PRIVACY-PRESERVING DOS ATTACKS AGAINST PSEUDONYMOUS AUTHENTICATION THROUGH CROSS DOMAIN AUTHENTICATION IN 5G-VANET

Dr.T.Rajagopalan[1], S.Prince chelladurai[2]

Department of Mathematics, University College of EngineeringAriyalur, Tamil Nadu, India, rajgopalant@gmail.com.

Department of Computer Science and Engineering, University College of Engineering Villupuram, Tamil Nadu, India,86.princee@gmail.com

ABSTRACT: The up and coming Fifth Generation (5G) systems can give ultra-solid ultra-low inactivity vehicle-to-everything for vehicular specially appointed systems (VANET) to advance street security, traffic the board, data dispersal, and programmed driving for drivers and travelers. Be that as it may, 5G-VANET additionally draws in colossal security and protection concerns. Albeit a few pseudonymous confirmation plans have been proposed for VANET, the costly expense for their underlying verification may cause genuine refusal of administration (DoS) assaults, which further more empowers to do extraordinary mischief to genuine space by means of VANET. Inspired by this, a riddle based co-confirmation (PML-CIDS) scheme is proposed here. In the PCA plot, the Hash astound is cautiously intended to moderate DoS assaults against the pseudonymous validation process, which is encouraged through community verification**.**

INDEX TERMS-Denial of service, pseudonymous authentication, VANET, PML-CIDS, 5G.

1. INTRODUCTION

The fifth age (5G) systems are intended to give great help to ultra-dependable ultra-low dormancy (URLLC) administrations [1], for example, vehicle-to-everything (V2X) of Vehicular Ad Hoc Networks (VANET) in Intelligence Transportation System [2]. In recent years, 5GVANETrelatedresearch and norms improvement have drawn boundless consideration both in industry and the scholarly world, e.g., the 5G Automotive Association (5GAA) thinks about that Cellular V2X (C-V2X) created in the Third Generation Partnership Project (3GPP) will be an appropriate innovation to give URLLC to 5G-VANET [3] and Qualcomm Technologies reports that its 5G-VANET chipset, which underpins C-V2X, will be accessible in 2018 [4]. Also, with the fast improvement of 5G-VANET, the related applications, for example, programmed

drivingwillalsocometoreallifeimmediately.However, itisnecessary to take note of that 5G-VANET is the basic point among the internet and genuine space, i.e., assaults against the internet can make incredible mischief genuine space by means of VANET, e.g., protection spills, traffic loss of motion and significantly progressively genuine Traffic mishaps [5] – [7]. Accordingly, it is of fundamental significance to relieve any assault in 5G-VANET

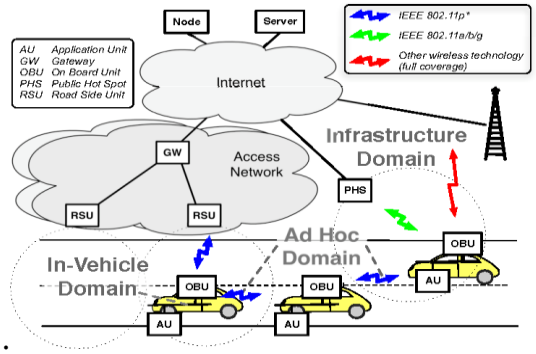

Fig 1: VANET Architecture

In VANET, Dedicated Short Range Communications (DSRC) is a great convention intended for interchanges between vehicles. As indicated by the DSRC, vehicles occasionally report constant traffic data including area, velocity, and acceleration of vehicles, critical traffic events, and so forth. By sharing such critical information, drivers or autopilot programs can have a good understanding of the surrounding driving condition and make opportune move to manage sudden abnormal situation such as traffic accidents. However, the appealing applications turned out to be twofold edged [8], which conceal the security and protection dangers. For instance, an attacker can easily forge fake traffic information to induce traffic accidents or track target vehicles by collecting location data of the vehicles in VANET. To guarantee both security and protection in VANET, pseudonymous verification plans have been proposed over the previous year's [9] – [13].

The fundamental structure of pseudonymous confirmation plans is as per the following: each real vehicle applies to a confided in outsider for countless computerized certificates called pseudonymous certificates, each timespan utilizing a pseudonymous certificate to issue traffic data. This plan empowers to keep unlawful assailant from posting false messages and seek after illicit vehicles through the confided in outsider while ensuring the area security of authentic

vehicles by an intermittent substitution of the pseudonymous certificates (i.e. the personality of the element can't be related with the area). It very well may be said that the pseudonymous confirmation plans is the foundation of the protection and security of VANET.

Be that as it may, in the pseudonymous verification conspires, the pseudonymous certificate is for the most part one-time and regularly replaced, which causes a large to be issued .In order to reduce the cost of digital certificates, the structure of vehicle advanced certificates is commonly progressively mind boggling, bringing about the greater expense of the underlying authentication in pseudonymous authentication schemes. The aggressors can manufacture an extensive number of phony certificates for the underlying confirmation to dispatch DoS assaults. In the event that the assailants utilize all the transmission data transfer capacity to send counterfeit certificates, the processing assets of the on-board units (OBUs) will be totally involved by the verification of enormous phony certificates, prompting disappointment of ordinary correspondences. In the low inertness and high data transfer capacity 5G-VANET, this sort of DoS assaults can be propelled result in lamentable consequences.

Thus,thispaperaimsathrowtorefrainattackersfromabusingthehighcostfortheinitialauthentic ationfor DoS assaults by producing a substantial number of false pseudonymous characters. It is worth to take note of that this situation is far not the same as the current DoS alleviation plans for VANET which center around securing correspondence transfer speed [14] and accept that every element has a one of a kind identity[15]– [20].

2. OVERVIEW OF VANETs

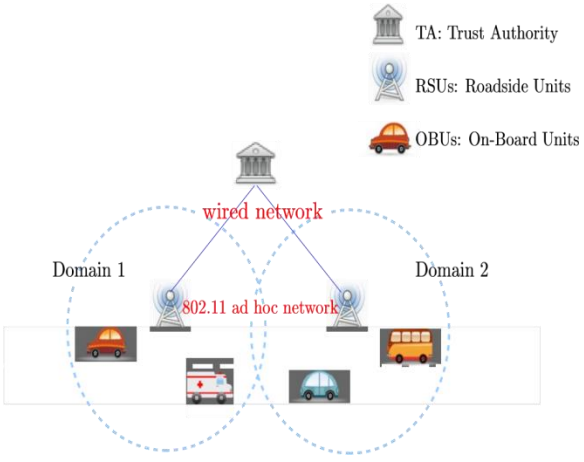

Fig 2. System Model

1) System Model: In a typical VANET, a trusted authority (TA) as the Transportation Regulation Center (TRC) is deployed in the backend. Each vehicle is assumed to have an on-board unit (OBU) authenticated and issued by TA and there are roadside units (RSUs) deployed at the roadsides by TA. The RSUs are assumed to connect with TA by dedicated wired links with high bandwidth, low delay, and low bit error rates. The communication between OBUs is using the Dedicated Short Range Communications (DSRC) protocol identified as IEEE 802.11p, as shown in Fig. 2. The basic application of VANET is to allow arbitrary vehicles to broadcast safety messages (e.g. road conditions, traffic accident information) to other nearby vehicles and RSUs may inform the traffic control center to adjust traffic lights for avoiding possible traffic congestion. The details of every role involved in the whole model are described as follows.

- *Trusted Authority* (*TA*): TA is fully trusted by all entities in the communication system and in charge of the registration of immobile RSUs at the road side and mobile OBUs equipped on the vehicles. Therefore, TA manages the VANET to hold all secrets and takes responsibilities for solving any misbehavior and dispute.
- *Roadside Unit* (*RSUs*): RSUs are deployed by TA, which hold storage and computation units. Without loss of generality, RSUs are densely distributed on the roadside. In our protocol, RSUs are used to issue safety message signatures to vehicles.
- *On-Board Unit* (*OBUs*): OBUs are equipped on the running vehicles, which mainly communicate with other vehicles via DSRC protocol for sharing traffic information to improve the whole safety of driving conditions.

Essential Attacks: VANET is noteworthy since it handles the traffic the board and roadside security. Sadly, VANET additionally accompanies a few difficulties, particularly in the parts of security and protection. We will depict the security dangers in vehicular systems. There are a few conceivable assaults on VANETs:

• Bogus Information Attack: An aggressor may send wrong data in the system to influence the conduct of different drivers and even reason intentional auto collisions. For instance, an aggressor may mimic a rescue vehicle to ask for different vehicles to give an approach to it or demand close-by RSUs to change traffic lights to green freely.

•Message Integrity Attack: An assailant may alter the substance of the messages sent by others to meet explicit purposes.

•ID Disclosure Attack: An assailant may foresee the moving way and follow the physical position of some devoted vehicle by gathering adequate routine traffic messages.

•Impersonation Attack: An assailant may profess to be another vehicle by utilizing counterfeit personalities and endeavor to maintain a strategic distance from obligation.

2) Security Requirements: In request to keep a correspondence organize stable, security issues must be all around tended to. A safe framework for VANET ought to fulfill the accompanying necessities:

•Authentication: A vehicle must most likely demonstrate its character legitimateness to another vehicle (for example messages are created and sent by genuine senders). At the end of the day, a vehicle can confirm the source legitimacy for any gotten message.

•Message Integrity: Vehicles ought to most likely recognize whether messages have been debased or not amid the transmission. Something else, an aggressor can supplant the security messages from any vehicle.

•Non-disavowal: Any vehicle can't deny reality that a message is produced and circulated without anyone else. It is important for mishap examination where the pernicious clients should pay for their mischievous activities.

•Conditional Anonymity: The personalities of vehicles ought to be avoided ordinary message collectors with the exception of TA to ensure the senders' private data.

•Safety Message Unsinkability: Deciding whether two diverse substantial messages are sent by the indistinguishable sender or not is infeasible for anybody aside from TA.

•Safety Message unforgedability: None can create a genuine wellbeing message without a RSU.

•Traceability: Due to the obscurity control, TA will install a vehicle's genuine personality into a nonexclusive wellbeing message when the vehicle asks for a security message signature from a RSU. This property ensures that the installed data can't be supplanted with some other string. In addition, nobody can uncover the genuine personality from any wellbeing message aside from TA.

•Privacy Preservation: Considering validation, namelessness, and unlink ability, client protection can be characterized as the three dimensions

3. RELATED WORKS AND CONTRIBUTIONS

A. Pseudonymous authentication in Vanet

The pseudonymous authentication for secure vehicular communication has attracted extensive attentions[9]–[13].In[9], Rayland Hubaux first proposed that each vehicle in VANET keeps a large number of pseudonymous certificates in a long time and randomly selects one pseudonymous certificate for each time signing the message. However, once a vehicle became illegitimate or revoked, all its pseudonymous certificates, more than 40,000 certificatesin[9], need to bead to a Certificate Revocation List (CRL). The CRL may increase so quickly that it cannot be noticed to all entities in VANET on time. To decrease the CRL size, the Efficient Conditional Privacy Preservation (ECPP) protocol was first developed by Lu et al. in [10]. According to ECPP, the Roadside Units (RSUs) can help each vehicle to update fewer shorttime pseudonymous certificates in time.

Furthermore, after Wasefal's effort RSUs-aided distribute certificate service was developed to a hierarchical authority architecture and an efficient Distributed Certificate Service (DCS) scheme was proposed to support batch signature verification. Furthermore, Sunetal. [12] Proposed the proxy re-signature cryptography based Pseudonymous Authentication Scheme (PASS) to decrease certificate updating cost on road. PASS supports RSUs-aided distributed certificate service while the overhead of updating certificates will not be affected by the amount of updated certificates. Moreover, utilizing the one-way hash chains technology in PASS, the size of CRL just increases linearly with the amount of revoked vehicles. In order to achieve efficient and lightweight pseudonyms, Rajput et al.

Proposed a hybrid approach combining the advantages of the pseudonym-based approaches and the group signature-based approaches, which can avoid to manage the CRL. Although the above introduced schemes have addressed almost all well-known security and performance issues in routine application, the structure of pseudonymous certificates becomes complex, and the first time verification cost increases as well, e.g., increasing from 1.2msec [9] to more than14.7 msec .As introduced in Section I ,the pseudonymous authentication schemes may be out of work when an adversary launches DoS attack by broadcasting huge numbers of forged pseudonymous identities.

B.Anti-dos attack methods in vanet

Comparatively speaking, few works have been proposed against DoS in VANET. Hasbullah et al. [14] surveyed the possible DoS attacks in VANET and proposed serious solution against bandwidth DoS attacks, including Channel Switching, Technology Switching, Frequency Hopping Spread Spectrum (FHSS), etc.. To mitigate the DoS attacks against the message signature, He and Zhu [15] utilized the pre-authentication scheme before verifying signature, which combines the advantages of the one-way hash chain and the group rekeying method. Verma et al. [16] designed a Bloom Filter table of IP address to filter DoS traffic in VANET. To mitigate outside attackers, Pooja et al. [17] used Hash based Message AuthenticationCode (HMAC) to authenticate the communicating vehicles. Mejri et al. [18] studied the use of game theory against DoS attacks in VANET. However, all these works [15]–[17] are not suitable to defend the DoS attack against initial process of pseudonymous identity authentication, because the mitigation technologies (i.e., one-way hash chain [15], IP address [16], HMAC signatures links [17] and game theory models [18]) by default suppose the messages belongs to the same entity while the identity of the entity cannot be associated with the messages in the pseudonymous authentication schemes.Considering the DoS attack against RSUs caused by the signature verification overhead, Sun et al. [22] proposed a privacy preserving mutual authentication resisting DoS attacks by cryptographic puzzle.Because their scheme is an ID-based signature scheme, they didn't analyze the possible DoS attack against OBUs caused by the initial certificate verification overhead. Different from existing works, we focus on the DoS attack against pseudonymous authentication schemes in 5G-VANET. We mainly address the following issues: 1) The designed cryptograph puzzle attaching to the first time certificate verification request to prevent attackers from forging a large amount of fake pseudonymous certificates in 5G-VANET; 2) The mutual trust clusterco-authentication to reverse the imbalance of computational resources between legitimate vehicles and attackers and to speedup certificates authentication.

C.cooperative verification in vanet

In recent years, the idea of cooperation among vehicles has been proposed in VANET [23]. Early, COMET (cooperative message-authentication scheme) [24] proposed by Zhang et al. is designed to mitigate the message signature verification overhead of each vehicle by collaborative working. In this scheme, each legitimate vehicle will initiatively afford a certain

amount of message signature verification based on their computing power. Because of the trust relationship between legitimate vehicles, legitimate vehicles need not to repeatedly verify the message verified by one legitimate vehicle. Considering the possible selfish behavior, Lin and Li in [25] achieve efficient cooperative message authentication by adopting the evidence token which reflects the personal contribution in cooperative authentication. In summary, several methods have been proposed to reduce the overhead of message signature verification. However, compared to the overhead of message signature verification, the overhead of the first time pseudonymous certificate verification is heavier, which is more desired for cooperative verification.

4. THE PROPOSED STRONG PRIVACY PRESERVING COMMUNICATION PROTOCOL

A.Overview of the proposed system

A Puzzle-based Co-Authentication scheme in 5G-VANET. Basically, during the process of pseudonymous identity authentication, vehicles try to construct trust clusters among legitimate vehicles, and then co-authenticate by trust clusters to accelerate the identity authentication process. Specially, our contributions are threefold:

- Firstly, a computational puzzle is well-designed with the real-time information such as location, the expected receiver, and so on. In this way, puzzles cannot be precomputed, which allows DoS attacks against pseudonymous authentication to be mitigated.
- Secondly, based on the trust transitivity relations between vehicles, the connected components theory is used to construct the trust clusters, which can efficiently speed up the formation of trust clusters.
- Thirdly, the trust clusters co-authentication scheme is proposed. The vehicles inside a same trust cluster work together to verify pseudonymous certificates and recommend the cluster header to other clusters.

In this venture we alter and expand a protection safeguarding AI based synergistic IDS **(PML-CIDS)** for VANETs. The proposed calculation utilizes the exchanging bearing strategy for multipliers to a class of exact hazard minimization issues to recognize the interruptions in the

VANETs. We utilize the differential security to catch the protection documentation of the PML-CIDS and propose a technique for double factor annoyance to give dynamic differential security.

B.System Model Description

A general VANET comprises of on-board units (OBU), application units (AU), and roadside units (RSU). The correspondence between OBUs (vehicle-to-vehicle), or between an OBU and a RSU (vehicle-to-framework) depends on remote access in-vehicle condition (WAVE). The RSUs can likewise interface with different foundations, for example, different RSUs and traffic the board focus, and the interchanges between them (framework to-foundation) are through different remote innovation. Each vehicle is outfitted with an OBU and one or different AU. It likewise has a lot of sensors to gather data and utilize the OBU to trade data with different OBUs or RSUs.

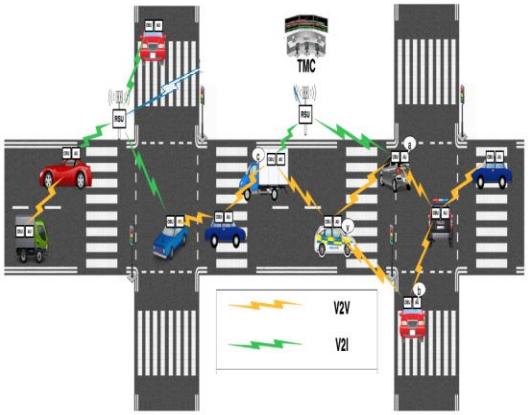

Fig 3: System Architecture

C.Proposed Methodology and Techniques

In this project the proposed system should address following challenges when detecting DDoS attacks in a cross-domain.

- The first challenge is to conduct cross-domain DDoS attack detection in VANET without revealing privacy of each network domain.
- The second challenge is to ensure efficient and accurate DDoS attack detection while preserving privacy.

We utilize bundle encryption to ensure the security of each system area. With a watchful structure, the figure content created by annoyance encryption can be straightforwardly determined in servers without the need to including complex secure calculation conventions. Regarding the second test, we apply the k Nearest Neighbors **(kNN)** calculation as a traffic classifier in light of the fact that kNN isn't touchy to anomalies and clamors in datasets, and its viability has been exhibited in numerous ongoing examinations.

All well-known security and performance issues in routine applicationProposed scheme can be easily combined with mutual pseudonymous authentication schemes to enhance the capacity of resisting DoS attacks and improving the efficiency of certificates verification.kNN will be a capacity for mitigating DoS attacks and decreasing the overhead of pseudonymous authentication.

D.Proposed Modules

- Implementation of Wireless Network
- Implementation of VANET scheme
- PCA Scheme deployment
- Implementation of Intrusion Detection Scheme
- Performance analysis

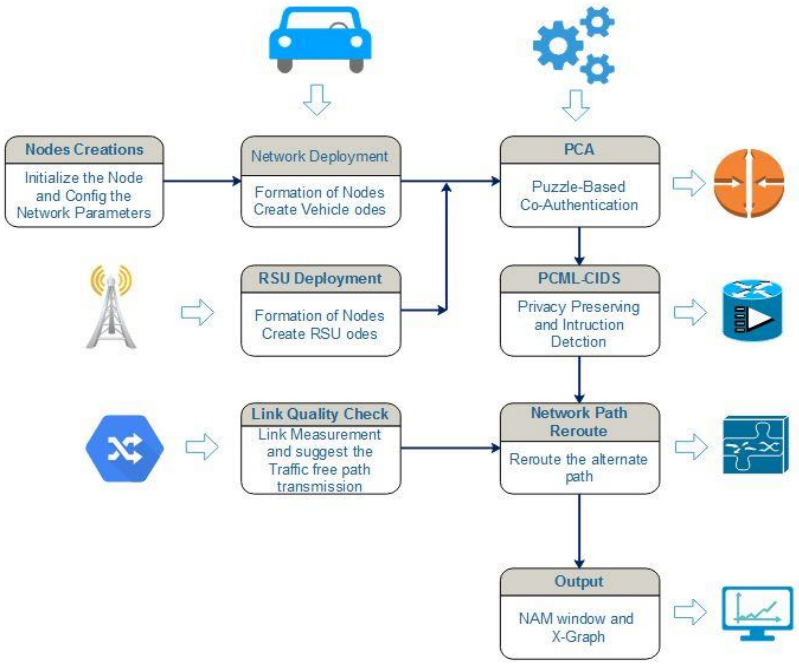

Fig 4: System Architecture

Implementation Of Wireless Network

In this module, a wireless network is created. All the nodes are configured and randomly deployed in the network area. Since our network is a VANET, nodes are assigned with initial energy, mobility and random way point of direction.The wireless networking model can be created using Tool Command Language (TCL) script with fixed number of nodes. The sample code discussed below models the wireless network with 2 nodes. Nodes are configured with the components of channel, networking interface, radio propagation model, Medium Access Control (MAC) protocol, adhoc routing protocol, interface queue, link layer, topography object, and antenna type. The wireless network with 2 nodes can be viewed in the Network Animator (NAM) window

Implementation Of Vanet Scheme

The success of V2X applications relies on the network connectivity, when there is a high vehicular density to sustain multi-hop communications or there exist fixed infrastructures such as RSUs. The aim of our work is to find some suitable relays which can forward the messages to the destination vehicle with a higher probability

PCA Scheme Deployment

Co-authentication actions will help to establish the mutual trust relationship between OBU1 and OBU5, and furthermore speed up the integration of the two mutual trust clusters, Meanwhile unaffected by the stronger computational power of attackers. Conclusively, in PCA scheme, the co-authentication based on the mutual trust cluster can greatly speed up the mutual authentication between legitimate vehicles in 5G-VANET to ensure rapid response to the routine traffic related messages.

Table 1

Element	Description
OBU_i	the vehicle i
$Cert_i$	the certificate of OBU_i
$Legal\_set$	the set of vehicles with legitimate certificates
$Fake\_set$	the set of vehicles with fake certificates
$Unverified\_set$	the set of vehicles with unverified certificates
$value_i$	the cumulative value of $Cert_i$ that $Cert_i \in Legal\_set \cup Unverified\_set$
$Value\_set$	the set of $value$
$Trust\_set$	the set of vehicles with trusted certificates

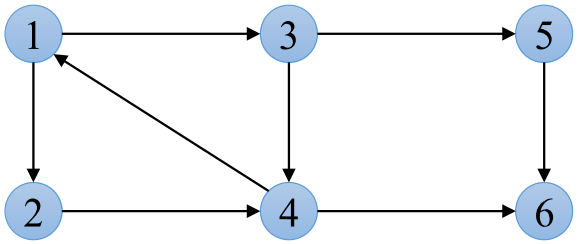

Fig 5:**Example of Directed graph.**

The utilization of emphatically associated parts will be helpful for development of the shared trust bunch. As appeared Table 2, in PCA conspire, the vehicle OBUi keeps up the arrangement of real declarations Legal_set = {hvLi}, the arrangement of phony testaments Fake_set = {hvFi}, the arrangement of unconfirmed endorsements unverified_set = {hvUi} and the arrangement of combined estimations of the genuine and the unsubstantiated authentications Value_set = {hvalueii}. Besides, every vehicle keeps up the trust relationship see G = (V,E), where G is a

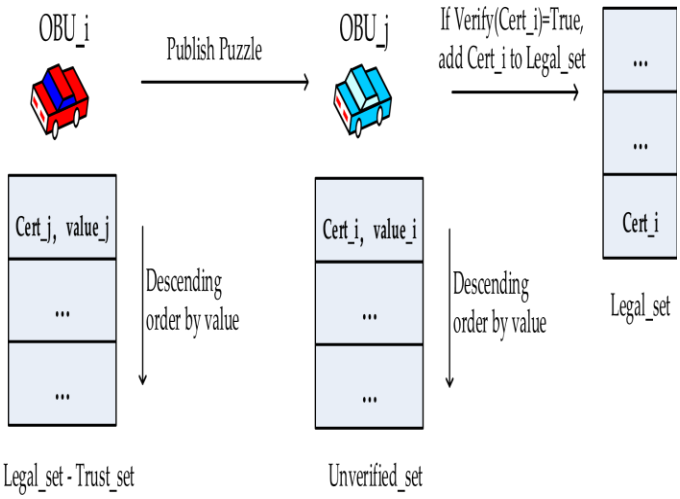

Fig 6: The process of verification

Coordinated diagram, V is the arrangement of every genuine vehicle and E is the arrangement of the trust connections. For the vehicle OBUi, Gi is its trust relationship view and V is the arrangement of the vehicles who are contained in Legal_set. On the off chance that the edge ei,j ∈ E, it implies OBUi have confirmed Certj is a real declaration, that is, OBUi trusts OBUj.

Algorithm 1 the Mutual Trust Cluster Solution Algorithm

Require: E: edge set of graph G; v_i: graph node of car i;

Ensure: *Trust_set*: the mutual trust cluster

1: $Trustset=\{VI\}$

2: $E_t = E$

3: $Trust\_set^* = 0$

4: **while** $Trust\_set$ 6= $Trust\_set^*$ **do**

5: **if** $Trust_set^*$6= 0 **then**

6: $Trust\_set^* = Trust\_set$

7: **end if**

8: $Trust\_set = Trust\_set^*$

9: **for** each $e_{k,j} \in E_t$ **do**

10: **if** $OBU_j \in Trust\_set^*$ **then**

11: $E_t = E_t - \{e_{k,j}\}$

12: $Trust\ set^* = Trustset^* \cup \{v_k\}$

13: **end if**

14: **end for**

15: **end while**

16: **return** *Trustset*

Compared with the time complexity $O(V + E)$ of these classical algorithm, the time complexity of our algorithm is $O(E)$, which can better accelerate the formation of the mutual trust. conclusion, the mutual trust cluster actually is the mutual trust relationship among timate vehicles. Once an unknown certificate have been verified by one vehicle of the mutual trust cluster, the other vehicles of the mutual trust cluster need not to verify this certificate again, which can significantly save the average computational resources of legitimate vehicles. Besides, in our

PCA scheme, when the mutual trust cluster is regarded as the object to be verified, the computational resources of all the members in the mutual trust cluster can be integrated to increase the puzzle value corresponding to the certificate to be verified, which is the other hand

of solution against the attacker's stronger computational power. These features will be described in the following subsection

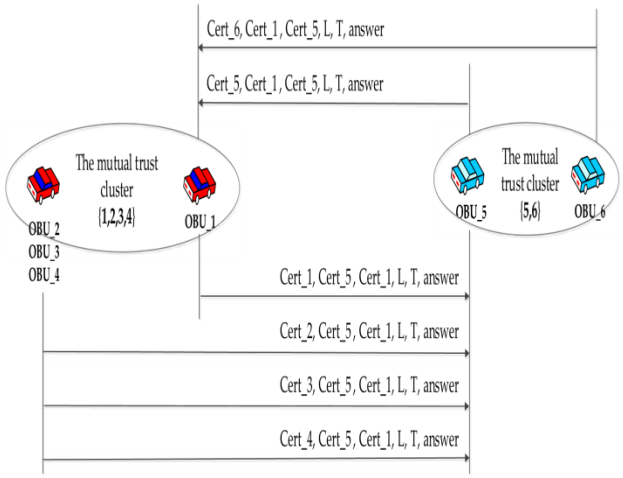

Fig 7:The process of co-authentication

5. IMPLEMENTATION OF INTRUSION DETECTION SCHEME

In the experiments, the task is to classifier whether a network activity is an attack or normal using logistic regression. There are four types of denial of service attacks presented, namely, jamming, unauthorized access to local system tampering privileges, and unauthorized access. Reconsidering the malicious road side attacker that is sending wrong emergency braking warnings, as described in the introduction, a defensive detection process could be as follows. A first event of a suspicious action within the active safety system would be discovered, if an emergency braking event is received from a previously unknown node.

One would normally expect such an event to come from a previously known node. A second event might come from another vehicle that previously passed this area and also received the same warning message. After passing the respective area, this car's intrusion detection system recognizes, that for itself, there was no emergency braking event and transfers this analysis to follow up cars. Combining these two events results in a strong evidence that the received warning message must be a fake warning.

Thus, the intrusion detection system tells the active safety system to ignore the warning and communicates the detection results to other nodes, especially follow up nodes. In order to realize such an effective intrusion detection system in VANETs, we advocate the use of a modular cross layer intrusion detection system. On every node, different modules are in charge

of collecting audit data on different layers. A local decision module receives continuously audit data summaries from the other modules and analyses them with the aid of additional information, available from other non-network devices, such as GPS, sensors and radar (side channel data or context data).

Figure 7. Therefore, theDoSattacks againstpseudonymousauthenticationwillbe fundamentally mitigated becausethe attacker cannot createa large number of forged certificates with valid puzzle values. As shown in Figure 5, according to our co-authentication mechanism, as the member of the mutual trust cluster {1, 2, 3, 4}, OBU1, OBU2 andOBU3 helptheirclusterheader OBU1 to generate puzzles to improve the puzzle value of Cert1. Similarly, OBU6 helps its cluster header OBU5 to generate puzzles to improve the puzzle value of Cert5.

Even if the DoS attackers use their all computational resources to generate puzzles, the co-authentication mechanism can integrate all computational resources of the mutual trust cluster to ensure that the puzzle values of legitimate vehicles will higher than attackers. Thus, these co-authentication actions will help to establish the mutual trust relationship between OBU1 and OBU5, and furthermore speed up the integration of the two mutual trust clusters, meanwhile unaffected by the stronger computational power of attackers. Conclusively, in PCA scheme, the co-authentication based on the mutual trust cluster can greatly speed up the mutual authentication between legitimate vehicles in 5G-VANET to ensure rapid response to the routine traffic related messages.

6. PERFORMANCE ANALYSIS

The ratio of data packets successfully delivered to destination nodes out of all the unique messages created. In this module, the performance of the proposed network coding method is analysed. Based on the analysed results X-graphs are plotted. Throughput, delay, energy consumption are the basic parameters considered here and X-graphs are plotted for these parameters

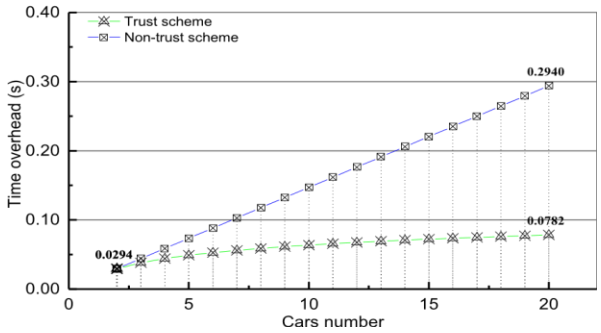

Fig 8: The theoretical time overhead of certificate verification when applying mutual trust cluster scheme and traditional scheme.

The entire pseudonymous authentication progress starts with the fact that all vehicles do not trust each other until each vehicle trusts the others. To further evaluate the time overhead optimizationof ourPCA schemeforthe entirepseudonymous authentication progress, we practice the entire pseudonymous authentication progress with and without PCA scheme in ns-2. In addition to the overhead of certificate verification, the overhead of the entire pseudonymous authentication progress includes the puzzles generation overhead, signature verification overhead, data transfer overhead, etc., which increase with the number of vehicles in the traditional scheme. The entire pseudonymous authentication progress is practiced with different number of vehicles, and the average time overhead of all vehicles are adopted to measure the performance of different scheme

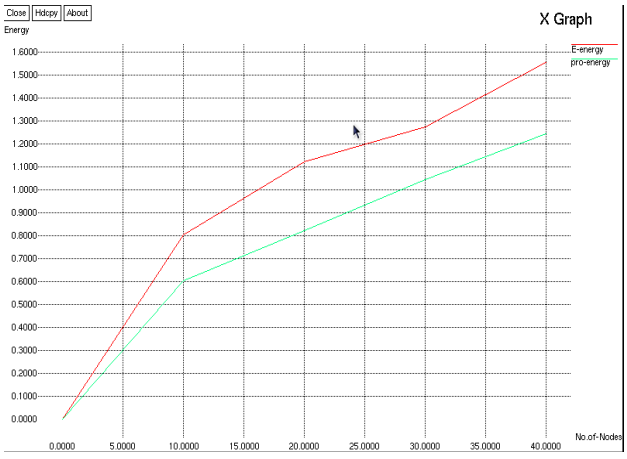

Fig 9: Energy consumption

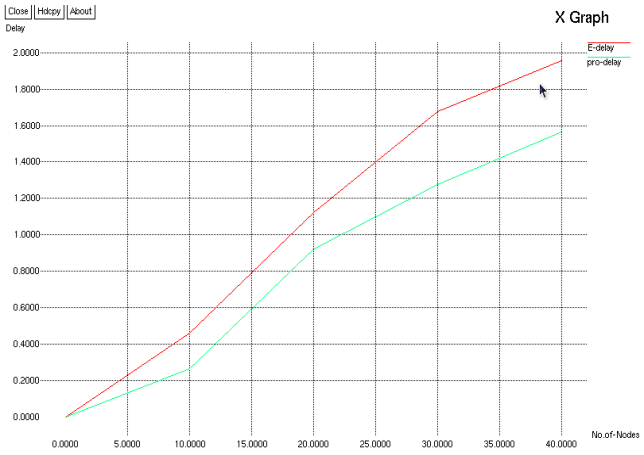

Fig 10: Delay Consumption

SIMULATION PARAMETERS	
PARAMETER	**VALUES**
Simulator	NS2
Area	1200 X 1200
Number of node	50
Physical Layer	IEEE 802.11
Routing protocol	AODV
Mobility model	Random way point
Radio type	802.11a/g
Transmission rate	1000 packets/s
Packet Size	1000
Pause time	0s
Source Node	10
Destination Node	30

7. CONCLUSION

VANET is projected to augment safety, comfort, transportation efficiency, and to overcome the environmental impacts of transportation, but at the presence of security footholds all the advantages can dim. In the presence of any weaknesses, attackers can exploit VANETs' availability, authentication, identification, confidentiality, integrity, data trust, privacy, and non-repudiation security goals. A successful security protocol shall be compliant with VANET security requirements with an all-inclusive approach. Moreover, there are many questions that need to be resolved prior to VANET's large-scale implementation. Several mature pseudonymous authentication schemes have beenproposedfor5G-VANETtoachievesecurityandprivacy of vehicles. However, the initial certificates verification overhead of pseudonymous authentication schemes may cause serious DoS attacks. In this paper,

we have proposed a puzzle based co-authentication scheme called PML-CIDS scheme. The hash puzzle is carefully designed to fundamentally restrict the attacker's capability to forge fake pseudonymous certificates, and collaborative verification is used to integrate the computing resources among legitimate vehicles, either as the certificate verifier or the certificate owner. Thus, our PML-CIDS scheme can provide capacity of resisting DoS attacks against pseudonymous authentication and improving the efficiency of certificates verification in 5G-VANET. Moreover, the PML-CIDS scheme can be easily combined with mutual pseudonymous authentication schemes to enhance the capacity of resisting DoS attacks and improving the efficiency of certificates verification.

REFERENCES

[1]. U. Rajput, F. Abbas, H. Eun, and H. Oh, ''A Hybrid Approach for Efficient Privacy-Preserving Authentication in VANET,'' IEEE Access, vol. 5, pp. 12014–12030, 2017.

[2]. C. Sun, J. Liu, X. Xu, and J. Ma, ''A Privacy-Preserving Mutual Authentication Resisting DoS Attacks in VANETS,'' IEEE Access, vol. 5, pp. 24012–24022, 2017.

[3]. C. Sun, J. Liu, X. Xu, and J. Ma, ''A privacy-preserving mutual authenticationresistingdosattacksinvanets,''*IEEEAccess*,vol.5,pp.24012–24022, 2017.

[4]. S. S. Manvi and S. Tangade, ''A survey on authentication schemes in VANETs for secured communication,'' *Veh. Commun.*, vol. 9, pp. 19 –30, Jul. 2017.

[5]. C. Sun, J. Liu, X. Xu, and J. Ma, ''A privacy-preserving mutual authenticationresistingdosattacksinvanets,''*IEEEAccess*,vol.5,pp.24012–24022, 2017

[6]. J. Li et al., ''Secure Distributed Deduplication Systems with Improved Reliability,'' IEEE Trans. Comput., vol. 64, no. 12, pp. 3569–3579, Dec. 2015.

[7]. N. Gupta, A. Prakash, and R. Tripathi, "Medium access control protocols for safety applications in Vehicular Ad-Hoc Network: A classification and comprehensive survey," Vehicular Communications, vol. 2, no. 4, pp. 223–237, 2015.

[8]. M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," Vehicular Communications, vol. 1, no. 2, pp. 53–66, 2014.

[9]. X. Lin and X. Li, ‘‘Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks,’’ IEEE Trans. Veh. Technol., vol. 62, no. 7, pp. 3339–3348, Sep. 2013

[10]. S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” Telecommunication Systems, vol. 50, no. 4, pp. 217–241, 2012.

[11]. A. Wasef, Y. Jiang, and X. Shen, ‘‘DCS: An efficient Distributed Certificate-Service Scheme for Vehicular Networks,’’ IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 533–549, Feb. 2010.

[12]. A. Wasef, Y. Jiang, and X. Shen, ‘‘DCS: An efficient distributedcertificate-service scheme for vehicular networks,’’ *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 533–549, Feb. 2010.

[13]. V. Yadav, S. Misra, and M. Afaque, “Security in vehicular ad hoc networks,” Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, p. 227, 2010.

[14]. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, ‘‘An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,’’ *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3589–3603 , 2010.

[15]. M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications,” IEEE Wireless Communications Magazine, Special Issue on InterVehicular Communications, vol. 13, no. LCAARTICLE-2006-015, pp. 8–15, 2006.