processors in order to satisfy different requirements of the vehicle. Additionally, a large amount of memory is very much required for every embedded processor.

3.Low communication bandwidth: - Usually communication among vehicles are carried out with the help of broadcasting. Sometimes in case of high-density routes, network bandwidth becomes bottleneck.

4.Lossy channel: - The communication among the vehicles are carried out through a lossy channel. Therefore, various broadcast authentication techniques become inefficient, if the anchor messages are lost.

5.Highly dynamic network topology: - The nodes of VANET are mobile in nature because vehicles usually travel within the network. These nodes have high relative speed. Apart from this, we can also mention that, all the vehicles must have a restricted communication range. Maximum theoretical communication range is 1000m, but practically the range lies between 100-300m. Hence, VANET topology is modified very frequently. We all know that, two separate vehicles traveling in the opposite direction may meet one time. On the contrary, two separate vehicles traveling in the same direction can become neighbors for some time. The mobility patterns of vehicles traveling in highway are different than that of vehicles traveling at the place of crossings.

6.Unavailability of infrastructure: - Vehicles are required to connect to the infrastructure with the help of roadside units in order to satisfy their various requirements. Two example of such requirements are: - receive cryptographic credentials and report malicious activities. As roadside units are not accessible from everywhere, thus a vehicle bound to send authenticated message with or without RSU.

7.Scalability: - In case of vast network, a VANET can include huge numbers of vehicles (sometimes millions). In case of VANET, every individual vehicle must check all messages of its neighbors. But, a vehicle can sign its own message only, not others. Hence, the verification process must be more powerful as compared to the process of signing.

Authentication Schemes of VANET:

1.Hash message authentication: - Group signature technique is considered as most efficient technique and it is implemented vastly. It is basically implemented to obtain anonymous authentication in case of VANET. Most of the traditional techniques have high computational overhead during the process of message verification and signature verification. Usually, 9ms time is required for identity verification of one entity. Again, 11ms time is required in order to verify a single group signature. Let us consider an example, if total ‘n’ numbers of revoked identity are included in the CRL, then RSU is able to check 1000/(9n + 1) messages per second.

2.Proxy- based authentication: - Conventional authentication algorithms for VANET, proxy-based authentication has its own significance. Here, in this case, an OBU is implemented as a proxy in order to decrease the overall computational overhead of RSU. Initially, RSU chooses a particular OBU within its communicational range as a proxy.

In the subsequent phase, that particular proxy OBU has the responsibility to verify others outside its range. The above-presented technique can decrease 88% computational overhead and it also enhances the authentication range of roadside units significantly.

3.OTP-based authentication: - One-time password technique is considered as the most efficient and effective authentication technique nowadays. There is a requirement of a one- time pre-shared key. By implementing this technique, the plaintext is paired with a random secret key in order to obtain the lightweight ciphertext. Every individual bit is encrypted with the help of XOR operation and that particular secret key. In the subsequent time, another lightweight identity-based authentication protocol is introduced. The above mentioned lightweight identity authentication protocol is not beneficial in case of the parallel session attack. Hence, the attacker can easily forge original certification in order to get through the authentication phase.

4.Secure mutual authentication: - In the above technique, initially OBU registers itself with the certification authority. After that, the certification authority will assign certificates. At the time when a vehicle enters into the RSU’s range, the OBU transmits its certification to the RTA and the RTA has the responsibility to verify these certifications. In case of valid certificates, RTA negotiates a session key along with OBU.

This key has significant role during the encryption of communication among RSU and OBU. Apart from this, RTA have to update the said session key in each new session.

5.Public-key based protocols:-Presently, ECPP is considered as an effective scheme in order to carry out secure vehicular communication smoothly. Generally, it involves an advanced PKI signature approach for the purpose of message authentication. RSU has the responsibility to issue a short-time anonymous certificate with the help of identity-based group signature technique.

This approach is beneficial in order to handle conditional privacy, but never considers the unlink –capability of OBU. Again, the tracing process is carried out by TA with the help of RSUs. Hence, it is quite impossible to trace the original identity of the sender from that compromised RSU. In the subsequent time, another efficient technique known as REA2P is proposed. This technique includes the identity-based group signature scheme, standard re-encryption technique and the identity based key establishment technique. These certificates have the responsibility to transmit verified and authenticated messages to other vehicles within that particular network. This approach is used to obtain unlink-ability and traceability in case of multiple compromised RSUs.

6.Secret-key based protocols: - Usually, MAC technique and hash operations are required for authentication of messages transmitted among vehicles. At the receiver end, the receiver requires a key that is present inside the key packet in order to evaluate the key-signature. Here, the signatures of the received messages are verified thoroughly.

Here, HMAC method and symmetric encryption is implemented in order to sign and verify all exchanged messages in between vehicles.

7.Group signature based protocols: - This group of protocols usually involve all decentralize group authentication techniques in order to carry out the communication in between different vehicles. Every individual group is managed with the help of a single RSU and this RSU uses an efficient group signature technique. This group can efficiently broadcast messages and these messages are usually verified in that particular group, or sometimes in their neighboring groups.

Here, an efficient signature authentication and verification scheme is implemented that decreases both the signature and encryption time significantly. All vehicles inside that group are authenticated through a single RSU.

It decreases the delay time of key re-newel. In every individual RSU, secret member key is used for the authentication of the vehicle.

8.Identity-based signature protocols: - SPECS approach is included in the category of identity-based signature protocols. This technique involves an efficient batch verification process along with bloom filter in order to verify all signatures of vehicles those are transmitted by vehicles. Here, binary search technique is implemented in order to discriminate among valid and invalid signatures in every individual group.

The verification of the exchanged messages is carried out with the help of RSUs. Therefore, the receiver is unable to receive the message till it receives notification from its neighboring RSUs.

In the subsequent time, SPECS approach is modified and extended and known as b-SPECS+. This approach is an extended version of the traditional SPECS approach. This technique is usually implemented in order to prevent impersonation attack. The signature verification process is performed with the help of neighbor RSUs.

The RSU usually broadcast a notification in case of valid signature. Within that time, if the receiver goes out of that particular communication range, then it can't get any notification. The prime objective of this technique is to maintain anonymity of the original identity. Again, vehicle tracking can be prohibited with the help of this approach.

At first, every individual vehicle is needed to be registered with the Motor Vehicles Division (MVD). Pseudonyms are produced by the vehicles with the help of RSUs. The mentioned pseudonyms have significant importance in order to transmit messages to other vehicles. Identity-Based Encryption approach is implemented in order to sign messages. Every individual vehicle receives a single or multiple token(s) when it gets itself registered. Else, the vehicle will be unable to access the communication service inside that particular range. Therefore, the level of anonymity is directly proportional to the numbers of pseudonyms.

9.Group communication-based protocols: - In this scheme, no fixed infrastructure of road is considered. Each group must have a single vehicle leader. Due to the mobility, it is very complicated task to create and maintain a group for an extended period of time.

10.Self-certified signature based protocols: - This privacy preservation technique depends upon on the anonymous self-certified signature technique. Every vehicle must have a single public key and a single private key. Vehicle must request the TA to get itself certified. The TA has the responsibility to issue a witness and it is embedded inside the original identity of the vehicle. These witnesses have significant role during the signing process.

The main contributions in this paper are:

1.A novel clone node detection model in intra vehicle to vehicle (V2V), vehicle to RSU (V2RSU) communication range is proposed to improve the data communication and packet delivery ratio.

2.In the real-time traffic management systems, traditional security models are not dynamically configurable and failed to trace the exact malicious nodes using location and time. In this paper, vehicle to vehicle (V2V), vehicle to RSU (V2RSU) based authentication model is designed and implemented for effective VANET communication and data security.

3.In the proposed model, malicious vehicle are marked with good/malicious ones and change their behavior in the VANET communication.

4.Proposed V2V and V2R based authentication model optimizes the overall network efficiency in terms of time and packet delivery ratio on realistic traffic management systems.

2. Related Work

P. J. Fernandez Ruiz, et.al, implemented data authentication on mobility and security of real VANETs [1]. Two most essential aspects of VANETs are analyzed here, those are: - mobility and security. Both of these aspects are controlled by Network Mobility and Internet Key Exchange version 2 protocols. Protocols (for example, IPsec, IKEv2, EAP and NEMO) are selected in order to fulfill the requirements of various real-world applications. EAP is slightly modified and extended in order to decrease the total handover time. The modified EAP is also known as EAP-FRM. In order to analyze both the aspects of mobility and security simultaneously, two techniques are considered. Both of these techniques have distinct characteristics. The proposed technique can easily predict the occurrences of handovers.

M. Bayat, et.al, developed an advanced and secure authentication technique for VANET with batch verification [2]. VANETs can be implemented in wide range of application domains. This model not only enhance the road security, but also enhance the overall efficiency of the road transportation network. On the other hand, there are numbers of security issues which are still unresolved. Therefore, an efficient and effective authentication scheme is very much essential in order to resolve the security issues in VAENT. In this paper, every malicious vehicle generates an authenticate signature and pretend it to the other vehicles.

T. W. Chim, et.al, proposed a new ensemble classification which depends upon the basic concepts of novel classifier selection method [3]. VANET is the present day's technology which has the responsibility for inter-communication in between all vehicles. This will definitely enhance the security of traditional driving. This technique follows the basic concept of permitting all vehicles to broadcast ad hoc messages. Every other vehicle in that particular traffic can receive those broadcasted messages. Those broadcasted messages are very vulnerable in terms of security and privacy. Therefore, an efficient and reliable authentication technique is necessary. These messages must be signed and authenticated in order to gain trust. The actual identities of vehicles are still in disguise. Only authorized entity can trace the above-mentioned identities.

All of the traditional techniques directly depend upon a tamper-proof hardware device which is a major drawback of all existing models. These models never include an effective message verification technique. In order to enhance the security level, the master secret is updated initially.

A.Das and D. Roychoudhury carried out a detail survey on different authentication techniques of VANETs [4]. They have studied and analyzed all traditional and previously developed VANET authentication techniques. Vehicle to vehicle and vehicle to infrastructure authentication techniques are considered and studied here. They emphasized on different problems like anonymity, unlinkability, traceability and computation and communication overhead.

At last they analyzed the drawbacks of all previously developed authentication approaches. This technique depends upon public-key signatures that meet all the relevant security objectives significantly. They considered various directions of future research, those are mentioned below:-

1.All traditional digital signature schemes results computation overhead at the time of signature generation and verification. Every individual message that is sent by vehicles need not have long-term security.

2.All problems related to distribution and storage of CRLs is required to be resolved efficiently.

3.The cancellation of certificates is required to be embedded inside authentication approaches and these approaches depend upon hash tree. There is necessity of an effective security architecture that will satisfy all security requirements in case of VANETs.

4.Additionally, different authentication approaches must be developed.

5.Batch communication often promotes privacy and unlinkability. But, the problems related to traceability are overlooked.

M. Han, et.al, tried to focus on heavy traffic areas [5]. They proposed an advanced and effective V2V authentication scheme. Development of an advanced and most secure authentication technique is necessary in all VANETs. The prime objective of this approach is to enhance the VANET security. In order to maintain proper and effective communication, data volume is required to be decreased and the communication process must be more secure in order to prevent all network attacks. It transmits a low data volume for communication in heavy traffic areas. It is also capable to prevent replay attack with the help of timestamp method. Hence, all security systems must be integrated with authentication methods in order to prevent all kinds of attacks.

H. Hsiao, et.al, presented a flooding-resilient broadcast authentication for vehicular ad-hoc networks [6]. Digital signatures are most widely accepted security mechanism in case of VANETs because of their authenticity and non-repudiation during every broadcast communication process. Traditional methods are use broadcast authentication standard in VANETs which is vulnerable to signature flooding. Signature flooding technique can be defined as a problem which occurs at the time of vast signature verification requests.

Y. Kim and J. Lee performed a secure analysis of vehicular authentication of RSUs in case of VANETs [7]. Many authors defined VANET as a network that is responsible for providing communication among V2V and V2I. To enhance the network efficiency, stability of transmission and security of reliability are very much important. In the above-proposed approach, a new and advanced Vehicular Authentication Security Scheme (VASS) is introduced to improve the security of RSUs and OBUs. This authentication technique depends upon an efficient ID-based authentication approach that uses hi-pass card and license plate number.

Further research can be carried out to extend the VASS technique in order to implement with vehicle to infrastructure communication.

Y. Liu, Zet.al, introduced an advanced anonymous authentication protocol with the help of batch operations [8]. Security and privacy are considered as two vital factors in all vehicular networking applications. All traditional authentication mechanisms involve serialized verification operations. Therefore, those mechanisms result performance problems. In this research paper, an advanced anonymous authentication technique is presented. This technique depends upon signature along with message recovery. The presented technique is capable of authenticating multiple signatures with the help of batch operations. Hence, this technique can decrease the amount of time required for the complete process of authentication.

Y. Liu, et.al, introduced a light-weight V2I authentication protocol with the help of group communication [9]. They termed their proposed technique as LVAP. The authentication protocol has significant importance in the security of VANET. Additionally, it can prevent various known threats such as eavesdropping, replay attack, man-in-the-middle attack, etc. The presented authentication technique completely depends upon symmetric encryption, group communication, and proactive authentication approach. This technique shows optimum performance in case of high density and low-density traffic.

S. Mitra et.al, developed identification, authentication and tracking system for vehicles in VANET [10]. Identification and authentication of vehicles is a very complex research problem nowadays. VANET should take care to permit only authenticated vehicles.

In this paper, vehicle identification number VIN is considered both for identification and authentication of a particular vehicle. Every individual vehicle has the responsibility to broadcast its VIN in an encrypted format. Root level certifying authority generally checks the authentication of vehicles and produces digital signature for that particular vehicle (only when the vehicles is found authorized). When a vehicle is moving inside the particular coverage area of a vehicle, then adds the digital signature of that vehicle and also provides a proper channel for that moving vehicle. That particular channel is occupied till the vehicle is present inside the coverage of base station.

The base station is capable to track each and every authenticated vehicle inside its coverage through channel sensing method. Communication and storage overhead are two major factors those affect the overall performance of the system. Additionally, variation of VIN processing time and total number of vehicles are two other important factors those can influence the system's performance significantly.

T. Oulhaci, et.al, proposed a secured message authentication protocol in case of VANETs [11]. The main objective is to construct proper communication in between vehicles in order to enhance the road safety as well as all types of driving conditions. In the VANETs, security is the prime concern because of vast amount of wireless transmission and high topology frequency modification. In this work, they presented the most secure as well as distributed certification system in order to result secure message authentication. The local certification authorities have the responsibility to authenticate vehicles with the help of public-key certificates. The signing process is based on threshold encryption technique. It follows the basic concept of threshold cryptography to detect the compromised roadside units. These compromised roadside units may lead to issue of false public-key certificates in order to misuse the service and certification. Additionally in this research paper, they have considered the privacy factor. An attacker can very easily gather information about a particular user from the network. For example, if an attacker gets access to the pseudonyms, he or she can easily trace that user's activities and all of his or her movements. Hence, they presented an advanced system that will satisfy the unlinkability.

Y. Sun, et.al, developed a new and advanced key management system for group-signature based anonymous authentication [12]. Group signature is considered as an important cryptographic primitive for anonymous authentication. It can eliminate vast overhead from large numbers of nodes and it may cause a major problem. In order to resolve the above issue, they introduced an effective distributes key management system.

Every individual vehicle has the responsibility to update its group secret key from time to time. Local group manager plays significant role throughout the complete management process. It can also protect the updated value of the group secret key. Hence, the local manager has no idea about the updated value at the time of group key updating process. Apart from this, it can also efficiently detect all compromised local authorities as well as malicious vehicles. Malicious users can use the anonymity characteristic of group signature in order to transmit forged message on behalf of original vehicles.

Future research effort must concentrate on the discrimination of various network attacks.

M. Wang, et.al, developed a new light-weight and efficient strong privacy-preserving authentication technique for secure communication in case of VANETs [13]. Optimized authentication in VANET is an open research question till date. Secure authentication mechanism along with strong privacy preservation can make an authentication algorithm optimized. The LESPP technique uses self-generated pseudo-identity in order to verify privacy of both sender and receiver. Additionally, conditional traceability is also verified by the presented technique. Lightweight symmetric encryption along with message authentication code is vital factors during the authentication process. The proposed approach is compared with other existing traditional public key based techniques. Furthermore, it is capable of preventing denial of service (DoS) attack. The key management center has the responsibility to reveal a particular vehicle’s original identity and distinguish it from the false identity. All the vehicles in LESPP are not required to maintain certificate revocation list (CRL). Hence, all overhead created because of CRL are usually eliminated.

Y. Xie, et.al, proposed an advanced identity-based authentication technique along with conditional privacy preservation in case of VANETs [14]. According to them, each and every vehicle usually broadcast messages and transmission depend upon Dedicated Short Range Communication protocol. In order to ensure reliability and integrity, various authentication techniques are implemented. Those messages are completely time-sensitive and processed from time to time. The OBUs and RSUs have restricted computation capability and it is almost impossible to carry out large numbers of message verification. Presently, various identity-based authentication techniques those use bilinear pairing are introduced in order to enhance the overall efficiency. Bilinear pairing method is efficient for complex operations. Till date there is no such approach that will require less computation cost.

Z. Zhou,et.al, developed an extended privacy-aware handoff authentication scheme for VANETs [15]. In case of VANETs, vehicle handover from one RSU to other is performed. Authentication of vehicles is very important and authentication is required to make the vehicular communication more secure. Presently, lightweight identity authentication protocol is considered as the most promising technique in VANETs. This approach depends upon the basic concepts of dynamic session secret process. The features of traditional cryptographic algorithms are not followed here. Additionally, no user location privacy reservation is obtained through LIAP. Again, this technique is not much strong enough to prevent and avoid parallel session attack. Hence, in order to enhance the overall security, they integrated the terminal’s pseudo-identity with a random number. Proposed encryption algorithm is executed in order to encrypt the message with the help of quadratic residues operation.

H. Zhu, et.al, introduced a new privacy-preserving authentication technique for VANETs [16]. They termed their proposed approach as PPAS in short. VANET can optimize the traffic efficiency through permitting arbitrary vehicles to broadcast messages. These messages are transmitted to other vehicles and RSUs. As wireless network is open in nature, hence it is very much vulnerable for forgery attack. Hence, both security and privacy constraints of messages must be satisfied. The original identity of vehicles can be traced with the help of only authorized entity. These original identities are not disclosed to other vehicles in the traffic. There are huge amount of research works done in the field of message authentication and verification. But, not a single approach is efficient enough for both authentication and message verification. Secure and privacy-preserving authentication technique is introduced in this research paper. It includes both regional authentication and roaming authentication simultaneously. This approach follows the basic concept of bilinear pairing. Secure communication along with anonymous authentication can be achieved with the help of the above-proposed technique.

A. Zhou, et.al, Yang developed a new security authentication technique that depends upon trust evaluation in VANETs [17]. As VANET is basically a wireless network and wireless networks are open in nature. With the openness of wireless network, the security challenges and vulnerabilities are increasing day by day. When a new node decides to access VANET network, it is required to be validated in order to enhance the security of VANET. The above-presented technique is basically depends upon trust evaluation. At first, when a particular vehicle needs to access data via the roadside base station, then that node is evaluated by trust evaluation method. According to the traditional security event record, the security degree of vehicle is identified. In case where certain group of nodes are used to construct a wireless network in order to communicate among themselves, then indirect trust evaluation method is implemented. After evaluation of the trust factor, all vehicle nodes are required to detect whether to accept the new vehicle node or not. Every individual node transmits a vector in order to demonstrate the standard trust value. Depending upon the correlation coefficient, they can easily discriminate malicious nodes from the normal nodes. All trust values assigned to that malicious node are discarded. After that, indirect trust values are evaluated through averaging all of the remaining trust values.

3. Proposed Model

In this section, we introduce the proposed security model for VANETs in which the V2V and V2R authentication is verified against malicious vehicles. The proposed model includes security solutions in three phases, namely V2V and vehicle-RSU security parameter initialization, V2V and vehicle-RSU setup and clone detection, V2V and V2R authentication verification for malicious message attacks. V2V and V2R communication ranges are shown in Figure 1.

3.1 Phase 1: V2V and Vehicle-RSU Security Parameter Initialization

In this phase, Trusted authority (System) initializes the security parameters for each vehicle and RSU in the VANET setup process. These parameters are used to provide strong data integrity signing and verification in the proposed authentication procedure.

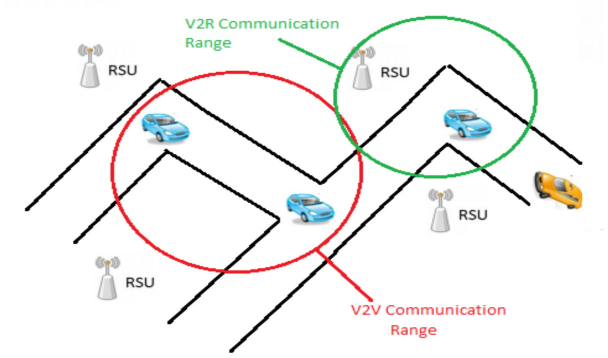

Fig. 1: V2V and V2R communication Range

Let $G_\alpha, G_\beta, G_\gamma$ are the cyclic abelian groups with multiplicative operation of prime order q. g_α, g_β are the generators of groups $G_\alpha \ and\ G_\beta$. Let $e \in G_\beta \times G_\alpha -> G_\gamma$ be the bilinear map defined from $G_\beta \times G_\alpha -> G_\gamma$ .Let ϕ be the isomorphism defined from $G_\beta \ to\ G_\alpha \quad such\ that\ \phi(g_\beta) = g_\alpha.$ Trusted authority TA (System) chooses a random number $m \in R_q^*$. Also, TA chooses three hash function [] with 256, 512 and 1024 bit generated values as $H_{256}(x), H_{512}(x), H_{1024}(x)$. Finally, T.A generates security parameters to each vehicle and RSU in the VANET as

$$\mathrm{VParams} = \{V - ID, \alpha, \beta, \gamma, G_\alpha, G_\beta, G_B, g_\alpha, g_\beta,$$

$$e, H_{256}(x), H_{512}(x), H_{1024}(x), \mathrm{Pub}_k^V, \mathrm{Enc}\}$$

$$\mathrm{RParams} = \{R - ID, \alpha, \beta, \gamma, G_\alpha, G_\beta, G_B, g_\alpha, g_\beta,$$

$$e, H_{256}(x), H_{512}(x), H_{1024}(x), \mathrm{Pub}_k^R, \mathrm{Enc}\}$$

Here V-ID is the vehicle identity and R-ID is the RSU identity.

$$\mathrm{Pub}_k^V = g_\alpha^{m1}; m1 \in R_q^*, \mathrm{Pub}_k^R = g_\alpha^{m2}; m2 \in R_q^*.$$

3.2 Phase 2: V2V and V2R Setup and Clone Detection

In this phase, each vehicle and RSU must communicate with the trusted authority T.A for security setup and clone identity verification process in a confidential channel. In figure 2, vehicle sends its identity, timestamp and nonce in an encrypted format to the T.A for vehicle security setup. Similarly, in figure 3 RSU sends its identity, timestamp and nonce in an encrypted format to the T.A for RSU security setup process.

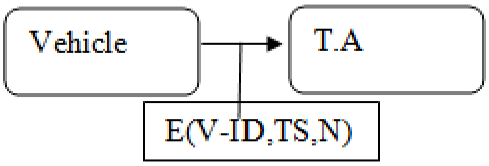

Fig. 2: Vehicle to T.A communication

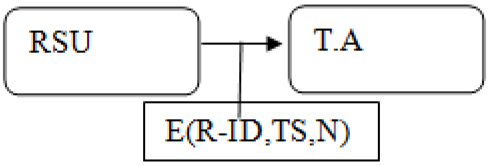

Fig. 3: RSU to T.A communication

T.A(System) chooses a random number r from the cyclic abelian group to perform R1 and R2.

DV=HexaTodecimal(V-ID);

DR=HexaTodecimal(R-ID);

Find the nearest relative prime θ to D such that θ >DV.

$$R_1 = H(V - ID \,||\, r)$$

$$R_2 = g_\beta^{\frac{1}{(m_1+R_1)\theta}} \qquad \text{for ehicle}$$

Find the nearest relative prime θ to DR such that θ >DR.

$$R_1 = H(R - ID \,||\, r)$$

$$R_2 = g_\beta^{\frac{1}{(m_2+R_1)\theta}} \qquad \text{for RTU}$$

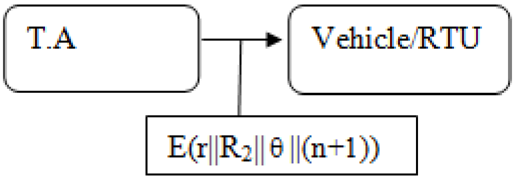

Fig. 4: T.A to Vehicle/RTU communication

Figure 4, describes the T.A communication to vehicle /RTU for security parameters initialization process. Each vehicle or RTU computes its signature and verifies at the T.A for clone node detection.

Signature Computation at Vehicle Side:

Vehicle decrypts the encrypted message E(r||R2|| θ ||(n+1))
From the T.A and computes its own signature for clone detection at the T.A.

$$e(R_2^\theta, \mathrm{Pub}_k^V, g_\alpha^{H(r||ID-V)}) = e(g_\beta^{\frac{\theta}{\theta(m_1+R_1)}}, g_\alpha^{m_1}.g_\alpha^{R_1})$$

$$= e(g_\beta^{\frac{1}{(m_1+R_1)}}, g_\alpha^{m_1+R_1})$$

$$= e(g_\beta, g_\alpha)^{\frac{1}{(m_1+R_1)}(m_1+R_1)}$$

$$= e(g_\beta, g_\alpha)^1$$

$$S_v = e(g_\beta, g_\alpha)$$

Vehicle sends its signature verification code S_v to the T.A for vehicle setup for authentication.

if($S_v \equiv e(g_\beta, g_\alpha)_{T.A}$)
then
Vehicle is not a clone node.
Else

Vehicle is a clone node with already existing signature S_v at time stamp TS.

Signature Computation at RTU Side:

RTU decrypts the encrypted message E(r||R2|| θ ||(n+1))
From the T.A and computes its own signature for clone detection at the T.A.

$$e(R_2^\theta, \mathrm{Pub}_k^R, g_\alpha^{H(r||ID-R)}) = e(g_\beta^{\frac{\theta}{\theta(m_2+R_1)}}, g_\alpha^{m_2}.g_\alpha^{R_1})$$

$$= e(g_\beta^{\frac{1}{(m_2+R_1)}}, g_\alpha^{m_2+R_1})$$

$$= e(g_\beta, g_\alpha)^{\frac{1}{(m_2+R_1)}(m_2+R_1)}$$

$$= e(g_\beta, g_\alpha)^1$$

$$S_R = e(g_\beta, g_\alpha)$$

RTU sends its signature verification code S_R to the T.A for vehicle setup for authentication.

if($S_R \equiv e(g_\beta, g_\alpha)_{T.A}$)
then
RTU is not a clone node.
Else

RTU is a clone node with already existing signature S_v at time stamp TS.

3.3 Phase 3: V2V and V2R Authentication Verification for Malicious Message Attack Detection

a) V2V authentication verification for malicious message attack detection

In this phase, each vehicle computes its authentication code to check the message integrity during the VANET communication process. Each vehicle use five fields such as Vehicle ID, Timestamp TS,Location L,Message M, R2 and Vehicle integrity.

Message authentication steps in the V2V communication is performed as follows:

Step 1: Vehicle chooses a random number $c_1 \in G_q^*$ to find the value $F = g_\beta^{c_1}$.

Step 2: Compute ρ_1, ρ_2, ρ_3 as

$$\rho_1 = g_\beta^{\frac{c_1}{\theta(m_1+R_1)}}$$

$$\rho_2 = Pub_k^{c_1} = g_\alpha^{m_1.c_1}$$

$$\rho_3 = g_\alpha^{c_1.R_1}$$

Step3: Select random numbers $c_2, c_3 \in G_q^*$ to find $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5.$

$$\delta_1 = \phi(F)^{c_2}$$

$$\delta_2 = g_\beta^{c_3}$$

$$\delta_3 = (Pub_k^V)^{c_3}$$

$$\delta_4 = H_{256}(M)^{c_2}$$

$$M = H_{512}(M)^{R_1}$$

Step 4: Perform the following integrity security operations as

$$\eta_1 = H_{1024}(F, \delta_1, \delta_2, \delta_3, \delta_4)$$

$$\eta_2 = c_2 + R_1.\eta_1$$

$$\eta_3 = c_3 + c_1.\eta_1$$

Step 5: Each vehicle initializes its vehicle integrity authentication code(VIA) for authentication checking at the other destination communication node.

$$VIA = \{ \rho_1, \rho_2, \rho_3, \eta_1, \eta_2, \eta_3, M, F\}$$

Step 6 : Finally, each vehicle's VIA is verified at the T.A before communicating to the other vehicle or RSU in two levels. In the first level, T.A decrypts the Vehicles VIA code to find the initial level of security verification as shown below.

b) Vehicle's VIA code verification level 1:

Verify : $e(\rho_1, \rho_2, \rho_3) = e(F, \phi(F))$

$$e(\rho_1, \rho_2, \rho_3) = e(R_2^{\theta c_1}, Pub_k^{c_1}, (g_\alpha^{R_1})^{c_1})$$

$$= e(R_2^{\theta c_1}, g_\alpha^{m_1 c_1}, (g_\alpha^{R_1})^{c_1})$$

$$= e(R_2^{\theta c_1}, g_\alpha^{m_1 c_1 + R_1 c_1})$$

$$= e(R_2^{\theta c_1}, g_\alpha^{(m_1+R_1)c_1})$$

$$= e(g_\beta^{\frac{c_1}{m_1+R_1}}, g_\alpha^{(m_1+R_1)c_1})$$

$$= e((g_\beta^{c_1})^{\frac{1}{m_1+R_1}}, (g_\alpha^{c_1})^{m_1+R_1})$$

$$= e((F)^{\frac{1}{m_1+R_1}}, (g_\alpha^{c_1})^{m_1+R_1})$$

$$= e((F)^{\frac{1}{m_1+R_1}}, \phi({g_\beta}^{c_1})^{m_1+R_1})$$

$$= e(F, \phi({g_\beta}^{c_1}))^{\frac{1}{m_1+R_1}.m_1+R_1}$$

$$= e(F, \phi({g_\beta}^{c_1}))$$

$$= e(F, \phi(F))$$

c) Vehicle's VIA code verification level 2:

After the verification of the level 1 security, each vehicle authentication code is verified at level 2 for malicious message integrity attacks. If the level 1 and level 2 are successfully verified then those nodes are treated as the normal legitimate vehicles and remaining nodes are treated as the malicious or suspicious vehicles.

Verifier 2: Conditions

$$\delta_1 = I_1 = \phi(F)^{\eta_2}.\rho_3^{-\eta_1}$$

$$\delta_2 = I_2 = g_\beta^{\eta_3}.F^{-(\eta_1+1)}.\phi(g_\alpha)^{c_1}$$

$$\delta_3 = I_3 = (Pub_k^V)^{\eta_3}.\rho_2^{-\eta_1}$$

$$\delta_4 = I_4 = H_{256}(M)^{\eta_2}.M^{-\eta_1}$$

=

Condition 1:

$$\delta_1 = I_1 = \phi(F)^{\eta_2}.\rho_3^{-\eta_1}$$

$$\delta_1 = \phi(F)^{\eta_2}.\rho_3^{-\eta_1}$$

$$= \phi(g_\beta^{c_1\eta_2}).g_\alpha^{-R_1c_1\eta_1}$$

$$= \phi(g_\beta)^{c_1\eta_2}.g_\alpha^{-R_1c_1\eta_1}$$

$$= {g_\alpha}^{c_1\eta_2}.g_\alpha^{-R_1c_1\eta_1}$$

$$= {g_\alpha}^{c_1\eta_2 - R_1c_1\eta_1}$$

$$= {g_\alpha}^{c_1(c_2+R_1\eta_1) - R_1c_1\eta_1}$$

$$= {g_\alpha}^{c_1c_2 + c_1R_1\eta_1 - R_1c_1\eta_1}$$

$$= {g_\alpha}^{c_1c_2}$$

$$= \phi(g_\beta)^{c_1c_2}$$

$$= \phi(g_\beta^{c_1})^{c_2}$$

$$= \phi(F)^{c_2}$$

Condition 2:

$$\delta_2 = I_2 = g_\beta^{\eta_3}.F^{-(\eta_1+1)}.\phi(g_\alpha)^{c_1}$$

$$\delta_2 = g_\beta^{\eta_3}.F^{-(\eta_1+1)}.\phi(g_\alpha)^{c_1}$$

$$\delta_2 = g_\beta^{c_3+c_1\eta_1}.F^{-(\eta_1+1)}.\phi(g_\alpha)^{c_1}$$

$$\delta_2 = g_\beta^{c_3+c_1\eta_1}.F^{-(\eta_1+1)}.g_\beta{}^{c_1}$$

$$\delta_2 = g_\beta^{c_3+c_1\eta_1}.(g_\beta^{c_1})^{-(\eta_1+1)}.g_\beta{}^{c_1}$$

$$\delta_2 = g_\beta^{c_3+c_1\eta_1}.g_\beta{}^{-c_1\eta_1-c_1}.g_\beta{}^{c_1}$$

$$\delta_2 = g_\beta^{c_3+c_1\eta_1}.g_\beta{}^{-c_1\eta_1-c_1+c_1}$$

$$\delta_2 = g_\beta^{c_3+c_1\eta_1}.g_\beta{}^{-c_1\eta_1}$$

$$\delta_2 = g_\beta^{c_3}$$

Condition 3:

$$\delta_3 = I_3 = (Pub_k^V)^{\eta_3}.\rho_2^{-\eta_1}$$

$$\delta_3 = (Pub_k^V)^{\eta_3}.\rho_2^{-\eta_1}$$

$$\delta_3 = (g_\alpha^{m_1})^{\eta_3}.\rho_2^{-\eta_1}$$

$$\delta_3 = (g_\alpha^{m_1})^{\eta_3}.Pub_k^{-c_1\eta_1}$$

$$\delta_3 = (g_\alpha^{m_1})^{(c_3+c_1\eta_1)}.Pub_k^{-c_1\eta_1}$$

$$\delta_3 = g_\alpha^{m_1c_3+m_1c_1\eta_1}.g_\alpha{}^{-m_1c_1\eta_1}$$

$$\delta_3 = g_\alpha^{m_1c_3+m_1c_1\eta_1-m_1c_1\eta_1}$$

$$\delta_3 = g_\alpha^{m_1c_3}$$

$$\delta_3 = (g_\alpha^{m_1})^{c_3}$$

$$\delta_3 = (Pub_k^V)^{c_3}$$

Condition 4:

$$\delta_4 = I_4 = H_{256}(M)^{\eta_2}.M^{-\eta_1}$$

$$\delta_4 = H_{256}(M)^{\eta_2}.M^{-\eta_1}$$

$$\delta_4 = H_{256}(M)^{c_2+R_1\eta_1}.M^{-\eta_1}$$

$$\delta_4 = H_{256}(M)^{c_2}H_{256}(M)^{R_1\eta_1}.M^{-\eta_1}$$

$$\delta_4 = H_{256}(M)^{c_2}(H_{256}(M)^{R_1})^{\eta_1}.M^{-\eta_1}$$

$$\delta_4 = H_{256}(M)^{c_2}(M)^{\eta_1}.M^{-\eta_1}$$

$$\delta_4 = H_{256}(M)^{c_2}$$

```
For each vehicle Vi in vehicles list
 For each neighbor vehicle Vj in neighbor list
   $If(\{V_i(I_1I_2I_3I_4), V_j(I_1I_2I_3I_4)\} \in true)$
 then
            Vi, Vj are trusted nodes
Else
            Either Vi,  or Vj   is malicious based on conditions.
Done
Done
```

Similarly, steps 1-6 are performed on V2R.

4. Experimental Results

Experimental results are designed and implemented using the java based VANET simulator and Real-time geographical map for VANET simulation. The basic properties of VANET simulator is given below in table 1:

Table 1: Simulation Parameters

Parameter	Description
Programming language	Java
Real-time Map	OpenStreetMap
Minimum number of Vehicles	100
Minimum number of Infrastructures	25
Communication data size	Variable
Minimum Memory required	4GB

5. Simulation Environment

Figure 5 describes the real-time traffic map for VANET simulation. This map is used to simulate the vehicles in the proposed model. Different paths and its outlines are shown in figure 6. During the data communication, each vehicle communicates with the other entities using the integrity verification method and the encryption method.

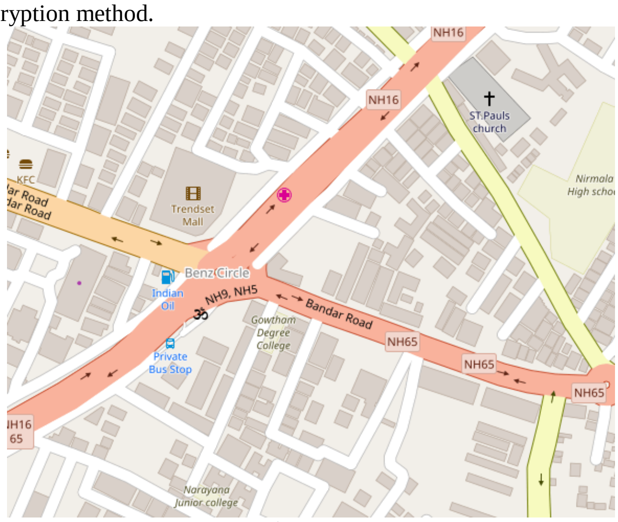

Fig. 5: Input OpenStreetMap for the proposed VANET realistic map

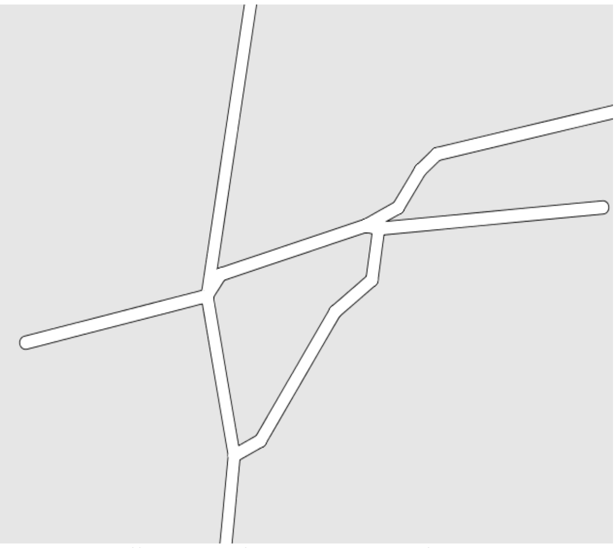

Fig. 5: Input traffic outline of the Realistic map of the OpenStreetMap in the proposed VANT simulation

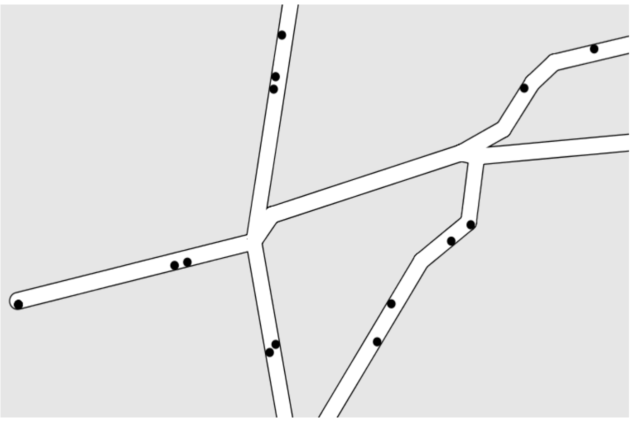

Fig. 6: Vehicle initialization in the VANET simulation.

Figure 6, describes the initialization of the vehicles in the VANET simulation model for data security. In this simulation mode, vehicles are initialized randomly in the VANET traffic path.

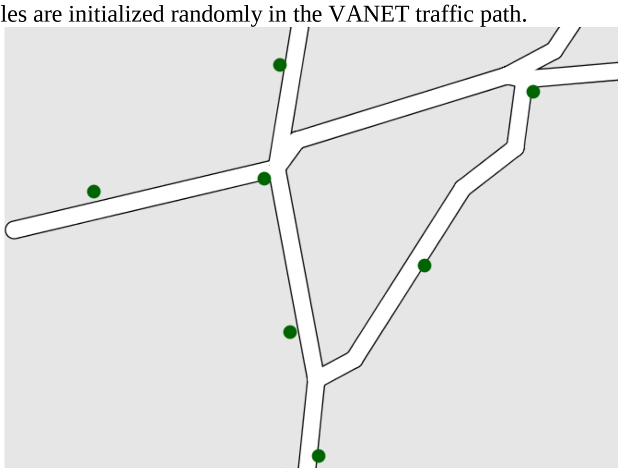

Fig. 7: RSU initialization of the proposed VANET simulation

Figure 7, describes the RSU initialization in the proposed VANET simulation. Here, RSU are placed randomly in different positions before the VANET communication.

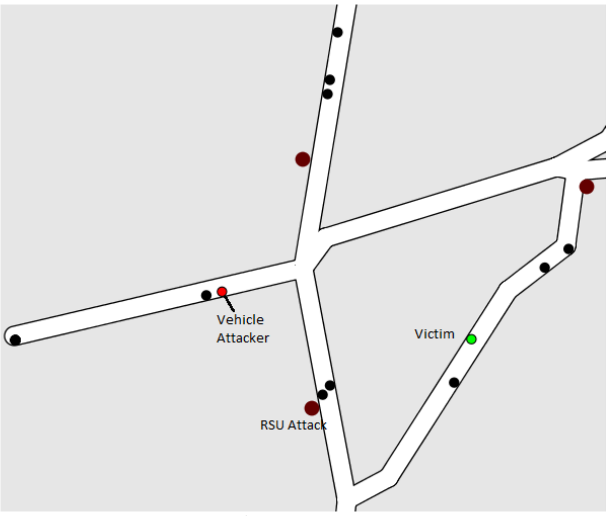

Fig. 8: Initialization of Vehicle attack and the RSU attacks

Figure 8 describes the initialization of vehicle attacks and RSU Sybil attacks in the VANET simulation.

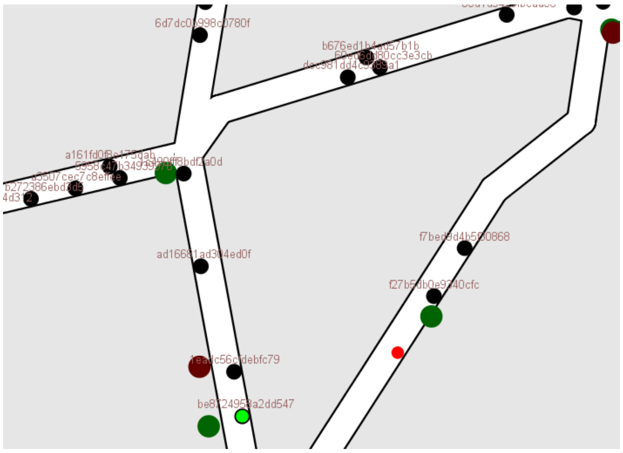

Fig. 9: Finding node cloning and malicious attacks using the proposed model.

Figure 9 describes the node clone detection and malicious node detection process using the proposed model in VANET simulation. Figure 10, shows the malicious Sybil attack (red vehicle) on the green vehicle node. Figure 11, describes the clone node detection simulation result. Figure 12 illustrates the malicious and clone node results in the proposed VANET simulation.

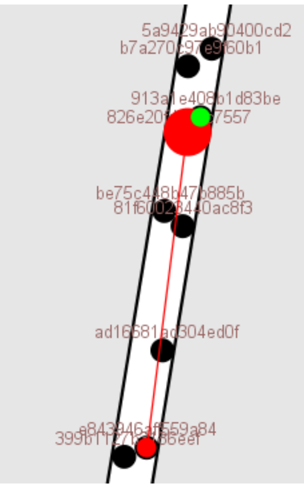

Fig. 10: Malicious attack vehicle detection

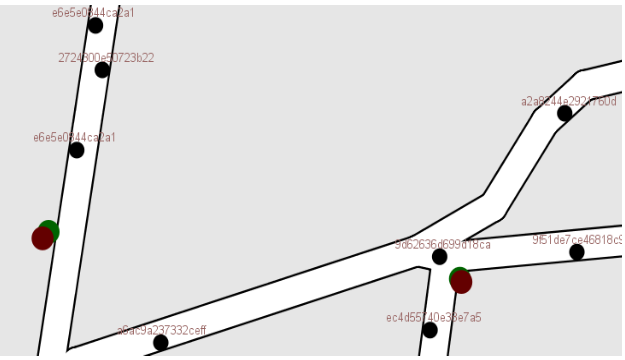

Fig. 11: Clone node detection

```
Malicious and clone Node Detection
Vehicle Flood Alert Message Source X,Y 63014 115378  Destination X,Y
63192 112172
Nearest RSU ID  4 With Vehicle Current Location 63014 115378 RSU
location ==> X: 63192 Y: 112172
Vehicle Flood Alert Message Source X,Y 63014 115378  Destination X,Y
63192 112172
Vehicle Flood Alert Message Source X,Y 64913 111177  Destination X,Y
63192 112172
Nearest Attack RSU ID  1 With Vehicle Current Location 65971 109527
RSU location ==> X: 63192 Y: 112172
Nearest RSU ID  6 With Vehicle Current Location 65971 109527 RSU
location ==> X: 63192 Y: 112172
Vehicle Malicious Alert Message Source X,Y 65971 109527  Destination
X,Y 63192 112172.
Vehicle Clone Alert Message Source X,Y 70674 100915  Destination X,Y
70908 101113 with ID=e6e50844ca2a1
```

Fig. 12: Malicious and Clone vehicle detection results

Table 2: Comparative analysis of proposed model to the existing models in terms of average clone node detection rate

Number of vehicles=500

#Clone nodes	LESPP (%)	Handoff Auth(%))	LVAP (%)	MLAS (%)	Proposed model(%)
10	83.64	79	87	93	98.19
20	81	77.46	89.5	92.53	97.34
30	78.34	81.54	85.65	94.75	98.93
40	81	80.54	91.45	93.54	96.86
50	77.54	79.64	92.54	91.54	97.94

Table 2, illustrates the performance of the present model to the existing models in terms of average clone node detection. From the table, proposed model has high clone node detection rate in V2V clone node detection during VANET communication.

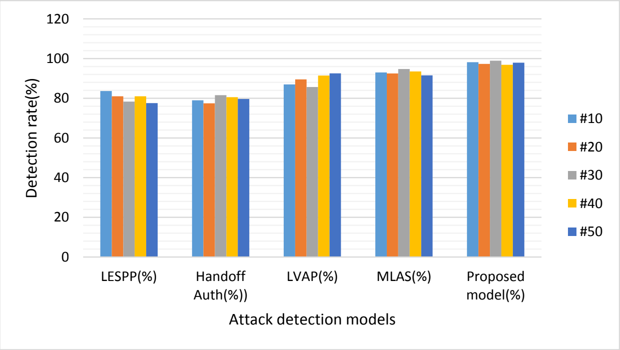

Fig. 13: Comparative analysis of proposed model to the existing models in terms of average clone node detection rate

Figure 13, illustrates the performance of the present model to the existing models in terms of average clone node detection. From the table, proposed model has high clone node detection rate in V2V clone node detection during VANET communication.

Table 3: Comparative analysis of proposed model to the existing models in terms of average malicious node detection rate, packet delivery ratio, and detection time

Model	**#Sybil Attacks(%)**	**Packet Delivery Ratio**	**Avg Detection Time(ms)**	**Avg Authentication Time(ms)**
LESPP	78.97	0.76	4975	5634
Handoff Auth	81.53	0.824	5294	6353
LVAP	90.88	0.9153	4983	5464
MLAS	94.35	0.9574	4793	5253
Proposed	98.94	0.989	4464	4985

Table 3 describes the malicious vehicle detection rate along with the packet delivery ratio, average authentication time, and detection time. From the table it is clearly analyzed that the proposed model has high computational performance than the existing models in VANET security.

6. Conclusion

Generally, vehicles broadcast messages to its neighboring vehicles and to the roadside infrastructures in VANET communication. These broadcasted messages are very much vulnerable for attacks. Thus, security and privacy are considered as prime factors in the process of communication. In order to provide security to these broadcasted messages, various advanced authentication and verification algorithms are proposed in the literature on limited data size and static VANETs. Also, most of the traditional data security and vehicle attack detection algorithms are based on static configurations with fixed attack vehicle's time and location in VANET. In this paper, we have designed and implemented a new V2V and V2I based data security and vehicle authentication protocol in dynamic VANETs. In the proposed model, V2V and V2I type of attacks such as cloning and Sybil attacks are detection with high computational accuracy along with the authentication process. Apart from this, the total transmission overhead is reduced in the proposed model. Integration of signature and message is the prime reason behind the reduction of transmission overhead. This technique is based on an identity-based signature approach along with malicious attack detection scheme. It permits the receiver to check the signature prior to execution of message integrity verification. Experimental results proved that the proposed model has high computational efficiency in terms of detection rate, detection time and packet delivery ratio.

References

[1] P. J. Fernandez Ruiz, F. B. Hidalgo, C. A. Nieto Guerra and A. F. Gomez Skarmeta, "Mobility and security in a real VANET deployed in a heterogeneous networks". "Security Comm. Networks (2012)".

[2] M. Bayat, M. Barmshoory, M. Rahimi and Md. Reza Aref, "A secure authentication scheme for VANETs with batch verification".

[3] T. W. Chim, S. M. Yiu, L. C. K. Hui, V. O. K. Li, "MLAS: Multiple level authentication scheme for VANETs", "Ad Hoc Networks 10 (2012), pp.1445–1456.

[4] A.Das and D. Roychoudhury, "Authentication schemes for VANETs: a survey"," Int. J. Vehicle Information and Communication Systems, Vol. 3, No. 1", pp. 1-27, 2013

[5] M. Han, S. J. Lee and W. Bae, "A Secure and Efficient V2V Authentication Method in Heavy Traffic Environment".

[6] H. Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur and A. Iyer, "Flooding-Resilient Broadcast Authentication for VANETs".

[7] Y. Kim and J. Lee, "A secure analysis of vehicular authentication security scheme of RSUs in VANET", J Comput Virol Hack Tech.

[8] Y. Liu, Z. He, S. Zhao and L. Wang, "An efficient anonymous authentication protocol using batch operations for VANETs", Multimedia Tools Appl .

[9] Y. Liu, W. Guo, Q. Zhong and G. Yao, "LVAP: Lightweight V2I authentication protocol using group communication in VANETs..

[10] S. Mitra and A. Mondal, "Identification, Authentication and Tracking Algorithm for Vehicles using VIN in Distributed VANET", ICACCI'12, August 3-5, 2012, Chennai, T Nadu, India, pp. 279-286, 2012.

[11] T. Oulhaci, M. Omar, F. Harzine and I. Harfi, "Secure and distributed certification system architecture for safety message authentication in VANET", Telecommunication System.

[12] Y. Sun, Z. Feng, Q. Hu and J. Su, "An efficient distributed key management scheme for group-signature based anonymous authentication in VANET", Security Comm. Networks 2012; 5: pp.79–86

[13] M. Wang, D. Liu, L. Zhu, Y. Xu and F. Wang, "LESPP: lightweight and efficient strong privacy-preserving authentication scheme for secure VANET communication".

[14] Y. Xie, L. Wu, J. Shen and A. Alelaiwi, "EIAS-CP: new efficient identity-based authentication scheme with conditional privacy-preserving for VANETs".

[15] Z. Zhou, H. Zhang and Z. Sun, "An Improved Privacy-Aware Handoff Authentication Protocol for VANETs".

[16] H. Zhu, T. Liu, G. Wei and H. Li, "PPAS: privacy protection authentication scheme for VANET", "Cluster Computing".

[17] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei and F. Yang, "A security authentication method based on trust evaluation in VANETs", "EURASIP Journal onWireless Communications and Networking", pp. 1-8.