CONTROLLING OVER THE SUMO BY TRACI IN VEHICULAR ADHOC NETWORK

Aditi Selokar[1], Vaishali Sahare[2]

[1] Student, Computer Science And Engineering, G.H R.I.E.T. For Women, Nagpur, Maharashtra, India.
[2]Assistant Professor, Computer Science And Engineering, G.H R.I.E.T. For Women, Nagpur, Maharashtra, India.

Abstract

Security is the main issue in the VANET because VANET provides the safety related application and save the human lives. VANET can save our time by providing the information not only about the busy traffic but also security. But the main issue is considering the security related such as security of the driver and passengers. The security information contains the information like location, identifier and the network. So for preventing from many attacks and save the lives of driver and passengers, there are many security related algorithms, protocols and infrastructure for secure key distribution, revocation and secure exchange of the messages which contain the private information. For providing the secure communication, we use a cryptography technique known as ECDSA is use. This cryptography technique provides the security from the various types of attack and can help in providing the authentication to the vehicles. The vehicles have the ability to self authenticated in the network but this authentication is not secure. So for this reason the ECDSA can provide the secure authentication to the vehicles and provide the secure communication between the vehicles. This paper can give the information about the proper route finder known as AODV to exchange the message. The advantage of this routing and cryptography method is that by using real tine road condition to compute the better route and at the same time, prevents from the traffic congestions.

***Keywords:** VANET, ECDSA, AODV, SUMO, Traci*

--***--

1. INTRODUCTATION

There is an increasing growth of vehicles on the road .for that we should provide safety information to the vehicles. It totally means that VANET should provide a secure vehicular traffic to the atmosphere and environment. Vehicular Adhoc Network nothing but a Mobile Adhoc Network. VANET provides vehicular communication such as vehicles to the vehicle (V-V) and vehicles to the nearby fixed equipments called as Road Side Units (RSU).VANET should also provide communication to the vehicles to the infrastructure called as the On Board Unit (OBU).In VANET there are two types of node exits they are as follow

1) OBS is a on board unit and it is working for mobile nodes.
2) RSU is a road side unit and is working for fixed node along with the route.

The VANET should communicate with each other in three ways they are as follow,
1) Vehicles to vehicles communication (It is also called as Inter-vehicles communication).
2) Vehicles to roadside communication (It is also called as Intra-vehicles communication).
3) Inter roadside communication.

IEEE 802.11p is an enhancement of the IEEE 802.11 standard to the Wireless Access in Vehicular Environments (WAVE) and it can also support Intelligent Transportation Systems (ITS) applications. Intelligent Transportation System application can include exchange the data between the vehicles which have higher speed and the RSU of the given frequency range defined by ITC band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 should be the higher layer standard and it is based on the IEEE 802.11p. Because of such frequency the special radio wave and sensors should be embedded in the car.

VANET provide ideal way of collecting traffic information and various physical quantities related to the traffic awareness at low cost and high accuracy. VANET can take attention from the academic and industrial development because of the various applications. VANET should provide a best facility for the future purpose. For example, safety information, alert messages, route information, location update, warning message, accident messages, etc.

VANET provides the various security algorithms for proper message transmission. When message should transmit then intimidator can change the message such as modifying the message, replaying the message, false information should be injected in the message. In this way the fake/false messages should be transfer from one vehicle to the other and which arises a misunderstanding between the physical quantities in the vehicle. This raises life critical issues. This causes the error in the system. For that VANET should provide authentication and message integrity. In this way the VANET should maintain the security, privacy and sensitivity in the system.

In previous paper, author uses conditional privacy-preserving authentication scheme, CPP-BAT. This is the ID base scheme. In this scheme the time required to transfer the message is more for that the duplicated message should be transfer from vehicle to the vehicle. This scheme should achieve the source identification but cannot achieve the destination identification. This scheme also achieves message integrity, identity anonymity and traceability while maintaining the efficiency as good as possible. But in this paper when the accident takes place, the sensor in the car can be activated and send the message to base station and from base station to police station, nearby road side unit, the nearby ambulance. So that delay can be minimized and message can be transmitted in small time. The message sending is only in encrypted format and this encrypted message is send only to the 100 meter range vehicles by using omnidirectational antenna. This 100 meter range vehicles can decrypt the messages by using public key and private key and provide service to the accidental place. In this way we are providing security to the network. For security purposed we are using cryptography technique known as Elliptical Curve Digital Signature Authentication (ECDSA) technique. In this paper length of the transmitted message is short. In this paper, use Ad hoc On-demand Distance Vector (AODV) protocol for proper route founder.

2. LITERATURE SURVEY 2

Kyung-Ah Shim [1], Author suggested that they uses the Binary Authentication Tree method .But this method cannot provide the proper message authentication to the system. For that author use a new method called as conditional privacy preserving authentication scheme for vehicle to Infrastructure communication and this conditional privacy preserving authentication scheme was based on secure identity-based signature, aggregate signature scheme and binary authentication.

Attila Altay Yavuz [2], in this paper author implemented rapid authentication (RA) scheme. This rapid authentication scheme was suitable for time-critical authentication of command. This rapid authentication scheme can control the messages in large and distributed manner.

Neeraj Kumar and Jong-Hyouk Lee [3], Author suggested a new peer-to-peer (P2P) cooperative caching scheme to minimize the load on infrastructure. The traffic information among vehicles can be shared in a P2P manner using a Markov chain and this Markov chain would be divided in three states. The replacement of existing data to accommodate newly arriving data was achieved in a probabilistic manner.

Senthil Ganesh N., Ranjani S. [4], Author tell us about the various security thread of the VANET. They tell us different types of security thread like Black Hole Attack, Malware, Spamming, Selfish Driver, Malicious Attacker, Denial of Services, Masquerading, Global Positioning System (GPS) Spoofing, Pranksters, Sybil Attack, Timing Attack, etc.

Vinh Hoa LA, Ana CAVALLI [5], Author tell us about the various types of security attack and their solutions .The attack are Sybil Attack, Bogus Information and Bush telegraph, Impersonation Attack and Masquerade, Timing Attack, Global Positioning System (GPS) Spoofing, Hidden vehicles and tunnel attack, Illusion Attack, ID Disclosure, Denial of Service (DoS) and Distributed Denial of Service (DDos),etc and also provide the prevention technique related this attack.

Ankita Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh Pandey, Tumpa Roy [6], Author tell us about the how we provide security to the VANET. And how we preserve the VANET network from attack.

Greeshma Sarath, Devesh C Jinwala and Sankita Patel [7], Author tells us about the ECDSA and its variant.

Mehdi Khabazian, Sonia Aïss, Mustafa Mehmet-Ali, [8], Author suggested about the analytical model for the performance evaluation of safety message dissemination in vehicular ad hoc networks with two priority classes. Author consider the IEEE 802.11 broadcasting protocol and 2-D Markov modeling protocol. By considering this two protocol author derive the joint distribution of the numbers and low-priority periodic messages which are in transmission mode and back off process in highway.

Josiane Nzouonta, Neeraj Rajgure, Guiling Wang and Cristian Borcea,[9], Author implemented a reactive protocol called as RBVT-R and proactive protocol called as RBVT-P. And all these protocols compared with MANET representative protocols such as AODV, OLSR, GPSR and protocols representative of VANETs (GSR)

Rongxing Lu, Xiaodong Li, Haojin Zhu, Xuemin (Sherman)Shen [10], all these authors proposed a new smart parking scheme for large parking lots through vehicular communication. The proposed scheme can provide the drivers for real-time parking navigation services, intelligent anti-theft protection and friendly parking information dissemination.

Ahmad Yusri Dak, Saadiah Yahya, Murizah Kassim[11],the author proposed a various security services that can secure the network from the attack. This paper provides the various security issues such as confidentiality, authenticity, integrity, availability and non-repudiation and this security issues have aim to secure communication between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I).

K.Susitra, S.Lakshmi Narasimman[12], the author provides the various authentication technique to improve the efficiency in the transport system communication. In this paper author provides the various algorithms that can be used in the vanet and their features scopes.

Rukaiya Shaikh, Disha Deotale[13],In this paper author tell us about the survey on various cryptographic algorithms for examples RSA, Elliptic Curve Cryptography, and Message Digest 5(MD5) with their pros and cons. They provide better security and privacy if we use combination of this algorithm.

K.Sivarama Krishna, Ms.Ch.Vijaya Durga[14], In this paper the author uses a routing protocol i.e AODV which allow the user to generate the real world mobility model for VANET simulations. In this paper author uses some tools which are Ns-2, MOVE and SUMO. MOVE is a tool for open source traffic simulator and the output of MOVE is the real world mobility model. The broadcasting of the MOVE simulator can be done by using NS-2 simulator.

Aqeel Khalique Kuldip Singh Sandeep Sood [15].In this paper, authors tells us about implementation of ECDSA and their security services.

Michael Behrisch, Laura Bieker, Jakob Erdmann, Daniel Krajzewicz[16].the author provides the idea about the SUMO and its implenmentation.

3. VANET SIMULATOR

3.1 Sumo

In VANET, there are various types of stimulator should be found such as SUMO, NS-2, OMNET, OMNET++, TRANSIMS, MatSim etc . But in this paper, we are using a SUMO stimulator. The SUMO is the latest version of the VANET stimulator network. SUMO is Simulation of Urban Mobility. SUMO can be a traffic simulation package. It means SUMO is use to simulate network of a city's size, but it can be use for smaller and larger network. SUMO can be a microscopic, space-continuous road traffic simulation. In future SUMO would be extended to be multi-modal. SUMO can provide traffic simulation. SUMO can also provide the facility of infrastructure changes as well as policy changes before implementing them on the road. In SUMO, the effect of the atmosphere or traffic light control algorithms could be tested and optimized in the simulation before being deployed in the real world.

Simulation of urban mobility is large simulation framework and open GL GUI base open source which is free and open traffic simulation. SUMO can allow intermodal traffic systems such as road side vehicles, public transport and pedestrians. SUMO can also provide supporting tools which can handle the various tasks such as route finding, visualization, network import and emission calculations. SUMO could enhance with custom models and provides various APIs to remotely control the simulation. The features of SUMO such as,

1) Multimodal traffic simulation such as vehicles, pedestrians.
2) Network size and simulated vehicles are not limited.
3) SUMO can be implemented in C++ and use portable libraries.
4) Online interaction – online interaction can be control with TraCI.
5) Microscopic simulation–for vehicles, pedestrians and public transport could be modeled explicitly.
6) Support import format such as VISUM, VISSIM, NavTeq, openstreetmap.
7) Traffic lights time schedule could be imported or generated automatically in SUMO.

SUMO support characteristics are as follow
1) Traffic Light Algorithms.
2) Vehicular Communications.
3) Evaluation of Traffic Surveillance Systems.
4) Route Choice and Dynamic Navigation.

3.2 TraCI

TraCI should be "Traffic Control Interface". TraCi give access to a running road traffic simulation, it allows to retrieve value of simulated objects and to manipulate their behavior "on-line". TraCI is communication link between the road traffic and network stimulator. TraCI can provide control over the behavior of the vehicle during simulation runtime and understands the influences of VANET application on traffic pattern. TraCI is an open source architecture which can couple two stimulators that are road traffic and network stimulator. The vehicular traffic and network stimulator would be connected in real time by using TraCI. Thus they enabling the control of mobility attributes of each stimulated vehicles. Thus the movement of each vehicle and its simulation can be shown in VANET and TraCI respectively. In such simulation setup and mobility pattern cannot be fixed.

4. CRYPOGRAPHY TECHNIQUE

4.1 Elliptic Curve Digital Signature Algorithum:

Elliptical Curve Cryptography (ECC) can be a public key encryption technique and it was based on elliptic curve theory that could be used to create faster, smaller and more efficient cryptography kyes.ECC can generate key by using the properties of the Elliptical Curve equation instead of traditional method of generation of the product of very large prime number. This technology would be used in conjunction with most public key encryption method such as RSA, Diffie-Hellman. Elliptical Curve Cryptography can provide the security level up to the 164 bit keys and other system require 1024 bit to achieve the security.

The Elliptic Curve Digital Signature Algorithm has the elliptic curve variant of the Digital Signature Algorithm. ECDSA provide more strong a cryptographically generate digital signatures. This digital signature can use in to solve the problem of elliptic curve discrete logarithmic algorithm. ECDSA can use smaller numbers 160/256 bits instead of 1024/2048 bits in RSA, DSA and provide the security up to the same level. The ECDSA was accepted in 1999 by an ANSI standard, and it was also accepted in 2000 by IEEE and NIST standards. It was accepted in 1998 by an ISO standard. The strength per key bit in elliptic curves is significantly greater because in elliptic curve there are discrete logarithm problems and also there are no sub exponential-time algorithms. Elliptic Curve Digital Signature Algorithm is an elliptic curve analogue of the DSA. Digital Signature scheme can use the following basic cryptography services:

- Data integrity.
- Data origin authentication
- Non repudiation

Elliptic curve digital signature algorithm consists of 3 phases: 1. Key generation, 2. Signature generation, 3.Signature verification. To generate the domain parameters a setup phase has to execute before the key generation phase. Domain parameters for an elliptic curve described an elliptic curve E, finite field Fp, and base point g ∈ E (Fp) (generator) with order n. The parameters should be chosen carefully so that ECDLP is resistant to all known attacks. The elliptic curve is chosen in such a way that (a,b) ∈ (1, P) and substitute in equation. So the domain parameters would be defined as p, E (a, b), g, n.

- **Key pair generation by using ECDSA:**

Let A is the signatory for message M. sender A performs the following steps to generate a public and private key:
1. Select unique and unpredictable integer, d, in the interval [1, n-1].
2. Compute Q = d*g. Where sender A's private key is d.
3. Sender A's public key is the combination of (E, g, n, Q).

- **Signature Generation by using ECDSA:**

By using sender A's private key, sender A generate signature for message M using the following steps:
(1) Select unique and unpredictable integer k in the interval [1, n-1]
(2) Compute k*g = (x1, y1) where x1 is an integer.
(3) Compute r = x1 mod n; If r = 0, then go to step 1.
(4) Compute h = H(M), where H is the SHA-512.
(5) Compute s = k-1(h + d*r) mod n; If s = 0, then go to step1.
(6) The signature of sender A for message M is the integer pair (r, s).

- **Signature Verification by using ECDSA:**

The receiver B can verify the authenticity of sender A's signature (r, s). For message M by performing the
Following operation:
(1)Obtain signature of sender A's public key (E, q, n, Q).
(2) Verify that values r and s are in the interval of [1,n-1]
(3) Compute w = s-1 (mod n).
(4) Compute h = H(M), where H is the secure hash algorithm used by sender A.
(5) Compute u1 = h*w (mod n).
(6) Compute u2 = r*w (mod n).
(7) Compute u1*g + u2*Q = (x0, y0)
(8) Compute v = x0(mod n).
(9) The signature for message M is verified if and only if v = r

- **Security of ECDSA:**

Public key was generated by computing the point Q, where Q = d*g. In order to crack the elliptic curve key, attackers have to generate the secret key d when Q and g are provided. The order of the Elliptic curve, E is any prime number (n), then computing d given d*g and g would take roughly 2*n=2 operations. For example, if the key length n is 192 bits, then attacker will be required to perform about 296 operations. If attacker had a super computer and perform one billion operations per second, it would take around two and half trillion years to find the secret key. This is the elliptic curve discrete logarithm problem behind ECDSA. The curve parameter chosen so carefully to secure elliptic curve from various well known attacks like Pollard's rho and Pohlig- HellmaProof of ECDSA signature Scheme. Signature send by A to B is (r, s) and s could be generated only by sender A because only sender A knows about its private key d. s = k-1(h + dr) mod n on rearranging
1. K = s-1 (h + dr).
2. K*g = s-1 *(h + dr)*g.
3. K*g = (s-1)h*g +(s-1)d*r*g.
4. r = h*w*g + r*w*d*g.
5. r = u1*g + u2*Q.

- **A Possible Attacks on ECDSA:**

The secret key k used for signing two or more messages and would be generated independently. In particular, a different secret key k could be used for signing different messages otherwise the private key d could be recovered. If a secure random or pseudo-random number generator could be used, then the chance of generating a repeated key k value is negligible. If same secret key (k) can use to generate signature of two different messages m1 and m2 then it will result in two signatures (r,s1) and (r, s2).
1.s1 = k-1(h1 + d*r)
2.s2 = k-1(h2 + dr) ; where h1 = SHA512 (m1) and SHA512 (m2).
3.ks1- ks2 = h1+dr-h2-dr
4.k = (h1-h2)/(s1-s2)
5.d = (k *s-h)/r

5. ROUTING PROTOCOL

To find the proper path and calculate the specified distance, routing algorithm is play a very important role. For this purposed we are using here the AODV routing algorithm.

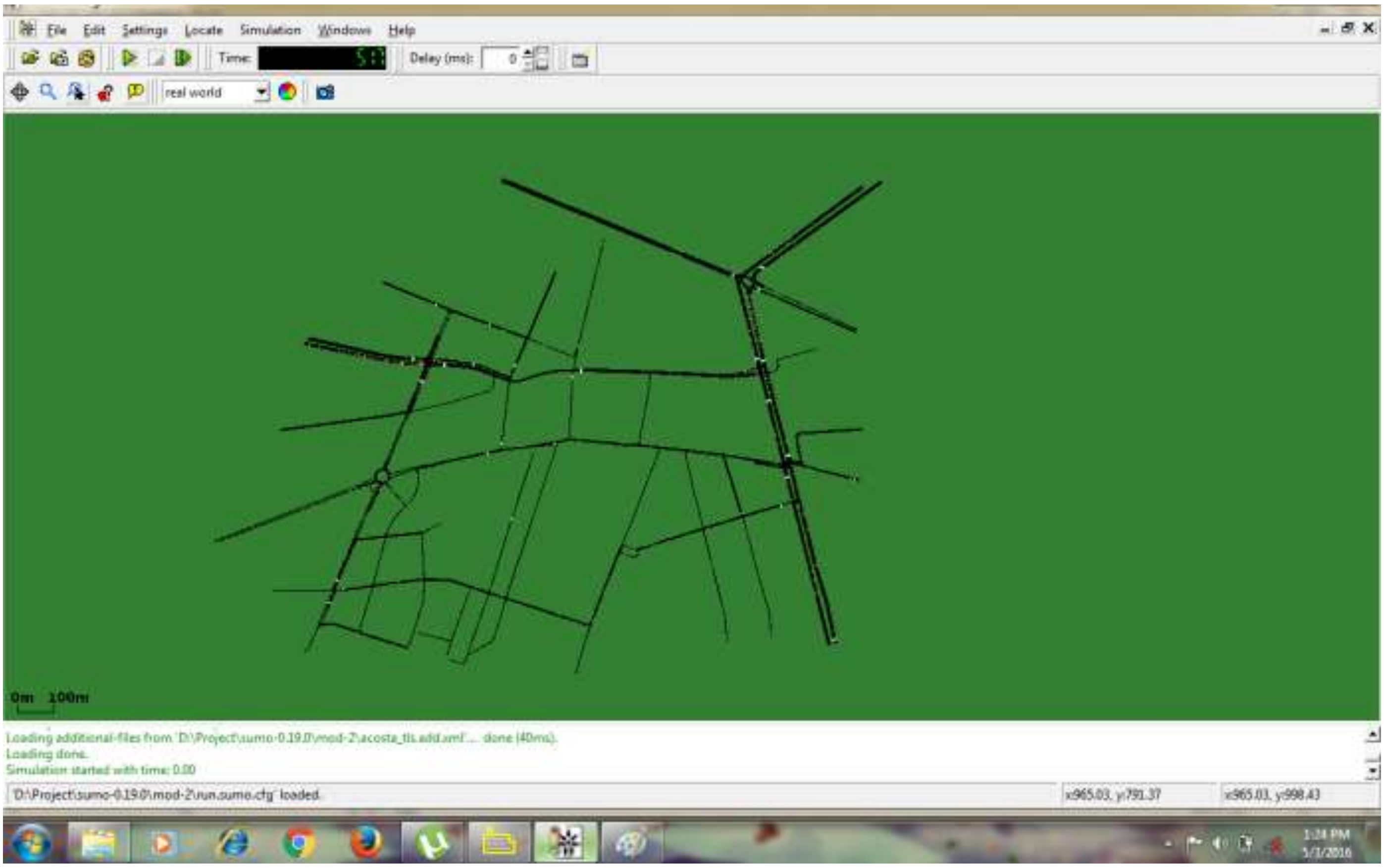
5.1 Aodv Routing Protocol:

Ad hoc On-demand Distance Vector (AODV) should be working as on demand routing algorithm. It was also called as the reactive routing algorithm. AODV protocol find route on demand by flooding the network with Route Request packets. AODV protocol combine some of the property of both Dynamic Source Routing and Destination sequence Distance Vector Routing protocols with significant differences. AODV is a reactive protocol. AODV protocol has a routing table and this routing table arrange properly. The reactive routing protocols do not update routing table periodically. When every node at the destination receives the control packet then the routing table updated periodically. The AODV routing protocol is developing in such way, it will work properly in ad hoc mobile networks. In AODV when sender node sends a packet to the destination node then this packet contains only destinations address. This is the difference between AODV and other routing protocols. The AODV protocol will be specially working in on demand condition. AODV protocol is capable of handling both unicast and multicast routing. The main advantage of AODV protocol is a loop free and self starting. The AODV protocol develops route by using two routers, one for route request and one for route reply. AODV protocol was attempted to improve the performance of DSR by maintaining the routing tables in such a way that the data packets will not contain the routes of the network. AODV routing protocol can be chosen on demand to find the route of the network.

6. PHASE 1

In phase 1, our aim is to develop the vehicular routes, vehicles and signals. But these vehicles are not in moving condition. For that we are using SUMO simulator. SUMO is the simple and advance VANET simulator. In that we are developing the route by using the AODV routing protocol. This route can be made by doing some java based programming in the SUMO.

In that vehicles have its unique id. It means it unique id has been separated from each other. In this project vehicles can be distinguish by their vehicle name_number_number. For example Togliatti_11_1971, Vittorio_Veneto_2_702, XXI_Aprile_7_982,etc. For simulation purposed we are taken 1000 vehicles. The main feature of the SUMO is that, it does not allow the duplication of the vehicles. For this reason, in SUMO vehicles have the unique id and this id cannot be duplicated.



Loading additional-files from 'D:\Project\sumo-0.19.0\mod-2\acosta_tls.add.xml' ... done (40ms).
Loading done.
Simulation started with time: 0.00

'D:\Project\sumo-0.19.0\mod-2\run.sumo.cfg' loaded.

x965.03, y791.37

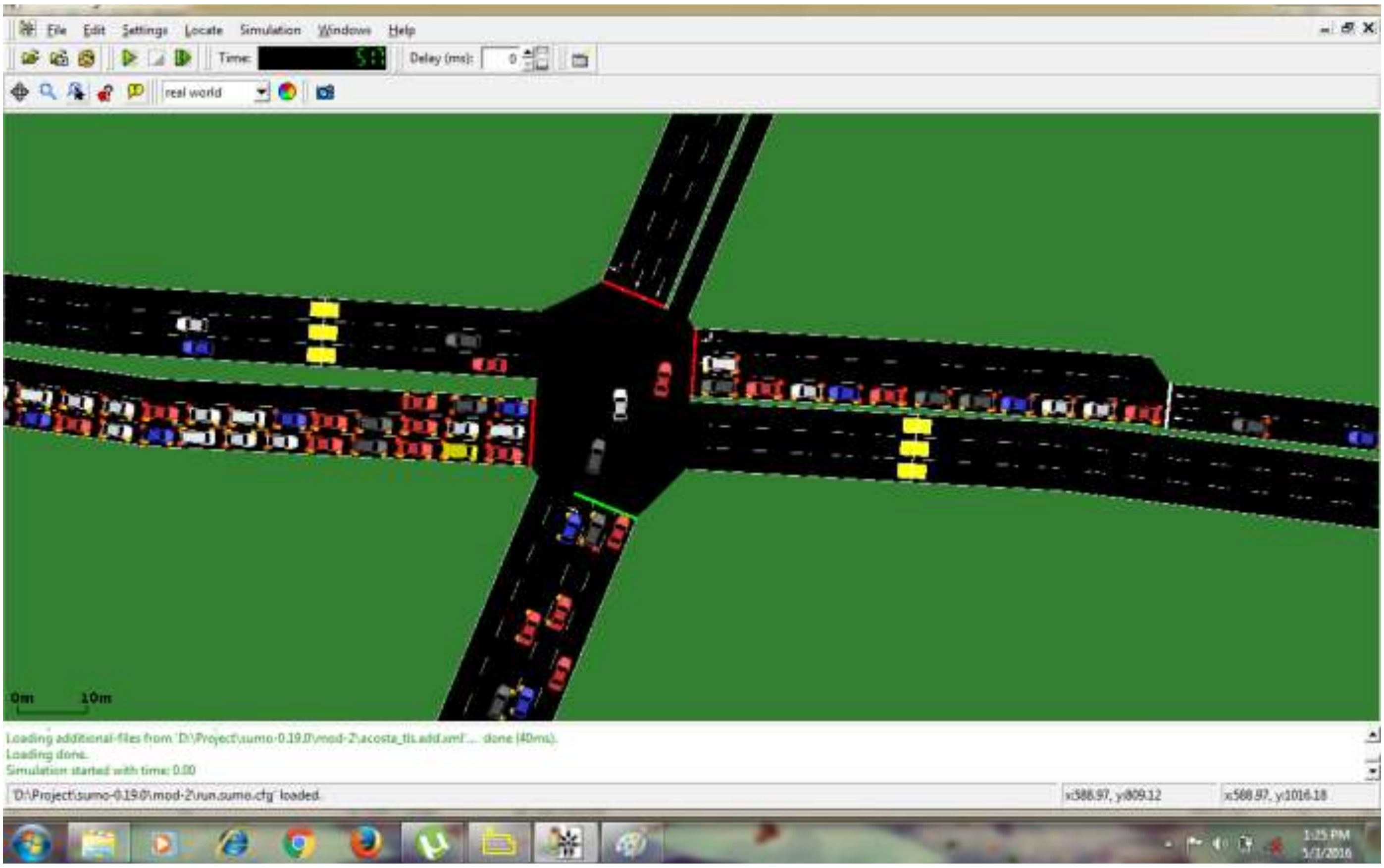
x965.03, y998.43

1:24 PM
5/1/2016

Fig 1- Discovery of vehicles route, vehicles and signals

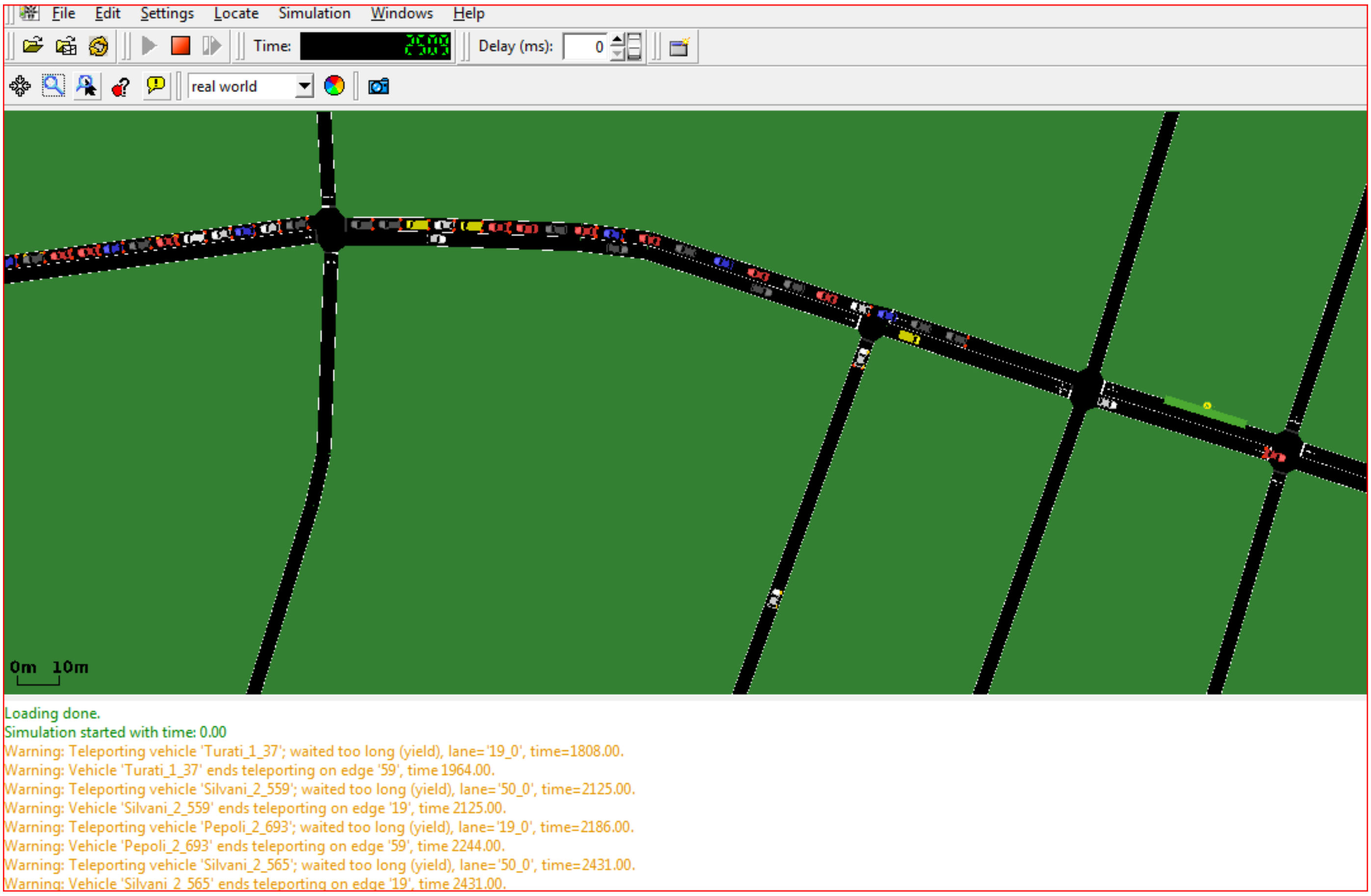
7. PHASE 2

In phase 2, our aim is to show vehicles are in running condition and vehicular communication in SUMO. It means that vehicles are communicated with each other by broadcasting the text message. But in SUMO only warning communications can be done and actual normal communication can be done in TraCI.



```
Loading additional-files from 'D:\Project\sumo-0.19.0\mod-2\acosta_tls.add.xml' ... done (40ms).
Loading done.
Simulation started with time: 0.00
'D:\Project\sumo-0.19.0\mod-2\run.sumo.cfg' loaded.    x:588.97, y:809.12    x:588.97, y:1016.18
```

Fig 2-Traffic signals and moving vehicles



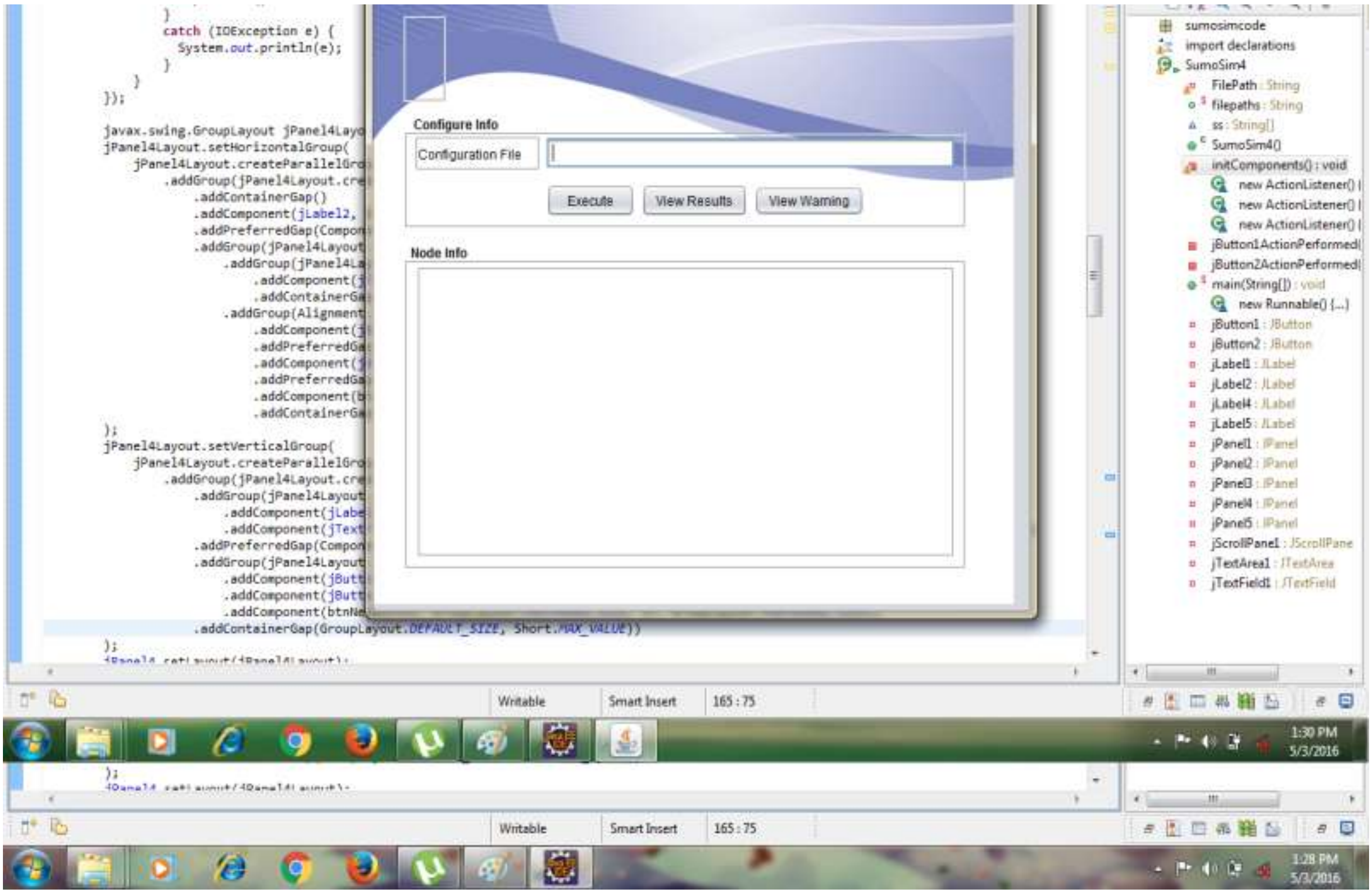
```
Loading done.
Simulation started with time: 0.00
Warning: Teleporting vehicle 'Turati_1_37'; waited too long (yield), lane='19_0', time=1808.00.
Warning: Vehicle 'Turati_1_37' ends teleporting on edge '59', time 1964.00.
Warning: Teleporting vehicle 'Silvani_2_559'; waited too long (yield), lane='50_0', time=2125.00.
Warning: Vehicle 'Silvani_2_559' ends teleporting on edge '19', time 2125.00.
Warning: Teleporting vehicle 'Pepoli_2_693'; waited too long (yield), lane='19_0', time=2186.00.
Warning: Vehicle 'Pepoli_2_693' ends teleporting on edge '59', time 2244.00.
Warning: Teleporting vehicle 'Silvani_2_565'; waited too long (yield), lane='50_0', time=2431.00.
Warning: Vehicle 'Silvani_2_565' ends teleporting on edge '19', time 2431.00.
```

Fig 3-Running condition of the vehicles and their broadcasting.

8. PHASE 3

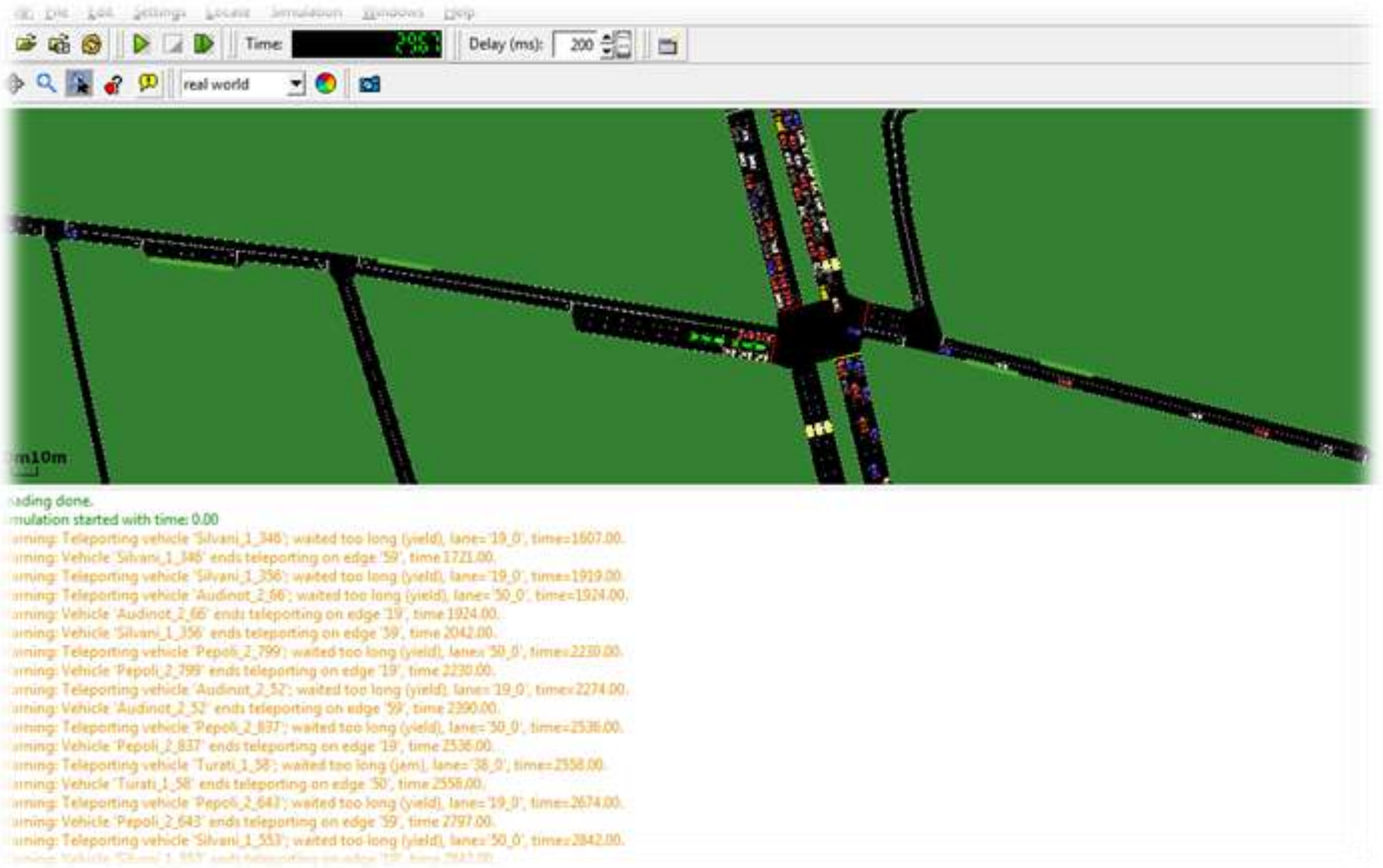
In phase 3, our aim is to controlling of SUMO by TraCI. It means that, in SUMO we can show the only warning messages broadcasting by the vehicles, but their actual communication can be done in TraCI. TraCI can control the vehicular activity in SUMO. For that TraCI can generate a normal communication and this communication can be shown n SUMO. For that reason, in TraCI messages can be divided into 3 types. And these types are 1) 15 byte message – it means vehicles can be communicated normally. They can establish their connection with each other by sending a simple text message with each other.2) 47 byte message – this 47 byte message can show the vehicle connection can be established properly. And vehicles can be communicated properly by sending and receiving the acknowledgement.3) 128 byte message – this 128 byte message shows the warning messages. Supposed to be considering in some area road accident will be occur and there is long traffic jam. Then at this time vehicle can broadcast the jamming/warning message to his back vehicle. And this vehicle can broadcast this message in his 100 meter range network. For this, warning message can be reach to vehicle and jamming cannot be occurs. For broadcasting purposed omnidirectional antenna will be used. This antenna will cover the proper direction of message broadcasting. For that bandwidth utilization is minimized. This antenna can be covered the direction at an angle 45°.So for that message will be broadcast at proper direction.

When vehicle can come under the OBU network area .Then vehicles can be self authentic. It means vehicles can be registered itself in the base station. This authentication can be transparent and pure. And then base station provides the originality of this vehicle. And this vehicle cannot have duplicated id



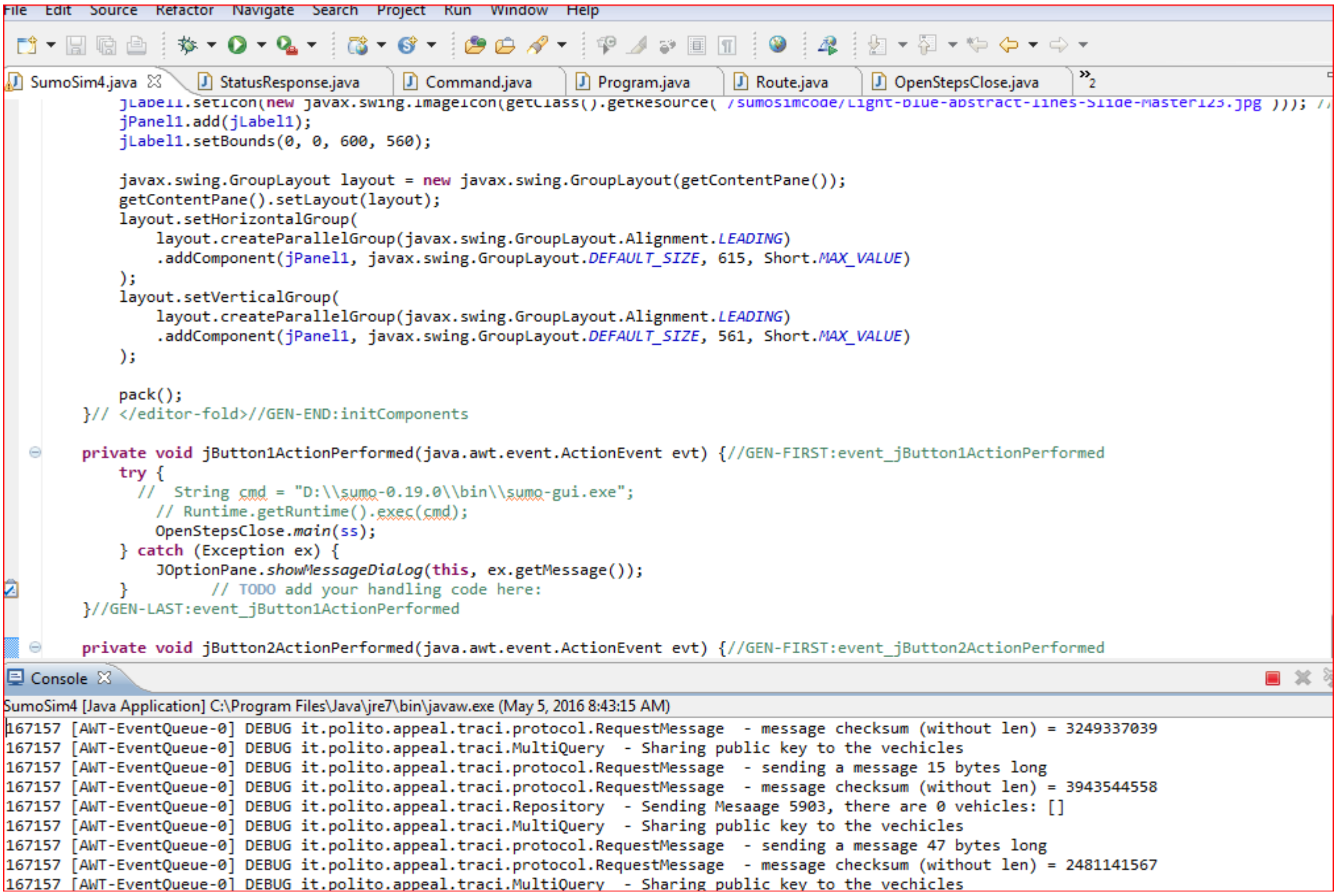
```
            }
            catch (IOException e) {
              System.out.println(e);
            }
        }
    });

    javax.swing.GroupLayout jPanel4Layo
    jPanel4Layout.setHorizontalGroup(
        jPanel4Layout.createParallelGro
            .addGroup(jPanel4Layout.cre
                .addContainerGap()
                .addComponent(jLabel2,
                .addPreferredGap(Compon
                .addGroup(jPanel4Layout
                    .addGroup(jPanel4La
                        .addComponent(j
                        .addContainerGa
                    .addGroup(Alignment
                        .addComponent(j
                        .addPreferredGa
                        .addComponent(j
                        .addPreferredGa
                        .addComponent(b
                        .addContainerGa
    );
    jPanel4Layout.setVerticalGroup(
        jPanel4Layout.createParallelGro
            .addGroup(jPanel4Layout.cre
                .addGroup(jPanel4Layout
                    .addComponent(jLabe
                    .addComponent(jText
                .addPreferredGap(Compon
                .addGroup(jPanel4Layout
                    .addComponent(jButt
                    .addComponent(jButt
                    .addComponent(btnNe
                .addContainerGap(GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE))
    );
```

Fig 4- Execution of TraCI



```
ading done.
mulation started with time: 0.00
arning: Teleporting vehicle 'Silvani_1_346'; waited too long (yield), lane='19_0', time=1607.00.
arning: Vehicle 'Silvani_1_346' ends teleporting on edge '59', time 1721.00.
arning: Teleporting vehicle 'Silvani_1_356'; waited too long (yield), lane='19_0', time=1919.00.
arning: Teleporting vehicle 'Audinot_2_66'; waited too long (yield), lane='50_0', time=1924.00.
arning: Vehicle 'Audinot_2_66' ends teleporting on edge '19', time 1924.00.
arning: Vehicle 'Silvani_1_356' ends teleporting on edge '59', time 2042.00.
arning: Teleporting vehicle 'Pepoli_2_799'; waited too long (yield), lane='50_0', time=2230.00.
arning: Vehicle 'Pepoli_2_799' ends teleporting on edge '19', time 2230.00.
arning: Teleporting vehicle 'Audinot_2_52'; waited too long (yield), lane='19_0', time=2274.00.
arning: Vehicle 'Audinot_2_52' ends teleporting on edge '59', time 2390.00.
arning: Teleporting vehicle 'Pepoli_2_837'; waited too long (yield), lane='50_0', time=2536.00.
arning: Vehicle 'Pepoli_2_837' ends teleporting on edge '19', time 2536.00.
arning: Teleporting vehicle 'Turati_1_58'; waited too long (jam), lane='38_0', time=2558.00.
arning: Vehicle 'Turati_1_58' ends teleporting on edge '50', time 2558.00.
arning: Teleporting vehicle 'Pepoli_2_643'; waited too long (yield), lane='19_0', time=2674.00.
arning: Vehicle 'Pepoli_2_643' ends teleporting on edge '59', time 2797.00.
arning: Teleporting vehicle 'Silvani_1_553'; waited too long (yield), lane='50_0', time=2842.00.
arning: Vehicle 'Silvani_1_553' ends teleporting on edge '19', time [illegible]
```

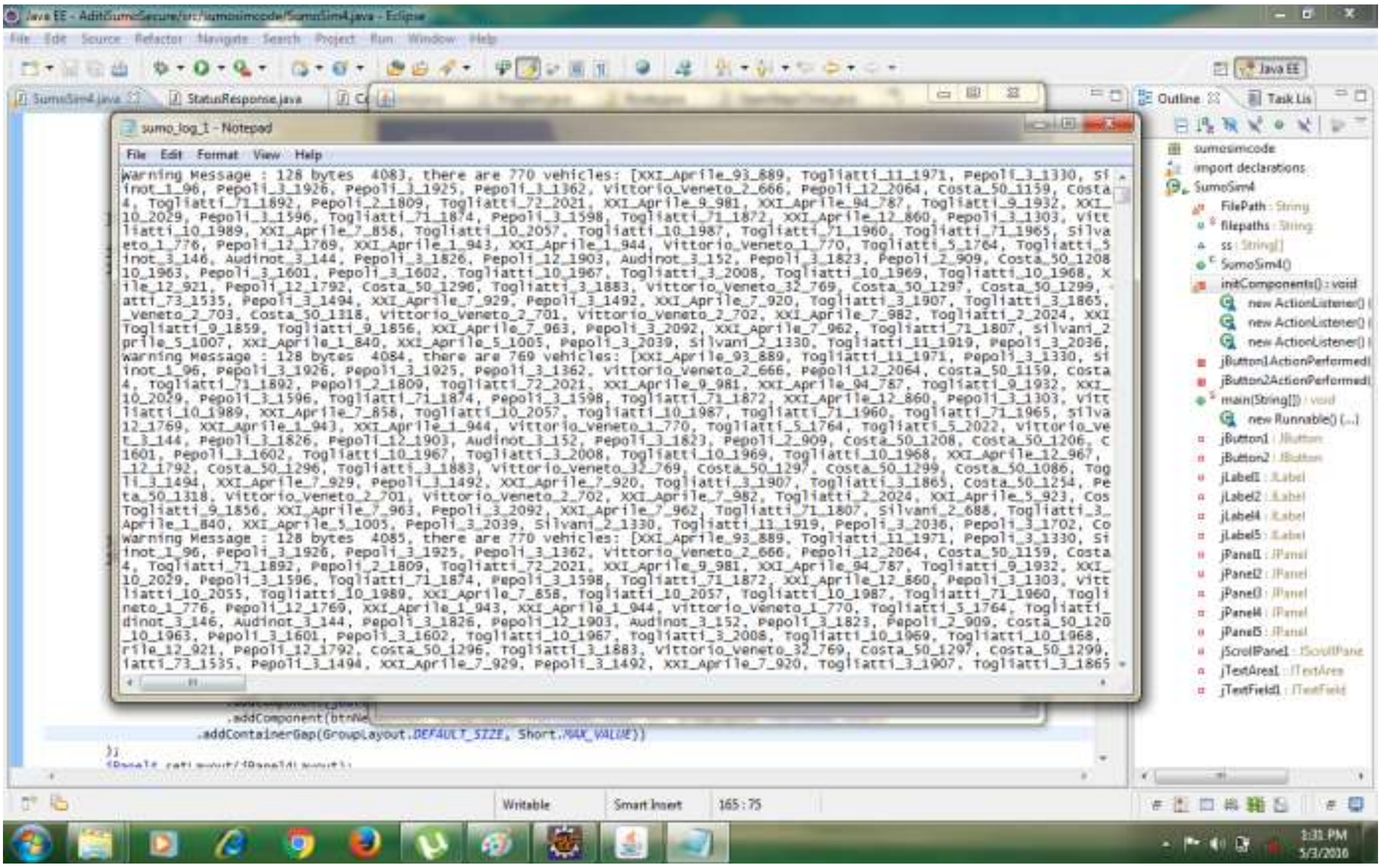
Fig 5-Vehicular communications in SUMO



```
        jLabel1.setIcon(new javax.swing.ImageIcon(getClass().getResource("/sumosimcode/Light-blue-abstract-lines-Slide-Master123.jpg"))); //
        jPanel1.add(jLabel1);
        jLabel1.setBounds(0, 0, 600, 560);

        javax.swing.GroupLayout layout = new javax.swing.GroupLayout(getContentPane());
        getContentPane().setLayout(layout);
        layout.setHorizontalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE, 615, Short.MAX_VALUE)
        );
        layout.setVerticalGroup(
            layout.createParallelGroup(javax.swing.GroupLayout.Alignment.LEADING)
            .addComponent(jPanel1, javax.swing.GroupLayout.DEFAULT_SIZE, 561, Short.MAX_VALUE)
        );

        pack();
    }// </editor-fold>//GEN-END:initComponents

    private void jButton1ActionPerformed(java.awt.event.ActionEvent evt) {//GEN-FIRST:event_jButton1ActionPerformed
        try {
          //  String cmd = "D:\\sumo-0.19.0\\bin\\sumo-gui.exe";
            // Runtime.getRuntime().exec(cmd);
            OpenStepsClose.main(ss);
        } catch (Exception ex) {
            JOptionPane.showMessageDialog(this, ex.getMessage());
        }          // TODO add your handling code here:
    }//GEN-LAST:event_jButton1ActionPerformed

    private void jButton2ActionPerformed(java.awt.event.ActionEvent evt) {//GEN-FIRST:event_jButton2ActionPerformed
```

```
SumoSim4 [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (May 5, 2016 8:43:15 AM)
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.protocol.RequestMessage  - message checksum (without len) = 3249337039
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.MultiQuery  - Sharing public key to the vechicles
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.protocol.RequestMessage  - sending a message 15 bytes long
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.protocol.RequestMessage  - message checksum (without len) = 3943544558
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.Repository  - Sending Mesaage 5903, there are 0 vehicles: []
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.MultiQuery  - Sharing public key to the vechicles
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.protocol.RequestMessage  - sending a message 47 bytes long
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.protocol.RequestMessage  - message checksum (without len) = 2481141567
167157 [AWT-EventQueue-0] DEBUG it.polito.appeal.traci.MultiQuery  - Sharing public key to the vechicles
```

Fig 6- Controlling over vehicular communication in TraCI


Java EE - AditSumoSecure/src/sumosimcode/SumoSim4.java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help
SumoSim4.java
StatusResponse.java
sumo_log_1 - Notepad
File Edit Format View Help
Outline
Task List
sumosimcode
import declarations
SumoSim4
Writable
Smart Insert
165 : 75
1:31 PM
5/3/2016

```
warning Message : 128 bytes  4083, there are 770 vehicles: [XXI_Aprile_93_889, Togliatti_11_1971, Pepoli_3_1330, Si
inot_1_96, Pepoli_3_1926, Pepoli_3_1925, Pepoli_3_1362, Vittorio_Veneto_2_666, Pepoli_12_2064, Costa_50_1159, Costa
4, Togliatti_71_1892, Pepoli_2_1809, Togliatti_72_2021, XXI_Aprile_9_981, XXI_Aprile_94_787, Togliatti_9_1932, XXI_
10_2029, Pepoli_3_1596, Togliatti_71_1874, Pepoli_3_1598, Togliatti_71_1872, XXI_Aprile_12_860, Pepoli_3_1303, Vitt
liatti_10_1989, XXI_Aprile_7_858, Togliatti_10_2057, Togliatti_10_1987, Togliatti_71_1960, Togliatti_71_1965, Silva
eto_1_776, Pepoli_12_1769, XXI_Aprile_1_943, XXI_Aprile_1_944, Vittorio_Veneto_1_770, Togliatti_5_1764, Togliatti_5
inot_3_146, Audinot_3_144, Pepoli_3_1826, Pepoli_12_1903, Audinot_3_152, Pepoli_3_1823, Pepoli_2_909, Costa_50_1208
10_1963, Pepoli_3_1601, Pepoli_3_1602, Togliatti_10_1967, Togliatti_3_2008, Togliatti_10_1969, Togliatti_10_1968, X
ile_12_921, Pepoli_12_1792, Costa_50_1296, Togliatti_3_1883, Vittorio_Veneto_32_769, Costa_50_1297, Costa_50_1299,
atti_73_1535, Pepoli_3_1494, XXI_Aprile_7_929, Pepoli_3_1492, XXI_Aprile_7_920, Togliatti_3_1907, Togliatti_3_1865,
_Veneto_2_703, Costa_50_1318, Vittorio_Veneto_2_701, Vittorio_Veneto_2_702, XXI_Aprile_7_982, Togliatti_2_2024, XXI
Togliatti_9_1859, Togliatti_9_1856, XXI_Aprile_7_963, Pepoli_3_2092, XXI_Aprile_7_962, Togliatti_71_1807, Silvani_2
prile_5_1007, XXI_Aprile_1_840, XXI_Aprile_5_1005, Pepoli_3_2039, Silvani_2_1330, Togliatti_11_1919, Pepoli_3_2036,
warning Message : 128 bytes  4084, there are 769 vehicles: [XXI_Aprile_93_889, Togliatti_11_1971, Pepoli_3_1330, Si
inot_1_96, Pepoli_3_1926, Pepoli_3_1925, Pepoli_3_1362, Vittorio_Veneto_2_666, Pepoli_12_2064, Costa_50_1159, Costa
4, Togliatti_71_1892, Pepoli_2_1809, Togliatti_72_2021, XXI_Aprile_9_981, XXI_Aprile_94_787, Togliatti_9_1932, XXI_
10_2029, Pepoli_3_1596, Togliatti_71_1874, Pepoli_3_1598, Togliatti_71_1872, XXI_Aprile_12_860, Pepoli_3_1303, Vitt
liatti_10_1989, XXI_Aprile_7_858, Togliatti_10_2057, Togliatti_10_1987, Togliatti_71_1960, Togliatti_71_1965, Silva
12_1769, XXI_Aprile_1_943, XXI_Aprile_1_944, Vittorio_Veneto_1_770, Togliatti_5_1764, Togliatti_5_2022, Vittorio_Ve
t_3_144, Pepoli_3_1826, Pepoli_12_1903, Audinot_3_152, Pepoli_3_1823, Pepoli_2_909, Costa_50_1208, Costa_50_1206, C
1601, Pepoli_3_1602, Togliatti_10_1967, Togliatti_3_2008, Togliatti_10_1969, Togliatti_10_1968, XXI_Aprile_12_967,
_12_1792, Costa_50_1296, Togliatti_3_1883, Vittorio_Veneto_32_769, Costa_50_1297, Costa_50_1299, Costa_50_1086, Tog
li_3_1494, XXI_Aprile_7_929, Pepoli_3_1492, XXI_Aprile_7_920, Togliatti_3_1907, Togliatti_3_1865, Costa_50_1254, Pe
ta_50_1318, Vittorio_Veneto_2_701, Vittorio_Veneto_2_702, XXI_Aprile_7_982, Togliatti_2_2024, XXI_Aprile_5_923, Cos
Togliatti_9_1856, XXI_Aprile_7_963, Pepoli_3_2092, XXI_Aprile_7_962, Togliatti_71_1807, Silvani_2_688, Togliatti_3_
Aprile_1_840, XXI_Aprile_5_1005, Pepoli_3_2039, Silvani_2_1330, Togliatti_11_1919, Pepoli_3_2036, Pepoli_3_1702, Co
warning Message : 128 bytes  4085, there are 770 vehicles: [XXI_Aprile_93_889, Togliatti_11_1971, Pepoli_3_1330, Si
inot_1_96, Pepoli_3_1926, Pepoli_3_1925, Pepoli_3_1362, Vittorio_Veneto_2_666, Pepoli_12_2064, Costa_50_1159, Costa
4, Togliatti_71_1892, Pepoli_2_1809, Togliatti_72_2021, XXI_Aprile_9_981, XXI_Aprile_94_787, Togliatti_9_1932, XXI_
10_2029, Pepoli_3_1596, Togliatti_71_1874, Pepoli_3_1598, Togliatti_71_1872, XXI_Aprile_12_860, Pepoli_3_1303, Vitt
liatti_10_2055, Togliatti_10_1989, XXI_Aprile_7_858, Togliatti_10_2057, Togliatti_10_1987, Togliatti_71_1960, Togli
neto_1_776, Pepoli_12_1769, XXI_Aprile_1_943, XXI_Aprile_1_944, Vittorio_Veneto_1_770, Togliatti_5_1764, Togliatti_
dinot_3_146, Audinot_3_144, Pepoli_3_1826, Pepoli_12_1903, Audinot_3_152, Pepoli_3_1823, Pepoli_2_909, Costa_50_120
_10_1963, Pepoli_3_1601, Pepoli_3_1602, Togliatti_10_1967, Togliatti_3_2008, Togliatti_10_1969, Togliatti_10_1968,
rile_12_921, Pepoli_12_1792, Costa_50_1296, Togliatti_3_1883, Vittorio_Veneto_32_769, Costa_50_1297, Costa_50_1299,
iatti_73_1535, Pepoli_3_1494, XXI_Aprile_7_929, Pepoli_3_1492, XXI_Aprile_7_920, Togliatti_3_1907, Togliatti_3_1865
```

```
                .addComponent(btnNe
            .addContainerGap(GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE))
);
```

Fig7– Output of warning messages can be generated by TraCI in SUMO

CONCLISION

In this paper, we can see the how the communication is possible in SUMO. And SUMO activity can be controlled by TraCI. In phase 1 we can see the route formation. In phase 2 we see the vehicular communication and in phase 3, controlling by TraCI on SUMO activity. Also we can see the cryptography technique and routing algorithm used in this paper.

REFERENCE

[1]. Kyung-Ah Shim “Reconstruction of a Secure Authentication Scheme for Vehicular Ad Hoc Networks Using a Binary Authentication Tree” IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 11, NOVEMBER 2013.

[2]. Attila Altay Yavuz “An Efficient Real-Time Broadcast Authentication Scheme for Command and Control Messages” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 10, OCTOBER 2014.

[3]. Neeraj Kumar and Jong-Hyouk Lee “Peer-to-Peer Cooperative Caching for Data Dissemination in Urban Vehicular Communications” IEEE SYSTEMS JOURNAL, VOL. 8, NO. 4, DECEMBER 2014.

[4]. Senthil Ganesh N. Ranjani S. “Security Threats on Vehicular Ad Hoc Networks (VANET)” International Journal of Electronics Communication and Computer Engineering Volume 4, Issue (6)NCRTCST-2013, ISSN 2249–071X.

[5]. Vinh Hoa LA, Ana CAVALLI “Security Attacks And Solutions in vehicular Ad-hoc network” International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April 2014.

[6]. [6].Agrawal, Aditi Garg, Niharika Chaudhiri, Shivanshu Gupta, Devesh Pandey, Tumpa Roy “ Security on Vehicular Ad Hoc Networks (VANET)” International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013).

[7]. Greeshma Sarath1 , Devesh C Jinwala2 and Sankita Patel,” A Survey On Elliptic Curve Digital Signature Algorithm And Its Variants” Dhinaharan Nagamalai et al. (Eds) : CSE, DBDM, CCNET, AIFL, SCOM, CICS, CSIP – 2014 pp. 121–136, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4411

[8]. Mehdi Khabazian, Member, IEEE, Sonia Aïssa, Senior Member, IEEE, and Mustafa Mehmet-Ali, Member, IEEE “Performance Modeling of Safety Messages Broadcast in Vehicular Ad Hoc Networks” IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 14, NO. 1, MARCH 2013.

[9]. Josiane Nzouonta, Neeraj Rajgure, Guiling Wang, Member, IEEE, and Cristian Borcea, Member, IEEE “VANET Routing on City Roads using Real-Time

Vehicular Traffic Information" December 14, 2007; revised July 24, 2008 and December 23, 2008. This work is supported in part by the National Science Foundation under Grants No. CNS-0520033, CNS-0834585, and CNS-0831753M.

[10]. Rashmi Raiya, Shubham Gandhi" Survey of Various Security Techniques in VANET" International Journal of Advanced Research in Computer Science and Software Engineering 4(6), June - 2014, pp. 431-433 Volume 4, Issue 6, June 2014 ISSN: 2277 128X.

[11]. Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim" A Literature Survey on Security Challenges in VANETs" International Journal of Computer Theory and Engineering, Vol. 4, No. 6, December 2012.

[12]. K.Susitra, S.Lakshmi Narasimman" A Survey on the Authentication Protocols in Vanet" K.Susitra ,INDIA / International Journal of Research and Computational Technology, Vol.7 Issue.1 ISSN: 0975-5662, March, 2015.

[13]. Rukaiya Shaikh, Disha Deotale" A Survey on VANET Security using ECC, RSA & MD5" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2015 Copyright to IJARCCE DOI 10.17148/IJARCCE.2015.4637 167.

[14]. K.SIVARAMAKRISHNA, Ms.CH.VIJAYA DURGA" Warning message dissemination in vanets using sumo and move" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015.

[15]. Aqeel Khalique Kuldip Singh Sandeep Sood" Implementation of Elliptic Curve Digital Signature Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 2 – No.2, May 2010

[16]. Michael Behrisch, Laura Bieker, Jakob Erdmann, Daniel Krajzewicz" SUMO – Simulation of Urban Mobility An Overview" IARIA, 2011. ISBN: 978-1-61208-169-4