ISSN 2319–7757
EISSN 2319–7765

Indian Journal of Engineering

Security Based Protocol Design for In-Vehicle Controller Area Network

Soumya Sukumaran[1], Neenu George[2]

1. Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamilnadu, India
2. Assistant Professor, ECE Department, Dhanalakshmi Srinivasan College of Engineering, Coimbatore, Tamilnadu, India

Publication History
Received: 20 February 2016
Accepted: 23 March 2016
Published: April-June 2016

Citation
Soumya Sukumaran, Neenu George. Security Based Protocol Design for In-Vehicle Controller Area Network. *Indian Journal of Engineering*, 2016, 13(32), 263-269

ABSTRACT

Vehicle networks which are currently connected to external networks permit conflicts to perform a long-range wireless attack using CAN susceptibilities. In this article shows that a long range of wireless attack is feasible using a real vehicle and a destructive Smartphone application in a connected car scenario. A security protocol is suggested for CAN as to plan in agreement with ongoing CAN requirements and also exhibits an active wireless attack using a real vehicle on a connected car scenario, in which a motorist's Smartphone is attached to the in-vehicle CAN. The attack examination involves two phases; they are preliminary and actual attack. In the preliminary phase, before initiating an actual attack, an attacker first attain a CAN data frame to impact control of the target vehicle using a diagnostic tool. The outcome shows that the suggested security protocol is more efficient than existing security protocols with reference to authentication delay and communication load.

Index Terms: Connected car, controller area network, In-vehicle network security, random key pre-distribution

Soumya Sukumaran and Neenu George,
Security Based Protocol Design for In-Vehicle Controller Area Network,
Indian Journal of Engineering, 2016, 13(32), 263-269,

I. INTRODUCTION

Vehicles of today have become gradually more dependent on software to handle their tasks. By launching wireless communications to vehicles, vehicular maintenance can greatly be enhanced and many other new applications can also be promoted to the vehicles. Although, the vehicle are not plotted with security in mind. General resemble to securing the connected car and usefulness of this resemble is revealed in a vehicular diagnostic scenario. As the most delegate trademark in the in-vehicle network is CAN. CAN has developed to the most important quality in the in-vehicle network because it abnormally reduces, the most of the communication lines and has higher data transmission reliability. The information security is not been examined yet in the design of CAN. Every bit of information transmitted can be crucial to motorist safety. When the data's are transmitted using the BUS network, CAN does not examine the confidentiality and authentication of the CAN data frame and make a way for a destructive to easily hack the data or initiate a replay attack. The condition will become unfavorable when a vehicle is attached to automotive diagnostic tools.

In order to check the features of the ECUs throughout a diagnostic process, the tool transmits CAN data frames without encryption and authentication to impact control of the ECUs. All over 90 years of huge-production, the motorist automobile has developed static which has a single gasoline powered internal combustion engine with four wheels and the well-known user interface of steering wheel, throttle, gearshift, and brake. Although, in the past two decades mostly the control system have changed immediately. These days, automobile is no more a mechanical device, but includes too much number of computers. These computers synchronize and detect sensors, components and the motorist. Even, the typical luxury sedan now includes over 100 MB of binary code individual computer with Electronic Control Units (ECUs) in usual automotive in turn communicating over one or more shared internal network buses. The automotive industry has always thinks about the safety with crucial engineering affect. Many advanced software like anti- lock brake system, automatic gear system have been launched specifically for expanding the safety of the driver and passengers. Because of the improved use of computerized control there will be group of potential threats. Representing this issue, the attack surface for new automobiles is expanding rapidly as more artificial services and communications functions are blend into vehicles. In the United States, the Onboard Diagnostics (OBD-II) port are extensively used in all new advanced vehicles, produce direct and standard access to internal automotive networks.

The telematics systems joined the internal automotive subsystems with a remote command center by using wide area cellular connection. To examine the current condition and the feasibly growing tendency of threats conducted several empirical tests on recent automotive technology. Keeping an eye on the focus of automotive systems based on CAN bus technology, summarize the outcomes of four selected tests conducted on the control systems for the window lift, warning light and airbag control system as well as the central gateway. In extension, identify basic security faultiness abused in these tests and the potential expectation to the safety and to discuss features countermeasures for the future. Although, these have special specifications with respect to the essential hardware and general system pattern, so a complete realization cannot be imagined to be available in the next few years. Existing automotive IT technology have primary fault on the secureness. Detection technology and proactive IT-forensic measures are planned to support a data analysis in order to restore incidents inside the automotive IT system. Therefore, in the long run, difficult solutions will be needful to enhance the overall system security. This will assist as secure basis for huge amount of automotive IT security services.

2. EXISTING SYSTEM

For constructing a secure in-vehicle CAN, a variety of research projects have been conducted over the past ten years. European-funded projects, EVITA grown a hardware security module (HSM) for On-Board network security. HSMs may be classified into three types according to the field, in which they are used. Full hardware security module are suitable for Vehicular Networks (Inter or Intra). Medium hardware security module are suitable for Intra Vehicle Networks and light hardware security module are suitable for sensors and actuators. EVITA-HSM uses communication security architecture for vehicles. It consists of a truncated 32-bit MAC with limited data payload of CAN data frames. It is interpreted that a 32-bit MAC is secure from collision attacks due to the limited properties of in-vehicle network. In order to provide an in-vehicle CAN communication environment secure against a replay attack data authentication techniques are designed.CAN data frame does not provide a particular security architecture for communication protocol. A security technique is used for the IT environment which cannot be immediately applied to CAN because of its unique features such as a limited data payload.

3. PROPOSED SYSTEM

In a connected car environment a practical wireless attack using a real vehicle, in which a motorist's Smartphone is attached to the in-vehicle CAN which is shown in Fig 1. The attack experiment includes of two phases, they are preliminary and actual attack. In the preliminary phase, before organizing an actual attack, an attacker first obtain a CAN data frame to impact control of the target vehicle using a diagnostic tool and also plan a security protocol to cure the accountabilities of CAN. Identical model vehicles with the same arrangement of automotive electronic subsystems could be used. To obtain a CAN data frame to impact control of an ECU a diagnostic tool is used and it does not need to be joined to the target vehicle throughout an actual attack. The attacker also assembles a destructive self-diagnostic app that overspread up as a normal one and sync it onto application markets. Besides using

Soumya Sukumaran and Neenu George,
Security Based Protocol Design for In-Vehicle Controller Area Network,
Indian Journal of Engineering, 2016, 13(32), 263-269,

a self-diagnostic application such as "Torque," "Car Gauge Pro," and an OBD2 scan tool such as "EML327," "PLX Kiwi," a driver can detect CAN status information even during driving.

Once the driver of the designed vehicle downloads the malicious self-diagnostic app, the Smartphone is bound by the charge of the attacker. In the actual attack phase, implementing the infected Smartphone of the driver, a long range wireless attack is carried out. That is, the attacker can inject CAN data frames individually of its location through the Smartphone if mobile communication such as 3G, 4G, or LTE is feasible. The Smartphone does not require to the attacker. The attack model is only realizable when the driver downloads the destructive self-diagnostic app. The attack model is still a sensible attack scenario and would be empirical in leading car makers are combining to bring Android OS in vehicles and connected car service are growing at a great rate. A security protocol is used to rehabilitate the vulnerabilities of CAN. In real time data processing data encryption and authentication techniques are acclaimed in the in-vehicle CAN. The message authentication code (MAC) is used for making allocation for the restricted data payload of the CAN data frame. Key management techniques maintain secure connectivity between external device and the in-vehicle CAN. In order to enhance the presentation, a key pre-distribution scheme used that depends on probabilistic key sharing among nodes within the network. A key pre-distribution is the method of distribution of keys onto nodes before classification. Key pre-distribution schemes are numerous methods that have been expanded by academicians for a better services of management in wireless sensor networks. It has three phases and in the time of these phases, secret keys are originated, placed in sensor nodes, and each sensor nodes explores the area in its communication extent to find another node to communicate. Keys may be randomly and then the nodes firmly decide mutual connectivity. Random key pre-distribution is used because it delivers better resiliency and it have various variants.

3.1. Module Description

The connected car is getting much awareness as the next generation. Vehicle-IT convergence technology, the fast expansion of mobile communication technology and the expansion of the smart device and application service are raised. In a vehicle, a number of ECUs are fixed and attached within CAN. The portal may be splits into Web-based and Smartphone app-based services. Nowadays, with the high execution and widespread of mobile communication technologies, more connected car scenarios are using smartphones. In common, a connected car is a vehicle that is always assigned to external networks while driving.

The components of a connected car are electronic control units and an in-vehicle network, gateway to arrange the vehicle with numerous services and communication link to attach the vehicle and portal. CAN is a high-integrity serial data communication technology enlarged for systematic communication between automotive applications. CAN is a multi-master broadcast communication bus system based on sender ID which enables ECUs to communicate on a single or dual wire network. In order to minimize the complexity and cost of in-vehicle network wiring the automobile makers create use of CAN protocol. In the CAN protocol, each ECU forwards information to other ECUs using a data frame. A sender ECU forwards data frames that contains its own ID. Other ECUs restores the data frame choosy after identifying the ID of the sender ECU in the data frame. Conforming to the length of the ID field the CAN protocol is separated into two modes they are CAN2.0A and CAN2.0B.The CAN 2.0B give assistance to conflict with CAN 2.0A. CAN 2.0B data frame format has a 29-bit ID field partitioned into two parts Base ID field and Extended ID field.To adjust the message priority the ID field is used. The use of the18-bit Extended ID field is firmly decided by the IDE field. The data field has a maximum of 8 bytes and contains data to be forwarded from the sender ECU to others. The cyclic redundancy check (CRC) field is used for recognizing the error of the transferred data frame. In order to register IT technology to vehicles, it is certain to make use of a number of automotive application components.

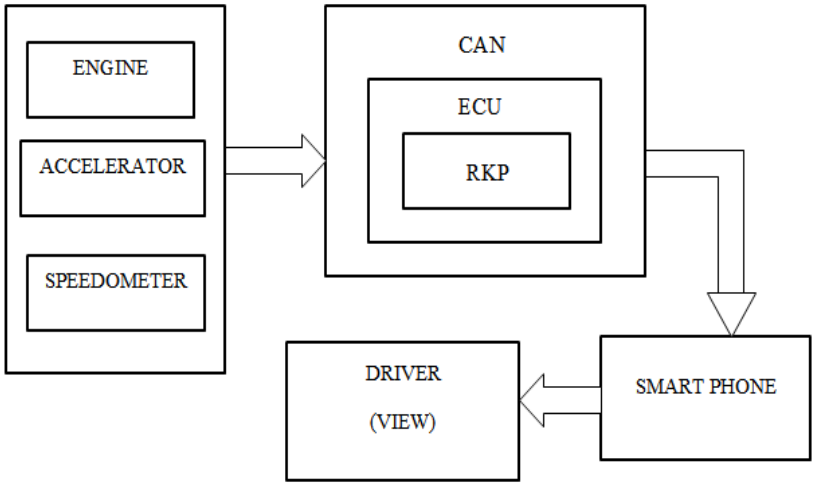

Figure 1 Block diagram

The electronic control unit (ECU) is the most vital component that controls one or more of the electrical systems and subsystems in a vehicle. In a motor vehicle one or more electrical systems or subsystems are controlled by the electronic control unit which is a generic term for any embedded system.

On-board architectures includes more than 70 ECUs that are interconnected with mixed communication networks such as the controller area network (CAN), local interconnect network (LIN). Electronic control unit consists of key elements like microcontroller, SRAM EEPROM Flash. It has inputs like digital inputs and analog inputs and outputs like relay drivers, H bridge drivers, Injector drivers, Logic outputs. For securing the real-time data processing in the in-vehicle CAN data encryption and authentication techniques are used. Key management techniques maintain secure connectivity between external device and the in-vehicle CAN. A MAC Protocol examines the restricted data payload of the CAN data frame. The key used in the protocol is used to attain secure data transmission and to plan secure and accurate security protocols which have a low-performance of an ECU and the restricted data payload of a CAN data frame. In order to produce confidentiality for a widespread data frame, it should be transmitted after encryption. In expansion, to verify a transmitted data frame, a MAC should be initiated and transmitted along with it and it is not easy to include a MAC in CAN data frame.

The CAN data frame includes of 120 bits, including a 64-bit data field. The total amount of CAN data frame transmission expands at least twice when the data field is used for a MAC where one data frame for the original data and at least one for a MAC. Such a technique is not proper since it will expand the CAN bus load at a great rate. A security protocol demands a well-organized data authentication technique that can be registered to the recent CAN data frame format. For secure communication, a CAN security protocol should offer a secure and fast key distribution mechanism for data frame encryption and authentication. In expansion, a well-organized and secure session key update protocol is demanded in order to improve the security of the session key and truncated MAC and it is also demanded to acquire the connectivity between an external device and a vehicle. MAC Key management is the technique of keys onto nodes before distribution. Therefore, the network uses their secret keys after delivery that is, when they reach their target position. The outcome is a communication network establishing in its own way, in accordance with the key pre-distribution scheme used in creation. Enhance the execution of the planned security protocol with an implementation of the encryption on hardware to boost the security technology. In order to explain the planned security protocol, first assumes the gateway and common ECUs pre-share and the long-term symmetric keys K and GK. Second assumption is, the loading of long-term symmetric keys is done through a secure channel.

Third assumption is, ECUs which use the message filtering functionality of CAN. Each ECU registers the ID of sender-ECU on its ID table, and each ECU gets a packet only if it has the sender ID registered on its ID table. For other packets, it shows filtering. The fourth assumption is, the sender and receiver ECUs organize data frames with a counter. When a data frame is completely transferred to the receiver, a data frame counter is incremented. Fifth assumption is, the gateway ECU has higher computing power than a common ECU. The last assumption is, a device certificate is loaded onto the gateway ECU and external devices. The planned security protocol is partitioned into five phases. Phases 1 and 2 use a well-organized security technique (Long term symmetric key and Authenticated Key Exchange Protocol 2 (AKEP2)) in order to implement an initial session key distribution. Symmetric keys loading phase is performed only when manufacturing a vehicle or changing an ECU. After starting a vehicle, every ECU functions an initial session key derivation process with GECU in a fixed order. The GECU derives the initial session keys with a particular ECU and other ECUs do not communicate but wait their turn. AKEP2 to implement a secure and well-organized key derivation process in the in-vehicle CAN scenario and it produces interactive entity authentication and absolute key distribution.

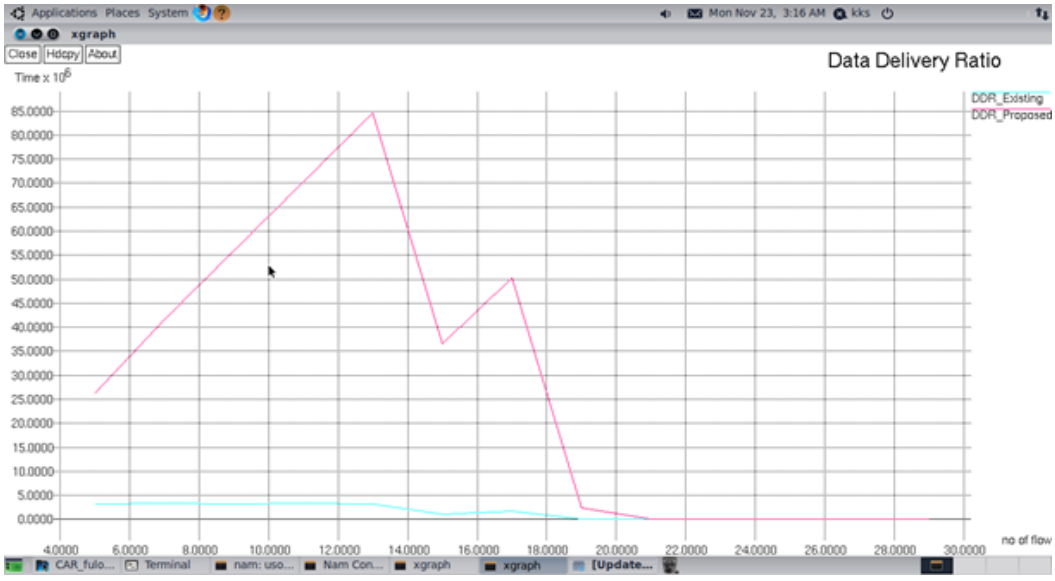

Figure 2 Data delivery ratio

4. RESULTS AND EVALUVATION

The suggested scheme is simulated on NS-2 and Ubuntu. The processing is performed in wireless sensor network domain. Using an Android Smartphone, can diagnose the vehicle problems. First the malicious app is assigned on the victim's Smartphone. The victim connect the Smartphone to the target vehicle using Bluetooth or Wi-Fi. The malicious app provides the victim with normal functions and it acts as a self-diagnostic app. The malicious app forwards the data frames of the in-vehicle CAN to the attacker's server using the Smartphone's mobile communication network. The attacker's server monitor the state of the target vehicle and transmitted a CAN data frame to impact control of an ECU to the in-vehicle CAN via the malicious app. The target vehicle had an actual fail caused by the unusual control data that was forwarded from the attacker's server. The simulation is implemented on NS-2. Firstly the reports are monitored and then forward to ECU. Then the reports are forwarded to CAN and then to APP. The APP receive the reports and thus outcomes are feed on Smartphone.

The data delivery ratio is 99.3566%. The performance of the dynamic source routing protocol has gradually increased. The Fig 2.shows time Vs number of flow of data packets. The performance of current data delivery ratio is very low compared to the newly designed one.

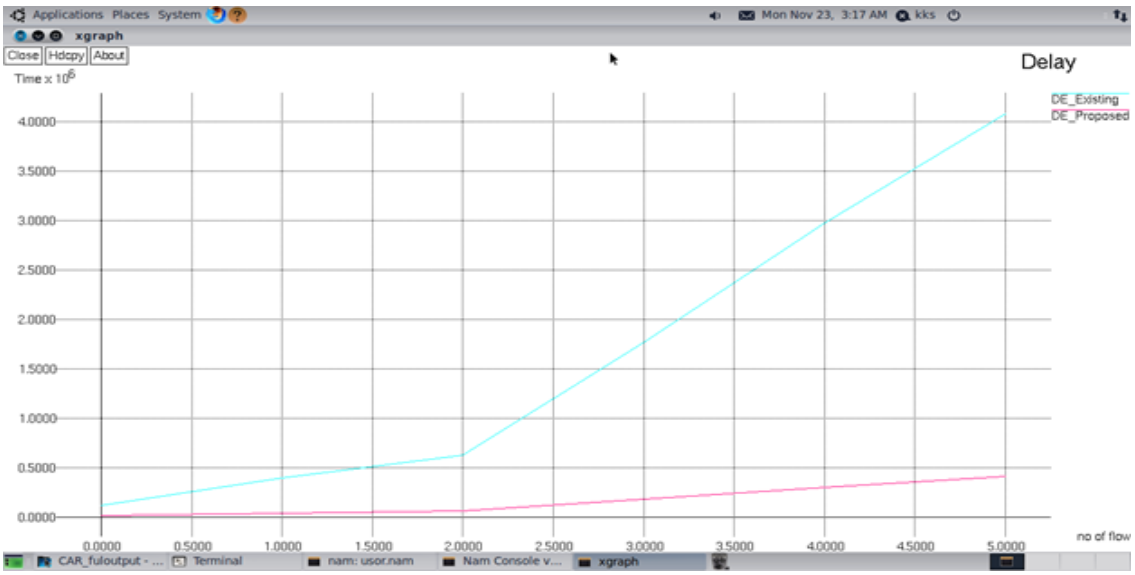

Figure 3 Delay

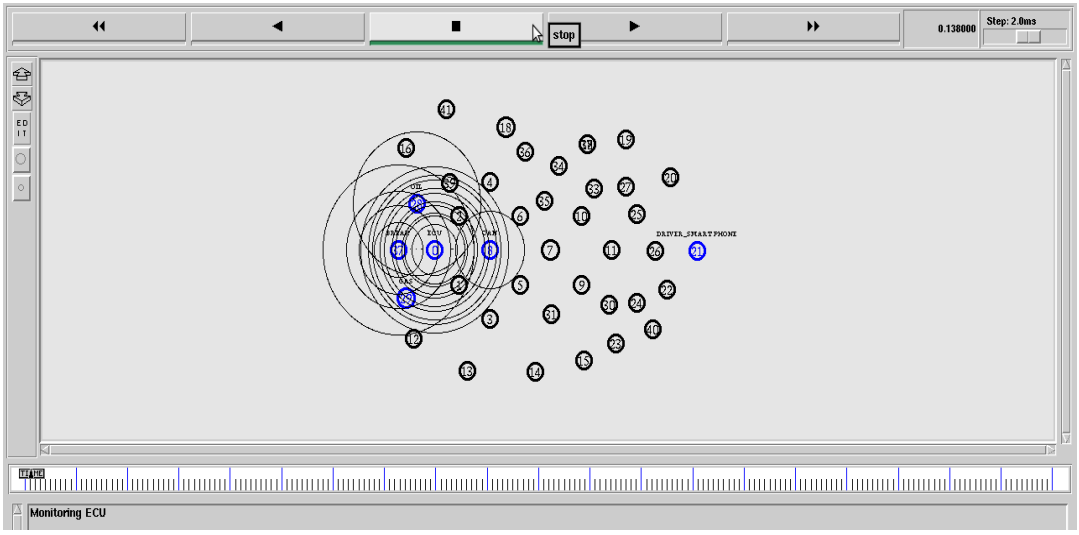

Figure 4 Monitoring ECUs

The average delay is 0.0827742%. The Fig 3.shows delay Vs number of flow of data packets. The delay of current is very high compared to the designed one. In current one, the average time taken by a data packet to arrive to the destination is large while compared to the newly designed one. The Electronic control unit (ECU) starts detecting the reports and it is shown in Fig 4. In a motor vehicle the one or more electrical systems and subsystems are controlled by the electronic circuit. Every part of motor vehicle is monitored by ECU.

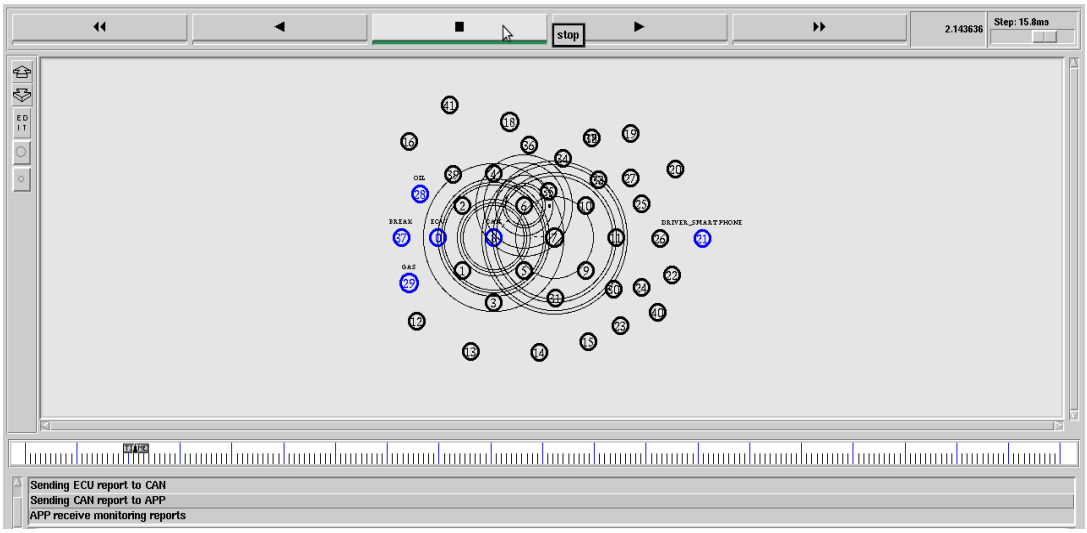

Figure 5 Sending reports to CAN and then to APP

The Fig 5 shows that the controller area network (CAN) forward the repots to APP which is assigned on the victim's android Smartphone. The APP receive the monitoring reports and it forwards data frames of the in-vehicle controller area network to the attacker's server using the Smartphone's mobile communication network which is mentioned on the Fig 6.

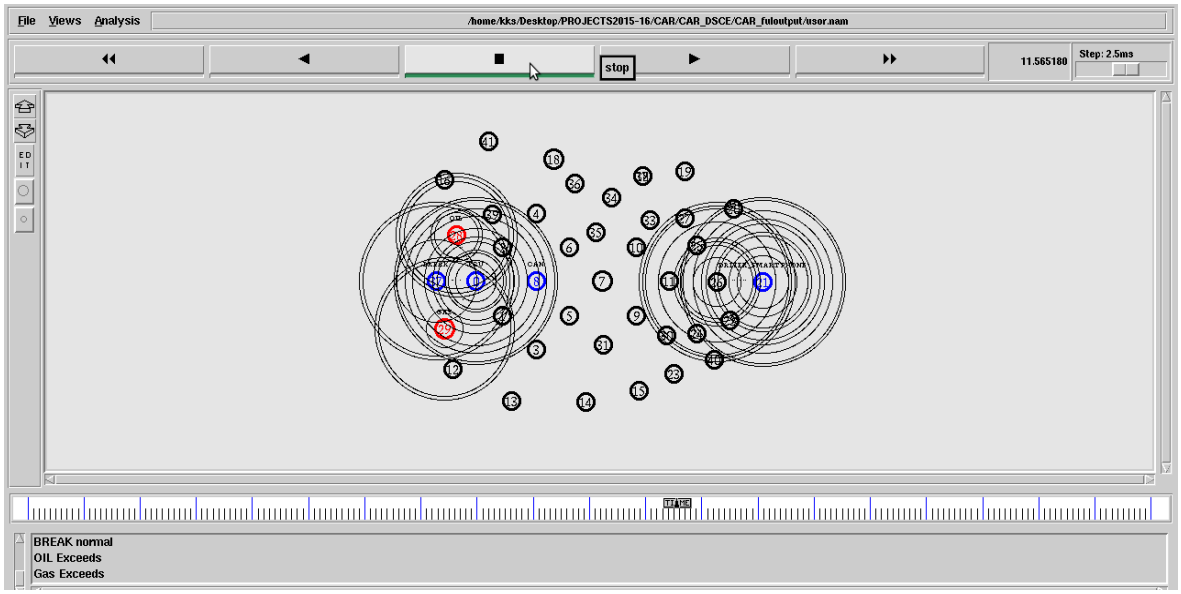

Figure 6 Output

5. CONCLUSION

Vehicles of today have become gradually more dependent on software's to handle their tasks. Cars are getting smarter, but that doesn't mean they are getting safer. As vehicles become more attached to the internet, automakers are failing to take the certain measures to protect them against cyber attacks. Many studies on the susceptibility of in-vehicle CAN have been done recently. An actual attack model is using destructive Smartphone app in the connected car scenario and determined it through empirical experiments. The security and performance of the planned security protocol is analyzed through a judgment based on both Secure-

ECU and Canoe. Random Key Pre-distribution is used for planning the system for allowing secureness and also security protocol is plotted for CAN as a cure in accordance with current CAN requirements. The system works by spreading a key ring to each participating node in the sensor network before classification. For the future, plan to enhance the performance of the planned security protocol with an execution of the hash algorithms on hardware to boost the security technology.

REFERENCES

1. B. Groza and S. Murvay, (2013) "Efficient protocols for secure broadcast in controller area networks," IEEE Trans. Ind. Informa., vol. 9, no. 4, pp. 2034–2042.
2. C. W. Lin and A. Sangiovanni Vincentelli, (2012) "Cyber-security for the Controller Area Network (CAN) communication protocol," inProc. Conf. IASE Int. Conf. Cyber Security, pp. 34.
3. D. K. Nilsson and U. E. Larson, (2008) "Secure firmware updates over the air in intelligent vehicles," in Proc. IEEEInt. Conf. Commun. Workshop, Beijing, China, pp. 380–3844–350.
4. H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann, (2011) "Car2X communication: Securing the last meter A cost-effective approach for ensuring trust in Car2X applications using in-vehicle symmetric cryptography" in Proc. Conf. Veh. Technol., San Francisco, CA, USA, pp. 1–5.
5. K. Koscher et al., (2010) "Experimental security analysis of a modern automobile," in Proc. IEEE Security Privacy. Symp. Oakland, CA, USA, pp. 447–462.
6. P. Kleberger, T. Olovsson, and E. Jonsson, (2011) "Security aspects of the in-vehicle network in the connected car," in Proc. IEEE Intell. Veh. Symp. pp. 528–533.
7. S. Checkoway et al., (2011) "Comprehensive experimental analyses of automotive attack surfaces," in Proc. 19th Conf. USENIX Sec., Washington, DC, p. 6.
8. S. Mangard, M. Aigner, and S. Dominikus, (2003) "A highly regular and scalable AES hardware architecture," IEEE Trans. Computer vol. 52, no. 4, pp. 483–491.
9. T. Hoppe, S. Kiltz, and J. Dittmann, (2011) "Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures," Rel. Eng. Syst. Safety, vol. 96, no. 1, pp. 11–25.
10. T. Nolte, H. Hansson, and L. L. Bello, (2008) "Efficient in-vehicle delayed data authentication based on compound message authentication codes," in Proc. Conf. IEEE 68th Int. Conf. Veh. Technol., Calgary, BC, Canada, pp. 1