ISSN: 2321-7782 (Online)
Volume 3, Issue 5, May 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Security and Authentication Process using ECC in VANET

Rukaiya Shaikh[1]
G.H.R.I.E.T., Savitribai Phule University, Pune
Lecturer, Dept.of Comp.Engg
Pune – India

Disha Deotale[2]
G.H.R.I.E.T., Savitribai Phule University, Pune
Professor, Dept.of Comp.Engg
Pune – India

Abstract: Vehicular ad hoc networking (VANET), is based on vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, these are the two key technology for improving road security and transport effectiveness. VANET also supports on-road infotainment. VANET may extensively get better our daily lives, especially driving experience. GPS and navigation systems are very beneficial, as they are very efficiently integrated with traffic reports to provide services to get the fastest route to work.

In this proposed work, A System that collects the real time road information from Vehicular ad hoc network (VANET) which, provide helps to the drivers to reach at desired destinations in a real-time and distributed manner. The proposed system has the advantage of using real-time road conditions which is used to compute a better route and at the same time, the information source can be properly authenticated.

In this system the use of Elliptic Curve algorithm to authenticate source and also reduce the delay and network overhead. Cars are highly personal devices that are kept for a long periods, therefore privacy of users should be enforced to protect its personal data from being disclosed to unauthorized observers. To protect the privacy of the vehicles, the message must be anonymously transmitted in VANETs. To protect the privacy of the drivers, the query (destination) and the driver who issues the query are guaranteed to be un-linkable to any party including the trusted authority. The anonymous credential is use to achieve this goal. Authentication and privacy preserving are basic requirements of any VANET security system; along with these basic requirements our system fulfills all other necessary security requirements. The entire authentication is done through main server. But if it fails then all system will stop from functioning. Hence a system is also proposed to solve single server problem by introducing replica server.

Keywords: Navigation, Secure Vehicular Sensor Network, Signature Verification, Pseudo Identity, Anonymous Credential, Proxy Re-encryption, Elliptic Curve Algorithm.

I. INTRODUCTION

In the old days, a driver usually refers to a hard copy of the atlas in order to find route to a certain destination. The drawbacks are quite obvious. With the introduction of Global Positioning System (GPS), GPS-based navigation systems become widely popular. However, the route searching procedure of these GPS systems is based on a local map database and real-time road conditions are not taken into account. Traffic Message Channel (TMC) which has been developed and used to learn about real-time road conditions. TMC makes use of FM radio data system to broadcast real-time traffic and weather information to drivers. Special equipment is required to decode or to filter all the information received. However, only special road conditions (e.g., severe traffic accident) are broadcasted and a driver cannot obtain information like the general fluency of a road from TMC.

Now a day, Vehicular Ad hoc Network (VANET) becomes more popular in many countries. It is an important element of the Intelligent Transportation Systems (ITSs). In a VANET, each vehicle is assumed to have an On-Board Unit (OBU) and there is Road-Side Units (RSU) that is installed along the roads. A Trusted Authority (TA) and some other application servers are installed in the back end. The OBUs and RSUs communicate using the Dedicated Short Range Communications (DSRC) protocol over the wireless channel. The RSUs, TA, and the application servers communicate by using a secure fixed network (e.g., the Internet).

VANET allow arbitrary vehicles to broadcast safety messages such as vehicle speed, turning direction, traffic accident information etc to other nearby vehicles on regular basis so that other vehicles may adjust their traveling routes and RSUs may inform the traffic control center to adjust traffic lights for avoiding traffic congestion.

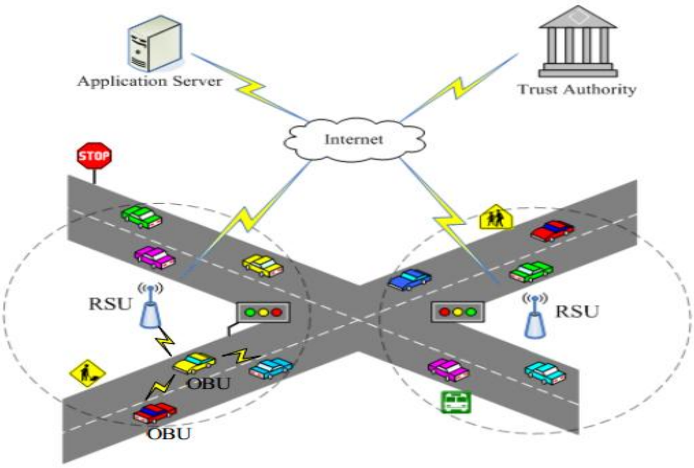


Figure 1:Overview of VANET

A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. As shown in figure 1 VANET is created using following units:

1. OBU (On-Board Units) – communication devices mounted on vehicles
2. RSU (Road Side Units) – communication units located aside the roads
3. OBU used to communicate with other vehicles or RSUs
4. SRSUs connect with application servers and trust authorities

By using these units VANET communicates with one another but, VANET adapts different types of communication patters. By using those patterns VANET decides how VANET packets flow from one unit to another. As shown in figure 2 types of communication patterns-

1. Roadside-to-Vehicle Communications (RVC or V2I)
2. Inter-Vehicle Communications (IVC or V2V)
3. Inter road side communication

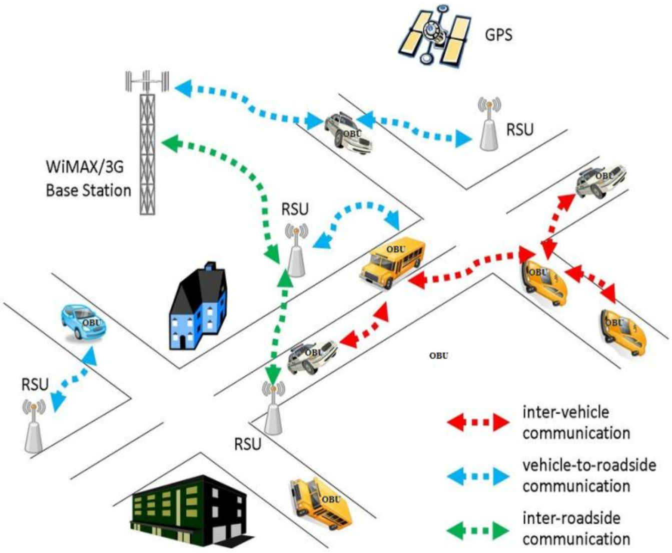

GPS
RSU
WiMAX/3G
Base Station
RSU
OBU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Figure 2: Types of communication patterns

In this paper, proposes a new application—VANET based system which makes use of the collected data to provide navigation service to drivers. Based on the destination and the current location of the driver (the query), the system can automatically search for a route that yields minimum travelling delay in a distributed manner using the online information of the road condition. Provided security for messages sent in the system with better authentication and signed to make sure that they were not modified by anyone. Also it's maintaining the privacy for query and navigation real time data which forwarded from server, RSU and OBU.

II. Literature Survey

So many studies have been reported on how to provide security and privacy preservation in VANETs.

In [5], author proposed work on securing vehicular ad hoc network, where each vehicle is pre-loaded with a large number of anonymous public and private key pairs and their corresponding public key certificates. There is a pseudo identity in each public key certificate. Traffic messages are signed with a public key based scheme, and each public and private key pair has a short life time to achieve privacy preserving. To avoid pre-loading a large number of anonymous key materials in each vehicle.

In [6], author introduced a group signature scheme to sign each message. In this scheme, each vehicle has only one public and private key pair. The public key is the same for all vehicles, and the private key of each vehicle is different. For a message signature, a vehicle only knows the authenticity of the signature, and the vehicle has no information on the identity of the message sender.

In [7], author introduced real-time navigation using VANET. This scheme is of a small scale that covers a car park. Here a car park is monitored by three RSUs that perform the roles of determining a vehicle's location, searching for a vacant parking space, and providing navigation service to guide the vehicle to go from the car park entrance to the selected parking space. In order to fulfill security requirement it assumes RSUs to be fully trusted. This makes sense because the three RSUs are installed indoors and can be monitored by security guards. Thus, the work provided by author it cannot be used to solve the navigation problem in wider area.

In 2014 VSPN: VANET-Based Secure and Privacy-Preserving Navigation[1] provides secure way to handle inter vehicle messages, finds shortest path and also preserve drivers and query privacy. But here main monitoring agent and authority server is handled by only single server. If that server fails then whole VANET application stops working properly. VANET is very high mobility model and here authentication done after every time frame T.

Here, authentication takes longer time which reduced here by using ECC algorithms.

2.1 Attacks: VANET facing many attacks, some of these attacks are as follows.

1) Denial of Service Attack (DoS): Denial of Service attack happens when the hacker or attacker takes control of a all the vehicle's resources.

2) Message Suppression. An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver. The attacker suppresses these packets and he can use that packet again in other time

3) Alteration Attack. In this type of attack, an attacker simply alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted.

4) Sybil Attack. Sybil attack is the creation of multiple fake nodes broadcasting false information.

III. Proposed System

The use of real time road conditions to compute a better route and at the same time, the information source can be properly authenticated. It utilizes the online road information collected by a vehicular ad hoc network (VANET) to guide the drivers to desired destinations in a real-time and distributed manner with Privacy-Preserving Navigation.

Hence a system is proposed to solve single server problem by introducing replica server. Whenever primary server stops functioning:

a. Every vehicle's and RSU's information is stored in backup/replica server.

b. Whenever main server not able to function then, every vehicle starts to communicate with Secondary server. All the process starts with step 1 with secondary server.

c. All the newly generated certificates are stored with secondary server.

d. All authentication and key sharing is done only by secondary server.

IV. System Implementation

A. System Architecture

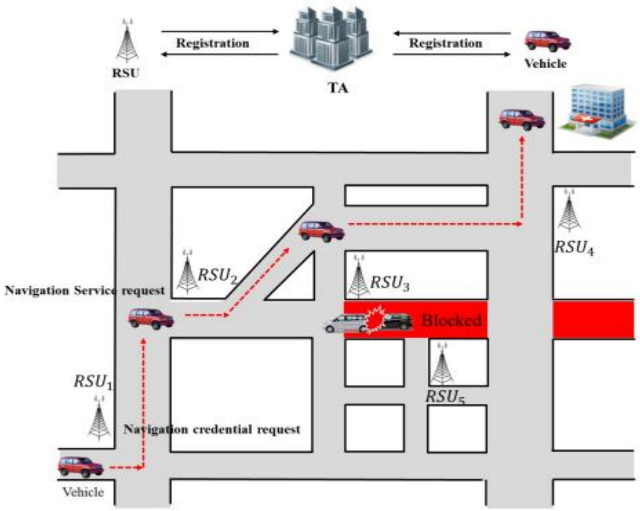


Figure 3 : System Architecture

It consists of a Trusted Authority (TA), a Tracing Manager (TM), RSUs and vehicles.

• **TA**- The responsibility of the TA is to issue digital certificates for vehicles and RSUs. Also; it maintains a Certificate Revocation List (CRL) containing the certificates of revoked vehicles. The TA is assumed to be completely trustable, hard to compromise, and powerful, i.e. with sufficient computation and storage capacity.

• **TM**- When the content of a safety message broadcast by a vehicle is found to be false, the TM should be able to determine the vehicle's real identity.

• **RSU**- RSUs are densely distributed in the road side. In our protocol, RSUs are used to issue secret member keys to vehicles and assist the TM to efficiently track the real identity of a vehicle from any safety message. Vehicle- Vehicles move along the roads, sharing collective environmental information, contained in safety messages, or requesting secret member keys from RSUs. OBUs are assumed to be embedded in each vehicle. By using OBUs, vehicles can communicate with each other as well as with the RSUs. The communication among them is based on the DSRC protocol [DSRC].

B. Basic Steps

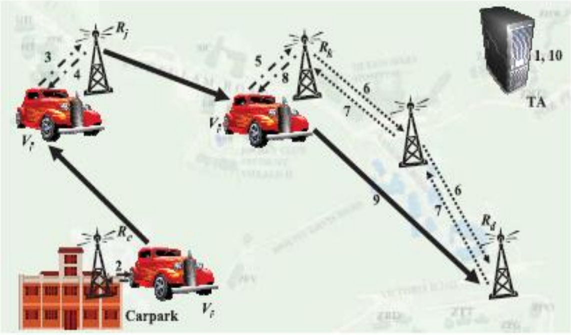


Figure 4 :Basic Steps

These are the Basic Steps:

1. First TA sets up parameters and generates anonymous credentials.
2. Vehicle Vi's tamper-proof device starts up and requests for the master secret s from RSU Rc.
3. Tamper-proof device requests for a navigation credential from RSU Rj.
4. RSU Rj verifies Vi's identity and sends its tamper proof device an anonymous credential.
5. After a random delay or after traveling for a random distance, Vi's tamper-proof device sends out its navigation request to RSU Rk.
6. RSU Rk forwards the navigation request to its neighbors. This process repeats until the request reaches RSU Rd covering the destination.
7. RSU Rd constructs the navigation reply message and sends it along the reverse path. Each hop along the path attaches the corresponding hop information (with signature).
8. RSU Rk forwards the navigation reply message to Vi's tamper-proof device which then verifies the messages from all RSUs along the route in a batch.
9. By presenting the navigation session number, each RSU along the route guides Vi to reach the next RSU closer to the destination.
10. Based on Vi's pseudo identity received from RSU Rj, TA reveals Vi's real identity for billing purpose.

C. Algorithm

A] Elliptic Curve Cryptographic Algorithm:

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

• The equation of an elliptic curve is given as,

y2 = x3 + ax + b

Few terms that will be used,

E -> Elliptic Curve

P -> Point on the curve

n -> Maximum limit (This should be a prime number)

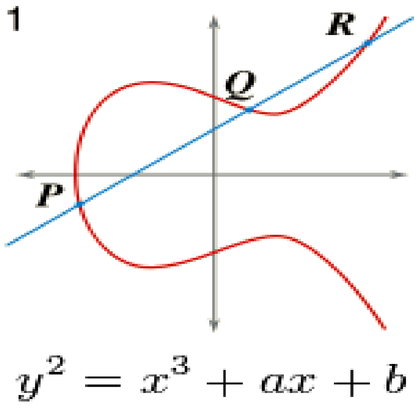


Figure 5: Simple Elliptic Curve

B] *Key Generation:*

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, we have to select a number 'd' within the range of 'n'. Using the following equation we can generate the public key

Q = d * P

Where:

d = the random number that we have selected within the range of (1 to n-1).

P = the point on the curve.

'Q' is the public key and 'd' is the private key.

C] Encryption:

Let 'm' be the message that we are sending. We have to represent this message on the curve. This has in-depth implementation details. All the advance research on ECC is done by a company called certicom.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)].Two cipher texts will be generated let it be C1 and C2.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be send.

D] Decryption:

We have to get back the message ‘m’ that was send to us,

M = C2 – d * C1

M is the original message that we have send.

D. Modules

1. VANET setup
2. Setup Process by TA
3. Credential Generation
4. Master Key Activation
5. Credential Request
6. Requesting for Navigation Service by Vehicle Tamper-Proof Device
7. Communications among RSUs
8. Verification
9. Destination Guidance by RSUs
10. Change of Route
11. Trace of Real Identity
12. Replica Server

E. Security Requirements

The aim at designing a scheme to provide VANET-based navigation to satisfy the following security requirements:

A. Message Integrity And Authentication - A vehicle should be authenticated before it can issue a navigation query. On the other hand, an RSU (vehicle) is able to verify that a message is indeed sent and signed by a certain vehicle (RSU) without being modified by anyone.

B. Identity Privacy Preserving - The real identity of a vehicle should be kept anonymous from other vehicles as well as from RSUs and a third-party should not be able to reveal a vehicle’s real identity by analyzing multiple messages sent by it.

C. Traceability - Although a vehicle’s real identity should be hidden from other vehicles and RSUs, TA should have the ability to obtain a vehicle’s real identity so that the vehicle can be charged for using the navigation service. Also TA has the role to maintain liability via non-repudiation property of messages when accidents happen on the road.

D. Confidentiality - The content of a query and that of a navigation result should be kept confidential from eavesdroppers.

E. Unlinkability - Even if all RSUs and TA collude, they cannot link up a vehicle’s query with its real identity.

F. Robust - An adversary can provide alternative to primary server

G. Efficient - Ad adversary model can provide efficient authentication model which reduces delay in make decision efficient.

F. Mathematical Model

A] Set Theory:

1] Let S be a system getting request and give response by packets

$S = \{I, O, F\}$

2] V is set of vehicles in city so it will contain n number of vehicle in city each vehicle required TA

$V = \{V1, V2, V3, \ldots\ldots\ldots\ldots\ldots \; Vn\};$

3] Let P is set of packets with request from vehicle to replica server in current location in city $P = \{p1, p2, \ldots\ldots ...pn\};$

4] Packet catch by replica server so R be a set of replica server in city RSU.Let R set of replica server in city $R = \{R1, R2. \ldots\ldots .Rn\};$

5] Mathematically, Get a packet and send to replica server to verify vehicle current location of vehicle IF (Not trusted) are placed along roadside.

6] Then L is set of location in city and PA is set of all paths in city

$L = \{L1, L2, \ldots\ldots\ldots\ldots\ldots\ldots .Ln\};$

$PA = \{PA1, PA2, \ldots\ldots\ldots\ldots\ldots .PAn\};$

7] CP be set of changed path for travel in city

$CP = \{c1, c2, \ldots\ldots\ldots cn\};$

Input Set Contains Set of request, packet, rules, operations

$I = \{V, P, R, PA, L\};$

In output set, it contain sets of flags and *ri* new rule which insert into set RL

O= {P,CP};

In Functional set, it will contain set of question, answer, flags, packet, cluster, snort, snort signature, set of rules and operation

F={V,P,R,L,PA,CP};

B] Complexity Analysis:

Let,

$\mathbf{T_{mul}}$ denote the time required to perform one point multiplication over an elliptic curve.

$\mathbf{T_{mtp}}$ denote the time required to perform one MapToPoint hash function.

$\mathbf{T_{par}}$ denote the time required to perform one pairing operation.

Consider the $\mathbf{T_{aenc}}$, $\mathbf{T_{adec}}$, $\mathbf{T_{senc}}$, $\mathbf{T_{sdec}}$, $\mathbf{T_{csig}}$, and $\mathbf{T_{renc}}$ denote the time required to perform Asymmetric Encryption, Asymmetric Decryption, Symmetric Encryption, Symmetric Decryption, Conventional Signature, and Re-encryption operations.

All these above operations dominate the speed of signature generation and signature verification, Here, consider only the time taken by these operations & neglected all other operation such as addition, scalar value manipulation, and one-way hash function.

Case 1 & 2 : In this proposed VSPN approach, have ignored the time complexity involved in setup because it is done in offline mode and It does not affect on efficiency of VSPN scheme.

Case 3: TA takes $\mathbf{T_{mul} + T_{mtp} + T_{senc}}$ of time to generate the navigation credential for the current period.

Case 4: Vehicle V_i takes $\mathbf{T_{csig}}$ of time to sign the master key request message. Next, the RSU nearby takes Tmul + Tmtp of time to verify Vi's certificate and then takes Trenc of time to re-encrypt the master key for Vi.

Case 5: When vehicle Vi requests for an anonymous credential, it takes 5Tmul + 2Tmtp of time for generating a signature. Finally, the RSU takes 2Tsenc of time to encrypt the credential for the current session for Vi.

Case 6 : When vehicle Vi requests for navigation service, it takes Taenc of time to encrypt the request message. The RSU nearby then takes Tadec of time to decrypt the message and then takes Tmtp of time to verify the anonymous credential presented by Vi.

Case 7: Each RSU hop takes $\mathbf{T_{mul} + T_{mtp}}$ of time to sign its hop information.

Case 8: Vehicle V_i takes 2 $\mathbf{T_{mtp}}$ of time to verify each RSU hop's certificate and signature on hop information.

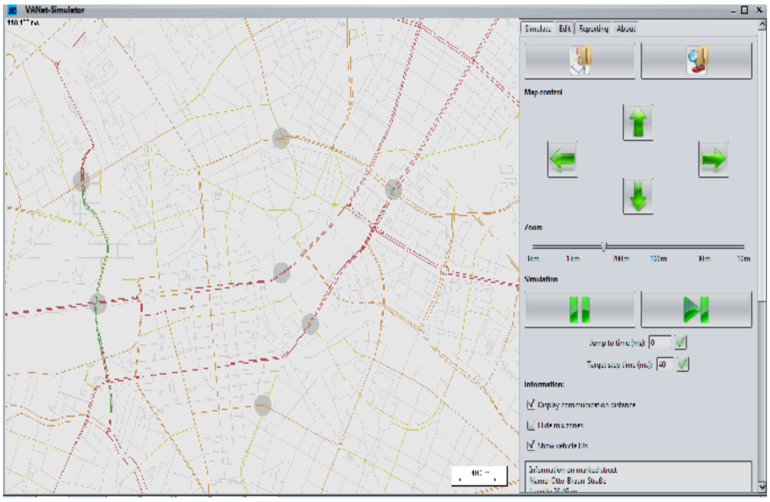
Case 9: Vehicle V_i takes T_{aenc} of time to generate the guiding service request message to an RSU nearby.

Case 10: If a road within an RSU's range is blocked that RSU takes $\mathbf{T_{mul} + T_{mtp}}$ of time to sign a road blocking message.

Case 11: TA can trace a vehicle's real identity in $\mathbf{T_{mul}}$ of time.

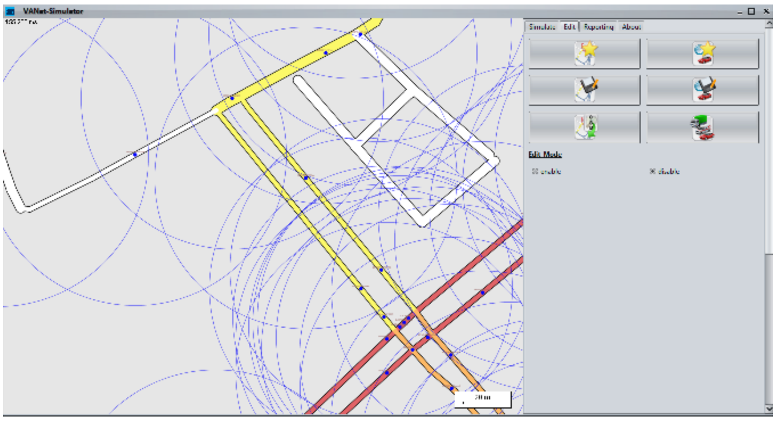
V. Simulation Methods

1: This is a simulation of Berlin Open Street Map project for VANET, used this map to create a street view.

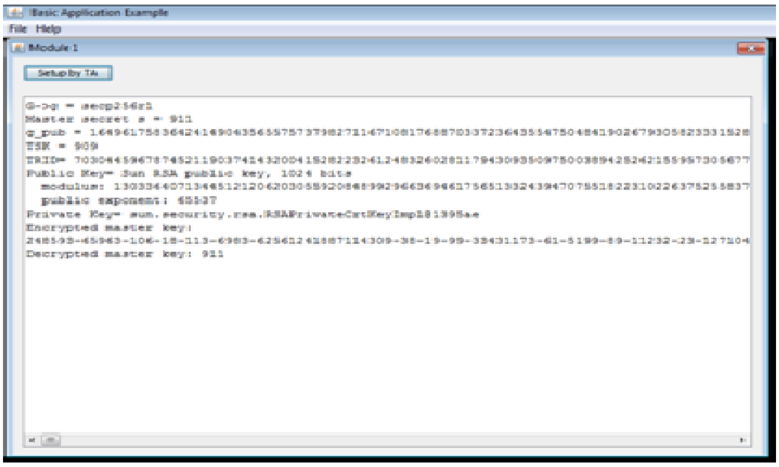


Jump to time (ms): 0
Target step time (ms): 40
☑ Display communication distance
□ Hide mix zones
☑ Show vehicle IDs
Information on marked street:
Name: Otto Braun Straße

2: This is zoom view of VANET infrastructure where vehicle are shown moving.



3: This is output of our ECC algorithm where generated the master secret key and generated ECC public and private keys for cryptography. Then this ECC keys is used for encryption of master keys.



```
G->g = secp256r1
Master secret s = 911
g_pub = 16496175836424149043565575737982711467108176887033723643554750484190267930582333 1528
TSK = 909
TRID= 7030445967874521190374243200415282232412483260281179430935097500389425242155957305677
Public Key= Sun RSA public key, 1024 bits
  modulus: 130336407134651212062030559208489929663696617565133243947075518223102263752 5 5837
  public exponent: 65537
Private Key= sun.security.rsa.RSAPrivateCrtKeyImpl@1395ae
Encrypted master key:
2485-93-45963-106-18-113-6983-625612 41887114309-38-19-99-33431173-61-5199-89-11232-23-12 7104
Decrypted master key: 911
```

VI. Conclusion

This system is proposed a VANET-based secure and privacy-preserving navigation scheme in this paper. It utilized the speed data and road conditions collected by RSUs to guide vehicles to desired destinations in a distributed manner. This scheme adopts some security primitives in a nontrivial way to provide a number of security features: 1) Vehicles are authenticated by means of pseudo identities. 2) Navigation queries and results are protected from eavesdroppers. Besides, with the idea of anonymous credential, no one including TA can link up a vehicle's navigation query and its identity. 3) Information provided by RSUs can be properly authenticated before the route is actually being used. Besides satisfying all security and privacy requirements, our solution is efficient in the sense that a vehicle can complete the whole navigation querying process and receive urgent notification in a very short time. The authentication process at vehicles can be even simpler because a vehicle only needs to check against the central server's signature on the processed result. And also in case centralize server fails then all system fails to work but here this problem is resolved by introducing replica server.

References

1. Chim, T., et al. "VSPN - VANET-based secure and privacy preserving navigation." (2012): 1-1.
2. J.Parthasarathy POSITIONING AND NAVIGATION SYSTEM USING GPS International Archives of the Photogrammetry, Remote Sensing and Spatial Information Science, Volume XXXVI, Part 6, Tokyo Japan 2006
3. Smitha Shekar B , Narendra Kumar G , Usha Rani H V , Divyashree C K , Gayatri George and Aparajitha Murali GPS Based Shortest Path for Ambulances using VANETs 2012 International Conference on Wireless Networks (ICWN 2012).
4. "Traffic Message Channel (TMC)," http://www.tmcforum.com/,2004.
5. M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," Journal of Computer Security, Vol. 15, No. 1, pp. 39-68, 2007.

6. X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: a secure and privacy-preserving protocol for vehicular communications” IEEE Transaction on Vehicular Technology, Vol. 56, No. 6, pp. 3442-3456, 2007.

7. R. Lu, X. Lin, H. Zhu, and X. Shen, “SPARK: A New VANET-Based Smart Parking Scheme for Large Parking Lots,” Proc. IEEE INFOCOM ’09, pp. 1413-1421, Apr. 2009.

8. D. Chaum, “Security without Identification: Transaction Systems to Make Big Brother Obsolete,” Comm. ACM, vol. 28, pp. 1030- 1044, 1985.

9. E. Aimeur, H. Hage, and F.S.M. Onana, “Anonymous Credentials for Privacy-Preserving E-learning,” Proc. IEEE MCETECH Conf. e-Technologies (MCETECH ’08), pp. 70-80, July 2008.

10. G. Samara, W. Al-Salihy, and R. Sures, “Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET),” Proc. IEEE Fourth Int’l Conf. New Trends in Information Science and Service Science (NISS ’10), pp. 393-398, May 2010.

11. K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust Location Privacy Scheme for VANET,” IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

12. K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, “AMOEBA: Robust Location Privacy Scheme for VANET,” IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

13. C. Zhang, X. Lin, R. Lu, and P.H. Ho, “RAISE: An Efficient RSUAided Message Authentication Scheme in Vehicular Communication Networks,” Proc. IEEE Int’l Conf. Comm. (ICC ’08), pp. 1451- 1457, May 2008.

14. T. Chim, S. Yiu, L.C. Hui, and V.O. Li, “SPECS: Secure and Privacy Enhancing Communications for VANET,” Elsevier Ad Hoc Networks, vol. 9, no. 2, pp. 189-203, Mar. 2010.

15. R. Hwang, Y. Hsiao, and Y. Liu, “Secure Communication Scheme of VANET with Privacy Preserving,” Proc. IEEE 17th Int’l Conf. Parallel and Distributed Systems (ICPADS ’11), pp. 654-659, Dec. 2011.