Dynamic Trust Based Authentication Algorithm Using RSA Crypto Key Exchange and Revocation in VANET Framework

Mrs. S. SuganthaPriya
Research Scholar, Department of Computer Science,
Dr. SNS Rajalakshmi College of Arts and Science,
Coimbatore, India.
sugantha2612@gmail.com

Dr. M.Mohanraj
Assistant Professor, Department of Computer Science,
Dr. SNS Rajalakshmi College of Arts and Science,
Coimbatore, India.
mohanrajsns@gmail.com

Abstract: Vehicular Ad-hoc Networks (VANETs) have emerged as a new application scenario that is envisioned to revolutionize the human driving experiences, optimize traffic flow control systems. Addressing security and privacy issues as the prerequisite of VANETs' development must be emphasized. This paper presents a novel approach of Dynamic trust based authentication (DTA) algorithm using RSA Crypto key exchange and revocation framework to measure the security related issues in VANET. The dynamic trust based authentication algorithm introduces a novel roadside unit (RSU) aided message authentication scheme to Base Station (BS), which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. In order to find invalid RSA signatures in a batch of signatures, to adopt group testing technique which can find invalid signatures efficiently. The experimental result analysis indicates that Dynamic trust based authentication (DTA) algorithm using RSA Crypto key exchange and revocation algorithm has very good adaption ability to the VANET network in terms of throughput, packet delivery ratio.

Keywords: *VANET, Base Station, RSU, RSA.*

INTRODUCTION

Vehicular Ad hoc Networks (VANET) is the subclass of Mobile Ad Hoc Networks (MANETs). VANET is one of the influencing areas for the improvement of Intelligent Transportation System (ITS) in order to provide safety and comfort to the road users. VANET assists vehicle drivers to communicate and to coordinate among themselves in order to avoid any critical situation through Vehicle to Vehicle communication e.g. road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc.

The VANET, a variant of the Mobile Ad-hoc Network (MANET), is a continuously self-configuring, infrastructure-less network which has emerged as a result of advances in wireless communications and networking technologies over the last few years [1-4]. Mobile nodes in VANETs are vehicles equipped with On-Board Units (OBUs), which are wireless communication devices. OBUs enable vehicles in VANETs to exchange traffic messages with nearby mobile nodes

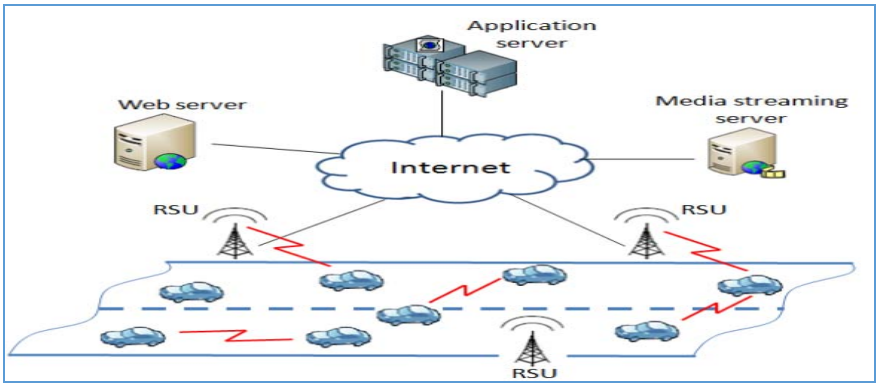

Fig. 1: Illustration of a VANET

Figure 1 describes some RSUs can act as a gateway for connectivity to other communication networks, such as the Internet. Each vehicle OBU has a wireless network interface which allows the vehicle to directly connect to other vehicles and RSUs within its communication range, as well as wireless or wired interfaces to which application units can be attached. By employing vehicle-to-vehicle (V2V) and vehicle-to-RSU (V2R) communications, VANETs can support a wide variety of applications in road safety, passenger infotainment, and vehicle traffic optimization, which are the main reason that VANETs have received significant support from government, academia, and industrial organizations over the globe.

The challenges of security must be considered during the design of VANET architecture, security protocols, cryptographic algorithm etc. The following list presents some security challenges [5].

Real time Constraint: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

Low tolerance for error: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.

Key Distribution: All the security mechanisms implemented in VANET dependent on keys. Each message is encrypted and need to decrypt at receiver end either with same key or different key. Also different manufacturer can install keys in different ways and in public key infrastructure trust on CA become major issue. Therefore distribution of keys among vehicles is a major challenge in designing a security protocols.

This paper present a Dynamic Trust Based Authentication Algorithm Using RSA Crypto Key Exchange and Revocation in VANET Framework is introduce a novel roadside unit (RSU) aided message authentication scheme to Base Station (BS), which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. The rest of the paper organized is as follows: Related work detailed is in Sect. 2. In Sect. 3, Design and implementation. In Sect. 4 Performance Evaluation and conclusion is in Sect. 5.

Related Work

(J. A. M. Naranjo, J. A. L. Ramos, and L. G. Casado, **2012) [6]** discussed an extended Euclidean algorithm provides a fast solution to the problem of finding the greatest common divisor of two numbers. In this paper, authors presented three applications of the algorithm to the security and privacy field. The first one allows one to privately distribute a secret to a set of recipients with only one multicast communication. It can be used for rekeying purposes in a Secure Multicast scenario. The second one is an authentication mechanism to be used in environments in which a public-key infrastructure is not available. Finally, the third application of the Extended Euclidean algorithm is a zero-knowledge proof that reduces the number of messages between the two parts involved, with the aid of a central server.

(P. Vijayakumar, S. Bose, and A. Kannan, **2013**) **[7]** considered the issue of large computation overhead caused by the safety message authentication. Especially, a cooperative message

authentication protocol (CMAP) is developed to alleviate vehicles' computation burden. With CMAP, all the vehicles share their verification results with each other in a cooperative way, so that the number of safety messages that each vehicle needs to verify reduces significantly. Furthermore, we study the verifier selection algorithms for a high detection rate of invalid messages in a practical 2-D road scenario. Another important contribution in this paper is that we develop an analytical model for CMAP and the existing probabilistic verification protocol, considering the hidden terminal impact.

(Rostamzadeh, et.al., **2015**) **[8]** proposed framework consists of two modules such that the first one applies three security checks to make sure the message is trusted. It assigns a trust value to each road segment and one to each neighborhood, instead of each car. Thus, it scales up easily and is completely distributed. Once a message is evaluated and considered to be trustworthy, their method then in the second module looks for a safe path through which the message is forwarded. Their frameworks are application-centric; in particular, it is capable of preserving traffic requirements specified by each application.

(Kang, et.al, **2016**) **[9]** discussedtheir scheme to integrate pseudonym with identity based signature (IBS) which could not only authenticate the messages in vehicular communication, but also protect the privacy of message generators. When vehicles receive numerous messages that need to be authenticated in a short time, we also apply batch verification to improve the efficiency of message disseminating. Then they adopted cipher text policy attribute based encryption (CP-ABE), which provides access control service to set expressive and flexible access structure for the specified vehicles in VANETs communication.

(Azees, et.al. **2017**) **[10]** proposed an efficient anonymous authentication scheme to avoid malicious vehicles entering into the VANET. In addition, the proposed scheme offers a conditional tracking mechanism to trace the vehicles or roadside units that abuse the VANET. As a result, their scheme revokes the privacy of misbehaving vehicles to provide conditional privacy in a computationally efficient way through which the VANET entities will be anonymous to each other until they are revoked from the VANET system. Moreover, the proposed scheme is implemented and the performance analysis shows that their scheme is computationally efficient with respect to the certificate and the signature verification process by keeping conditional privacy in VANETs.

(Islam, et.al. **2018**) **[11]**discussed about a privacy preserving authentication (CPPA) protocols based on CA-PKC (certificate authority-based public key cryptography), and ID-PKC (identity-based public key cryptography) have been put forwarded. In addition, some of these CPPA protocols use elliptic curve or bilinear-pairing for their implementation. The computation cost for bilinear-pairing and elliptic curve is very high compared to the cryptographic general hash function. Therefore, all the earlier protocols suffer from the heavy computational burden and some security weaknesses as well. Therefore, bilinear-pairing-free, robust and efficient CPPA with group-key agreement protocol for VANETs is essential. The authors presented a password-based conditional privacy preserving authentication and group-key generation (PW-CPPA-GKA) protocol for VANETs.

*(Zheng, et.al.,***2019**) **[12]** proposed a traceable and decentralized the Internet of Vehicle system framework for communication among smart vehicles by employing of a secure access authentication scheme between vehicles and RoadSide Units (RSUs). On the one hand, this

scheme allows that vehicles employ pseudonyms for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications anonymously in the non-fully trusted environment. On the other hand, the transparency of vehicles in authentication and announcement is preformed efficiently by the blockchain technology. In addition, the transaction information is tamper-resistant that provides the distributed and decentralized property for the different cloud servers. With the help of Certificate Authority (CA) and the RoadSide Units (RSUs), our proposal achieves the conditional privacy to trace the real identity of the malicious vehicle in the anonymous announcements as well.

METHODOLOGY

The proposed method accepts the Network Simulator 2.34 simulation parameters as input, where the Dynamic Trust Based Authentication Algorithm Using RSA Crypto Key Exchange and Revocation algorithm is applied. The overall proposed flow diagram in figure 1 follows a simulation procedure form start to end state.

Network Model (Vechicle Registration)

Vehicular Networks (VNs) consist of vehicles, Road-Side Units (RSUs) and a collection of backbone servers accessible via the RSUs. We assume that a single VN Operator (VNO) is responsible for deploying RSUs in the network. Due to their relevance to life-critical applications, VNs have to satisfy several strict requirements, namely sender and data authenticity, availability, liability, and real-time delivery.

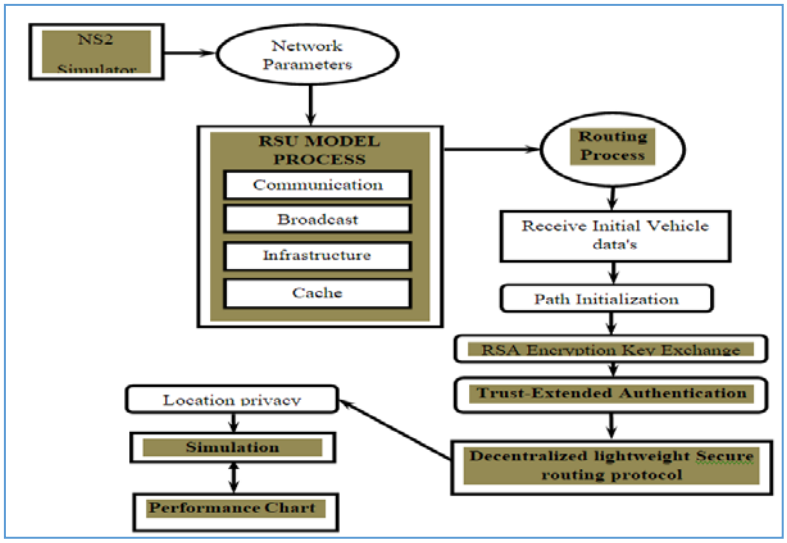

Fig.2: Proposed system flow diagram

The network model design is using network simulator 2.35 (NS 2.35) and the data packets by using the CBR (Constant Bit Rate) traffic model. The road system in our network consists of links and connectors. Each vehicle has a different ID. A connector joins two links. Roadways may have only one link (one-way path) or two links (2-way path) which depends upon the scenario. A link refers to one side of a roadway where vehicles move in the same direction. A link may have one or more Road side unit (RSU). RSU are defined areas on a link which generally allow only one type of vehicle to RSU within it. To define vehicle nodes (waypoints) which are also numbered starting from 1 along the imaginary central line of a link in its direction. Nodes are chosen in such a way that the shape of the imaginary line that joins them is most similar to the shape of the link. In addition, the distance between nodes is greater than

the average length of vehicles (5 m) so that a vehicle can occupy 2 nodes at the same time. We have placed the RSUs in the position of the nodes. Each of the RSUs is connected to the RSU through a wireless connection. So the transmission time from the RSU to RSU is negligible. The coverage area of RSUs is set in such a way that during some period of time a vehicle comes under the range of RSU while moving in the lane.

RSU MODEL PROCESS

To create a RSU network model to particularly interested in deploying n RSUs with transmission range R on a network topology of area equals to E and k intersections. In this model, i represents an intersection between two paths, and each element $v_j \in S_i$ is a vehicle crossing intersection i. An intersection is limited by the transmission range R of the RSU (assuming it is placed in the center of two crossroads). The weight (Distance) of $v_j$represents the time the vehicle remains in the intersection. In the case, there are v vehicles going around during the observation period, and τ is the minimum time required for a vehicle to contact a RSU and successfully transmit information. Note that the transmission does not need to be done by single RSUs. One of them can start transmission and another one finish it, as long as the sum of the times the vehicle remains in both intersection reaches the minimum time required for information dissemination.

Let $V = \{v_1, \ldots, v_v\}$ denote a set of vehicles, and $S_i \subseteq V$ represent a subset of vehicles that enters intersection i. To choose at most k sets in order to maximize the cardinality of $S_1 \cup S_2 \cup \ldots \cup S_k$. Consider $T_{n,v}$ the matrix of vehicle intersection, where $T_{i,j} \geq 0$ represents the total time vehicle j spends in intersection i. The maximum coverage problem with time threshold can be formulated as:

$$max \sum_{j=1}^{v} min\left(\tau, \sum_{i=1}^{n} T_{i,j} y_i\right) \text{eqn. (1)}$$

$$\sum_{i=1}^{n} y_i \leq k; \quad y_i \in \{0,1\}, \forall i \text{eqn. (2)}$$

where$y_i$indicates whether there is a RSU in intersection i. The objective function of equation (1) represents the maximum RSU coverage problem, while the controlling described in equation (2) ensures that at most k intersections are selected.

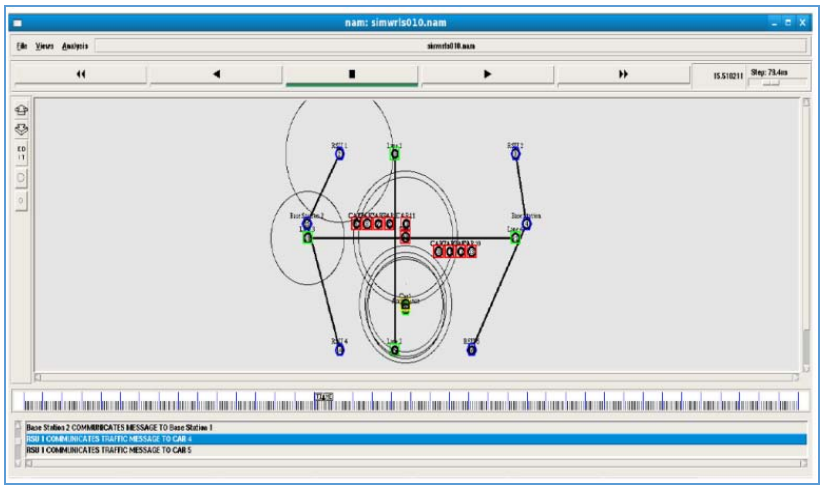

Fig.3:Communication between the RSU 1 and Car 4 Result

RSA CRYPTO KEY EXCHANGE AND REVOCATION

The RSA crypto key Encryption is a recommendation that defines structures for ensuring confidentiality on the message level. Similarly to Signature, it is possible to encrypt whole information's or only parts of them. Encryption, which is now an everywhere way of assuring a message is delivered privately, makes it so no intruder can bypass the cipher-text, which is essentially white noise. RSA would only be used to securely transmit the message keys. Thus, an efficient computing method of decryption must be found, so as to make RSA completely stand-alone and reliable.

Encrypt a message by raising it to the e^{th} power modulo n to obtain C, the cipher-text. We then decrypt C by raising it to the d^{th} power modulo n to obtain M again.

The encryption key generation as given below,

Select two large prime numbers p and q about the same size,

Typically each p, q has between 512 and 2048 bits

Compute n,

$n = pq$ and $\omega(n) = (q-1)(p-1)$ eqn. (2)

Select e,

$1 < e < \omega(n)$, s.t $\gcd(e, \omega(n)) = 1$ eqn. (3)

"gcd" means greatest common divisor

Compute d,

$1 < d < \omega(n)$, s.t $ed = 1 \bmod \omega(n)$ eqn. (4)

Algorithm1: Secure RSA Encryption

Step 1: The en-cipher-text value e is the binate portrayal.
Step 2: Put cipher text value as real.

Step 3: for *i = n, n-1, n-2,* …,0:

Put *C* is rest of squares of C when spitted by integer.

Step 4: Stop. Currently *C* is the enciphered form of text.

Vehicles rely on the presence of RSUs at road intersections to initiate a *Key Establishment* mechanism and establish a symmetric key. RSUs advertise their presence by periodically broadcasting beacons. As soon as a vehicle *vi*enters in the of transmission range of an RSU, *RBeacon*, it initiates the key establishment protocol described. As the vehicle knows its own location and the location of the RSU (announced in the beacon), it can estimate whether it is within the mix-zone, defined by a transmission range *RCMIX <RBeacon*. If so, the vehicle *vi*broadcasts one or, if needed, several key request messages (first message in Table 1). The RSU replies with the symmetric key *SK* encrypted with the public key of vehicle *vi*and a signature. *vi*receives and decrypts the message. If the message is validated, *vi*acknowledges it and *SK* can be used to encrypt all subsequent safety messages until *vi* leaves the mix-zone. In case RSUs are co-located (i.e., their mix-zones overlap), vehicles are aware of all CMIX keys so that they can decrypt all messages. Alternatively, co-located RSUs could coordinate to use the same CMIX key.

DYNAMIC TRUST BASED AUTHENTICATION ALGORITHM

The dynamic trust based authentication algorithm is based on decentralized authentication scheme, and the LEs need not to keep the authentication information of the entire vehicles. The proposed scheme involves eight procedures;

- Initial registration,
- Login,
- General authentication,
- Password change,
- Trust-extended authentication,
- Key update,
- Key revocation,
- Secure communication.

Before a vehicle can join a VANET, its on-board unit (OBU) must register with the AS. When a vehicle wants to access the service, it has to perform the login procedure. Next, the OBU checks the authentication state itself (i.e., the lifetime of the key). If the lifetime of the key is reduced to zero, the vehicle is mistrustful, and vice versa. The MV performs the general or trust-extended authentication procedure to be authenticated. The trustful vehicles assist other MVs in performing the authentication procedure or communicate with other trustful vehicles (i.e., secure communication procedure) to access the Internet. The trustful vehicle performs the key update procedure with the law executor (LE) when the key lifetime is below the predefined threshold.

The trust-extended mechanism based on the concept of transitive trust relationships to improve the performance of the authentication procedure. The state of a mistrustful OBU becomes trustful and then obtains an authorized parameter (i.e., PSK - A secure key set that is pre shared among LEs and the Authenticated Server) when the OBU is authenticated successfully. Then, the trustful OBU plays the role of LE temporarily to assist with the

authentication procedure of a mistrustful OBU. In this procedure, the trustful vehicle performs the authentication procedure and works as an LE. Note that it still does not need to store the authentication information of the user. Hence, our scheme only has a few storage spaces. Then, the steps of the general authentication and the trust extended authentication procedures are the same. As a result, all vehicles in a VANET can complete the authentication procedure quickly.

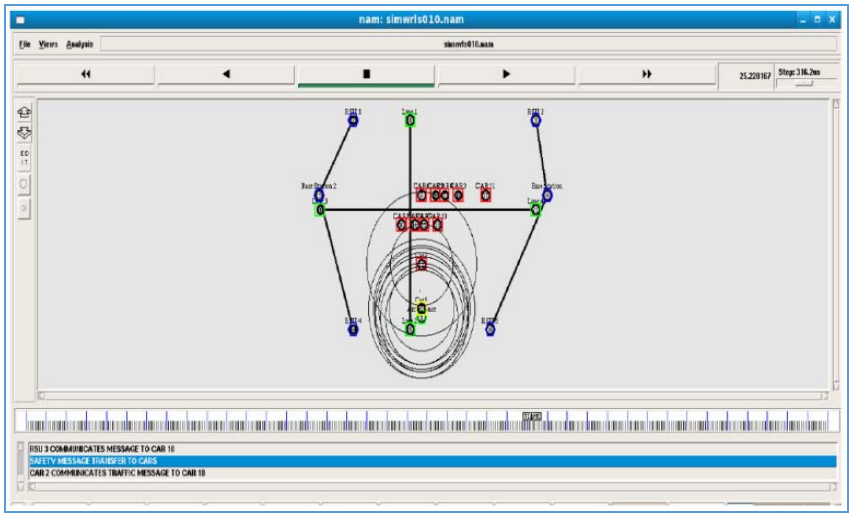

Fig.4:Dynamic Trust based Authentication Algorithm Result

PERFORMANCE EVALUATION

The proposed simulation environment is a grid topology over a 3000m × 3000m area. To use a tool (mobility model generator for vehicular networks; MOVE) to rapidly generate realistic mobility models for VANET simulations. The law executor (LEs) and normal vehicles are distributed randomly in the network. Each simulation result is the average of ten runs. The parameters and values used in the simulations are listed in Table 1.

Table 1: Simulation Parameter

PARAMETER	VALUE
Network size	3000m×3000m
Number of normal vehicles	100
Packet size	512 bytes
Hello message interval	100 ms
Simulation time	100 s
Transmission range (R)	100m, 200m, 300m
Number of LEs (LE)	5, 10, 15
Moving speed of vehicle (V)	10m/s, 20m/s, 30m/s

MAC protocol	IEEE 802.11

The performance of the protocol is evaluated with the following parameters:

- Throughput
- Packet Delivery Ratio (PDR)
- Comparison Ratio

THROUGHPUT: The ratio of the entire amount of data that arrives at a receiver from a source to the time it takes for the destination to obtain the final message is referred to as throughput.

T eqn. (5)

Fig.5:Graph of Throughput Ratio

PDR: The ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%). This parameter is also called "success rate of the protocols", and is described as follows:

$$PDR = \left(\frac{Receivepacketno}{SendPacketno}\right) \times 100 \; eqn.(6)$$

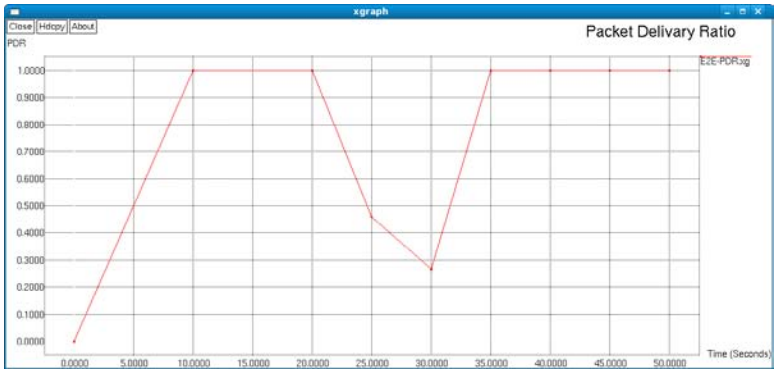

Fig.6:Graph of Packet Delivery Ratio

Comparison Ratio Average end-to-end delay comparisons of existing methods signify how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time.

$$D_{end-end} = N(d_{trans} + d_{prop} + d_{proc} \quad eqn.(7)$$

Where $D_{end\text{-}end}$= end-to-end delay, d_{trans}= transmission delay, d_{prop}= propagation delay, d_{proc} = processing delay, d_{queue}= Queuing delay and N= number of links.

This metric is useful in understanding the delay caused while discovering path from source to destination.

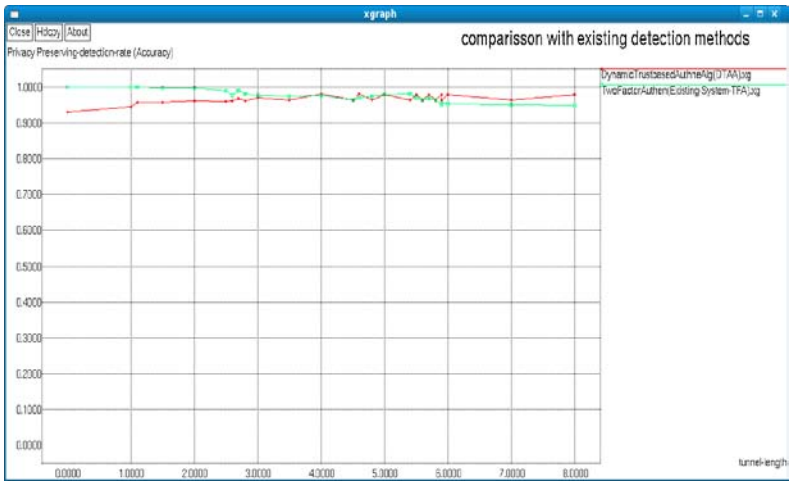

Fig.7:Graph of Comparison Result

CONCLUSION

In this paper implemented and evaluated a VANET network using Dynamic Trust Based Authentication Algorithm Using RSA Crypto Key Exchange and Revocation algorithm in NS 2.35 Framework. The Dynamic Trust based Authentication (DTA) algorithm introduces a novel roadside unit (RSU) aided message authentication scheme to Base Station (BS), which makes RSUs responsible for verifying the authenticity of messages sent from vehicles and for notifying the results back to vehicles. Meanwhile, authentication scheme can make vehicles verify a batch of signatures once instead of one after another, and thus it efficiently increases vehicles' message verification speed. In addition, DTA scheme achieves conditional privacy: a distinct crypto key identity is generated along with each message, and a trust authority can trace a vehicle's real identity from its fake identity. In order to find invalid RSA signatures in a batch of signatures, to adopt group testing technique which can find invalid signatures efficiently.

The future work will focus on develop to identify a malicious packet dropping detection technique that effectively detects the packet dropping attack in any environment while keeping the generated overheads minimal will be focus.

REFERENCES

1. T. Chim, S. Yiu, L. Hui, and V. Li(2011). SPECS: Secure and privacy enhancing communications schemes for VANETs. Ad Hoc Networks, 9, 12, 189-203.
2. S. Zeadally, R. Hunt, Y. Chen, A. Irwin, and A. Hassan (2012), Vehicular Ad Hoc Networks (VANETs): Status, Results, and Challenges. Telecommunication Systems, 50, 4.
3. M. Ghosh, A. Varghese, A. Gupta, A. Kherani, and S. Muthaiah (2010). Detecting misbehaviors in VANET with integrated root-cause analysis. Ad Hoc Networks, 8, 7, 778-790.
4. J. Tellez, S. Zeadally, and J. Camara (2010). Security Attacks and Solutions for Vehicular Ad-Hoc Networks, IET Communications Journal, 4, 7.
5. Moustafa,H., Zhang,Y.(2009). Vehicular networks: Techniques. Standards, and Applications, CRC Press
6. J. A. M. Naranjo, J. A. L. Ramos, and L. G. Casado (2012). A suite of algorithms for key distribution and authentication in centralized secure multicast environments, J. Comput. Appl. Math., 236,12, 3042–3051.
7. P. Vijayakumar, S. Bose, and A. Kannan (2013). Centralized key distribution protocol using the greatest common divisor method. Comput. Math. Appl.,65, 9, 1360–1368.
8. K. Rostamzadeh, H. Nicanfar, N. Torabi, S. Gopalakrishnan, and V. C. M. Leung (2015). A context-aware trust-based information dissemination framework for vehicular networks. IEEE Internet of Things Journal, 2, 2, 121–132.
9. Q. Kang, X. Liu, Y. Yao, Z. Wang, and Y. Li (2016). Efficient authentication and access control of message dissemination over vehicular ad hoc network. Neurocomputing, 181, 132–138.
10. M. Azees, P. Vijayakumar, and L. J. Deboarh (2017). EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 18,9, 2467–2476.
11. S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy (2018). A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Generation Computer Systems, 84, 216–227.
12. D. Zheng, C. Jing, R. Guo, S. Gao and L. Wang (2019). A traceable blockchain-based access authentication system with privacy preservation in VANETs. IEEE Access, 7, 117716-117726.