ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Adaptive Cruise With Antisteering Control Using WSN

[1]R.Jagadeesh, [2]S.Murali, [3]R.Loganathan, [4]S.Vinothkumar

[1]Assistant professor, Dept. of ECE, Aksheyaa college of engineering, Madhuranthagam, Tamil Nadu, India

[2]Assistant professor, Dept. of ECE, Aksheyaa college of engineering, Madhuranthagam, Tamil Nadu, India

[3]Assistant professor, Dept. of ECE, Aksheyaa college of engineering, Madhuranthagam, Tamil Nadu, India

[4]Professor, Dept. of ECE, Aksheyaa college of engineering, Madhuranthagam, Tamil Nadu, India

ABSTRACT: In this project we design the autonomous and manual vehicle system using the embedded system with wireless communication. In this system we provide high security by using the communication like automatic for RF and manual. Using the RF system we can control the vehicle remote via and using obstacle sensor we can find obstacle in the path. Society is becoming increasingly dependent on embedded computing and sensor technology to enable complex networks of autonomous systems, such as robots, unmanned Ground/Aerial vehicles (UAVs), autonomous-driving cars, and unmanned underwater vehicles (UUVs). Smart Just Drive for Automotive using embedded blue tooth is designed to provide comfortable feel to the user or passenger to check the vehicle status by checking different vehicle parameters like engine temperature, fuel levels etc., and remote by using Smart mobile with Bluetooth Connectivity. This is an inexpensive device which reduces the problem associated with anti- theft control as well. In this paper, we present an automotive security system to disable an automobile and its key auto starting systems through wireless remote control when it is stolen. It hence deters thieves from committing the theft.

KEYWORDS: Automotive, CAN Bus, ECU, MEMS, Accelerometer, Navigation control module (NCM), 3333 Engine control module (ECM), and 333 Electronic brake control module (EBCM).

I.INTRODUCTION

Automobile in-vehicle networks have historically been isolated from attackers due to the limited access possibilities, but with the advent of wireless Internet-based connectivity between the vehicle and its surroundings, this is about to change. The introduction of a wireless gateway as an entry point to the in-vehicle network allows for remote interaction with vehicle firmware, even when the vehicle is running. This allows remote diagnostics and thus, vehicle owner's donors have to drive to a service station to get their car diagnosed. Moreover, firmware updates can easily be applied to thousands of vehicles simultaneously, instead of interfacing every vehicle through the on-board diagnostics (OBD) module, thus removing the need for attaching and detachingcables. In addition, vehicle-to-vehicle and vehicle-to-roadside communication, inter-vehicle communications systems allow vehicles to alert each other of changing weather conditions and to obtain area information from roadside stations.

However, the new technology also introduces new security and safety issues for the manufacturer to consider; cyber-attacks on vehicles are introduced. We dense cyber-attacks as attacks that target the vehicle network. An attacker could, for example, use the firmware update feature to inject unwanted code into the vehicle network while the vehicle is running. As an illustration, consider the case of a speeding vehicle that hits the face of a rock. This incident is either caused by the driver itself, or by vehicle malfunction or physical tampering. If the brake wire is found to be cut, the cause of the accident is most certainly an act of physical tampering, and a criminal investigation needs to be initiated to bring the responsible to a court of law. Current in-vehicle network produces data necessary for the operation and maintenance of the vehicle, and to protect the vehicle from safety-related incidents.

However, when an intelligent attacker is introduced, there is a need to produce data that can reveal both the presence of malicious code, and provide evidence that will aid investigation of a cyber-attack. In this paper, we state a set of requirements for digital forensic investigations of cyber-attacks on automobile in vehicle networks. We analyze the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

current in-vehicle network structure, including node layout and external interfaces. Based on the analysis we derive an attacker model and dense attacker actions.

II RELATED WORKS

The network in the vehicle consists of nodes, gateways, and buses. A node is an Electronic Control Unit, or ECU, Which is connected to the bus? The bus is the shared data transfer media, e.g., copper cables. The buses and the nodes form a network. Data may be transferred from one network to another through a gateway. The ROM memory contains the firmware that is executed on the ECU. Each ECU is responsible for the functionality of a certain area in the vehicle. For example, one ECU is responsible for the head lights system, and one ECU handles the driver door functionality (e.g., lock and window). For more complex functions such as the engine system, a number of Excusers co-operating. Each ECU also has a RAM data area for parameter storage (e.g., which lights are turned on etc.).There are different network types in an in-vehicle network [21]:Controller area network (CAN), local interconnect network (LIN), and media oriented systems transport (MOST). CAN is the most common network in a vehicle today. There are often several CAN networks, e.g., power train and comfort CAN [22]. LIN is a communication protocol used for non-safety critical sensor/actuator systems where CAN is too expensive or not suitable. Communication in LIN is based on a master-slave architecture, where the master is connected to the CAN bus and relays traffic between the CAN and the LIN networks [23]. The MOST protocol is used to carry audio and video information. This network often employs a ring topology with optical fiber for sending/receiving data in a master-slave fashion. The master is connected to the CAN bus and relays traffic between the CAN and MOST networks [21].Two common administrative functions that exist for vehicles are diagnostics and firmware updates. Diagnostics is used to eject single data parameters in nodes [24], and is used for reading node status, such as the passenger door is locked, or controlling node activity (e.g., unlock the passenger door) by writing node status. Diagnostics is usually done through the OBD interface and can be performed.

Firmware update is the process of re-cashing the memory of the ECU to install new firmware, e.g., in the case of vehicle functionality problems [10]. The new application binary is transmitted on the bus, and the target ECU ashes the binary to its ROM and reboots. The well-known security design principle defense-in-depth still applies but must be adapted to the in-vehicle network setting. In this paper we discuss five layers of defense-in-depth: prevention, detection, deflection, countermeasures, and recovery. We therefore focus on intrusion attacks and analyze what methods an attacker can use to read and write data from and to the ECUs.An attacker that wants to elect the in-vehicle network and the ECUs has three means of doing this. The three actions an attacker can perform are diagnostics requests, low-level requests, and update the node rewire. Sending diagnostics queries (SD): An attacker can send read or write requests to get or set certain parameter values in an ECU. Sending low-level requests (SL): An attacker can send low-level read or write requests to read or write the byte value of a certain memory address. Performing _rewire updates (FU): An attacker can update an ECU with new rewire through re-hashing. Thus, an attacker can change the functionality of an ECU to perform malicious acts.

III.THE NEED FOR SECURITY

Current in-vehicle networks primarily meet safety requirements. They are thus designed to withstand failures caused by non-malicious and inadvertent flaws which are produced by chance or by component malfunction. Deployed protection mechanisms are therefore realized by means of fault-tolerance techniques, such as redundancy, replication, and diversity. Since the in-vehicle network historically has been isolated, threats other than those against the safety of the vehicle have not been considered. Therefore, protection against threats originating from intelligent attackers (i.e., security protection) has not been included in the requirements or the design of such networks. Alongside the emerging trend of allowing external communicating parties to interact with the in-vehicle network, an imminent need for security arises. There exist a number of security best practices; however, since the in-vehicle net-work is a non-traditional network in the sense that it consists of resource-constrained embedded computers and the traffic patterns differs from IP-networks, a new set of best practices for such networks must be developed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

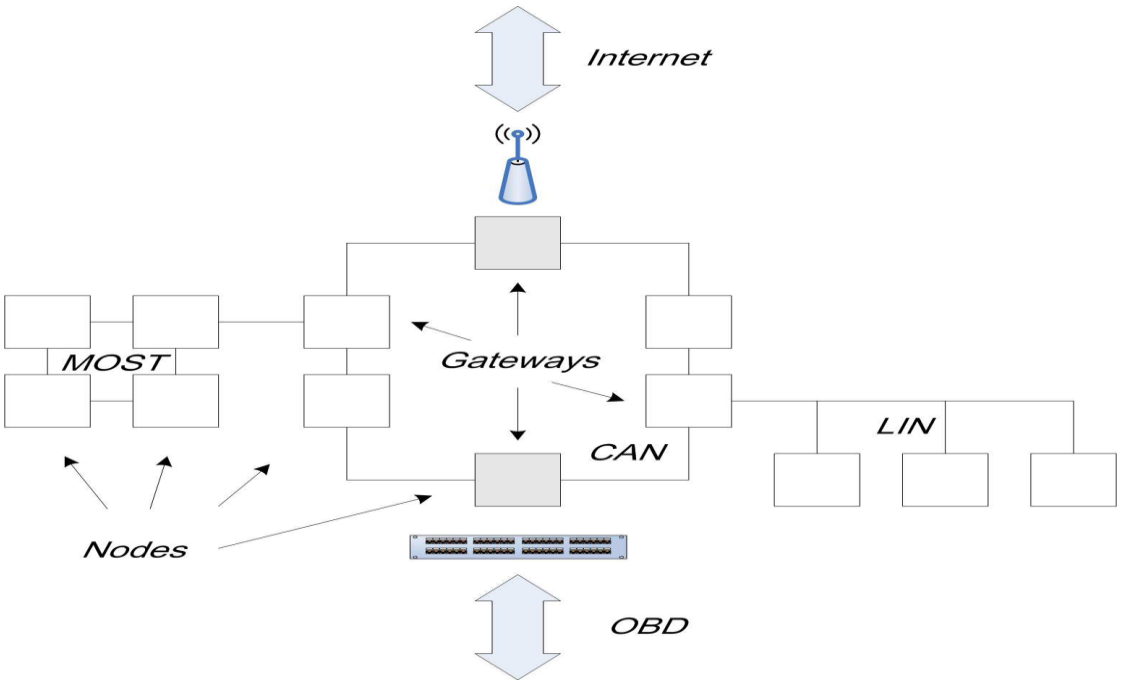


Figure 1: An in-vehicle network consisting of the CAN, LIN, and MOST networks, and two external

A.Prevention.

Prevention is necessary to allow only authorized accesses to interact with the vehicle and within the vehicle. For external communication, proper authentication mechanisms are essential to prevent attackers from sending bogus data or accessing services in the vehicle. In addition, access control and firewalls are necessary to prevent unauthorized accesses and intrusions to the vehicle. For communication within the vehicle, i.e., communication between the embedded computers in the in-vehicle network, proper authentication mechanisms are important to prevent attackers from hijacking an embedded computer or sending false data. The communication protocols in the in-vehicle network have currently no security protection and must be redesigned to incorporate several security features. To determine which ECUs to protect and prevent access to a classification based on safety-security characteristics should be consulted.

B. Detection

Detection is imperative to find attacks on the vehicles and in the in-vehicle network. For external communication, the wireless gateway on the vehicle must incorporate an adequate logging mechanism and provide intrusion detection capabilities. Unauthorized access attempts to services and intrusion attempts to the vehicle must be detected and properly logged by an intrusion detection system. For the in-vehicle network, a lightweight detection and logging mechanism must exist. It is imperative that this mechanism is lightweight since most communication on this network has real-time constraints. Unauthorized access attempts and intrusion attempts to the embedded computers must be detected and logged by a dedicated detection process.

C. Problem Definition

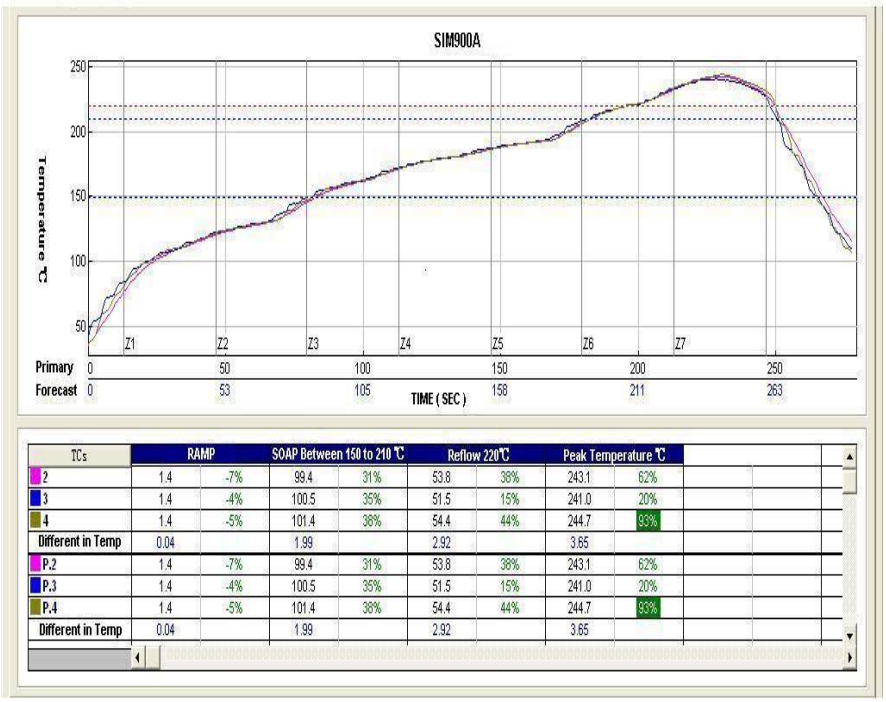
In this section, we formulate a dentition of the problem and the design goals for a complete solution for in vehicle network digital forensic investigations. In addition, we present the considered attacker model, based on terms presented by Howard and Longsta in the CERT taxonomy. We dense an event as an action which is intended to result in a change of state of a selected target. We further a security violation as an event that violates security policy rules, and an attack as a series of steps, where one or more events are included, taken by an attacker to violate the security policy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015



TCs	RAMP		SOAP Between 150 to 210 ℃		Reflow 220℃		Peak Temperature ℃	
2	1.4	-7%	99.4	31%	53.8	38%	243.1	62%
3	1.4	-4%	100.5	35%	51.5	15%	241.0	20%
4	1.4	-5%	101.4	38%	54.4	44%	244.7	93%
Different in Temp	0.04		1.99		2.92		3.65	
P.2	1.4	-7%	99.4	31%	53.8	38%	243.1	62%
P.3	1.4	-4%	100.5	35%	51.5	15%	241.0	20%
P.4	1.4	-5%	101.4	38%	54.4	44%	244.7	93%
Different in Temp	0.04		1.99		2.92		3.65	

Figure 2: Prevention diagram of an in-vehicle network system

Design Goals

To properly perform a digital forensic investigation the necessary data must be present. A method to detect events in the vehicle must be present. To perform a digital forensic investigation, an alert about a security violating event must have been triggered to provide reason to initiate the forensic investigation. Data to answer the questions who, what, where, when, and why must be produced in the vehicle. During the forensic investigation, this data must be available in the ECUs for an investigator to extract the necessary information when needed. Information about the current state (e.g., firmware versions)in a vehicle must be available and stored in a secure location. To detect whether the vehicle has been tampered with, the extracted data must be compared to the original data.

Attacker Model

In our attacker model, we assume that an attacker can access the in-vehicle network from either the Internet interface or the OBD interface. We further assume that the attacker can perform the actions presented in , e.g., inject, modify, and replay messages on the bus as shown in. Moreover, we assume that the attacker can install software, and delete potential logs to hide its presence. We assume that an attacker after a successful intrusion attempts to either read from, or write data to the ECUs. By reading data, an attacker can attack congeniality (secret keys) and privacy (read private driver information).By writing data, an attacker can attack integrity (change functionality of ECUs) and availability (disable ECUs). We therefore focus on intrusion attacks and analyze what methods an attacker can use to read and write data from and to the ECUs.An attacker that wants to eject the in-vehicle network and the ECUs has three means of doing this. The three actions an attacker can perform are diagnostics requests, low-level requests, and update the node firmware. Sending diagnostics queries (SD): An attacker can send read or write requests to get or set certain parameter values in an ECU. Sending low-level requests (SL): An attacker can send low-level read or write requests to read or write the byte value of a certain memory address. Performing firmware updates (FU): An attacker can update an ECU with new firmware through re-cashing. Thus, an attacker can change the functionality of an ECU to perform malicious acts.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

IV. REQUIREMENTS FOR A DIGITAL INVESTIGATION

The present vehicle network is primarily designed to support operational safety and maintenance considerations. As discussed earlier, this is not sufficient for protecting against cyber attacks. We use the design goals along with the attacker model to derive a set of requirements for supporting the digital investigation. The set of requirements is divided according to the design goals and are denoted: Event detection requirements, Forensic data requirements and State information requirements.

Event Detection Requirements

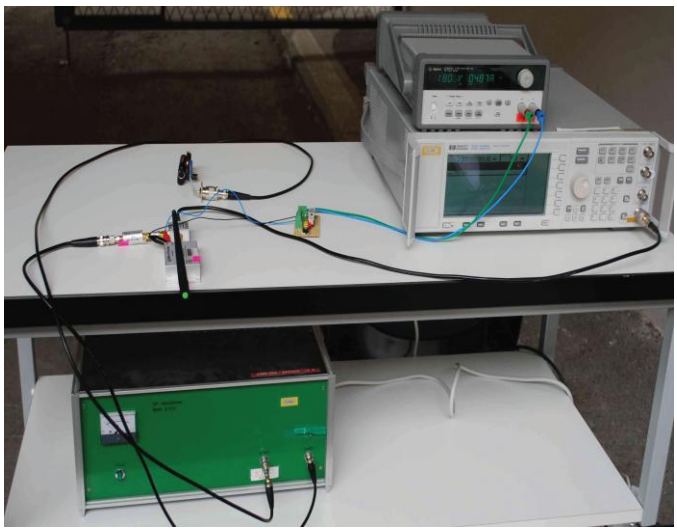


Figure 3(a) Key side.

To detect an event at an early stage it is necessary to introduce a detection mechanism to the in-vehicle network. The event detection requirements address what devices need to be present to detect and alert the appropriate authority that a security violation has been detected. A model-based detection system [4] maintains a list of allowed communication patterns and alerts when prohibited events occur. Also, the alert data is used together with the event data to aid investigation. In addition, there is a need for a storage device and a device. (>50K$) cars, 1 minivan and 2 cars in the compact class(<30K$). We had two different models for only two of the tested manufacturers. During the evaluation of the 10 different PKES systems, we observed that all of them differ in their implementation. We also noticed that even if they rely on the same general idea and similar chips the overall system behaves differently for each model 7. The differences were found in timings (as shown below), modulation and protocol details (e.g., number of exchanged messages, message length). Only the aftermarket system was obviously not using any secure authentication mechanisms. When possible, on each car we measured the distances for the relay, the maximum acceptable delay and the key response time and spread. In this section we describe different attack scenarios and discuss the implications of relay attacks on PKES systems. Common Scenario: Parking Lot. In this scenario, the attackers can install their relay setup in an underground parking, placing one relay antenna close to the passage point (a corridor, a payment machine, an elevator). When the user parks and leaves his car, the Passive Keyless Entry confident that his car is locked (feedback from the car is often provided to the owner with indicator lights or horn).Once the car is out of user's sight, the attackers can place the second antenna to the door handle. The signals will now be relayed between the passage point and the car. When the car owner passes in front of this second antenna with his key in the pocket, the key will receive the signals from the car and will send the *open* command to the car.

The results show large differences between different car models. The key response standard deviations vary from 4 to 196 μs, and the maximum spread - from 11 to 436μs.These values show that the current implementations exhibit large variance.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

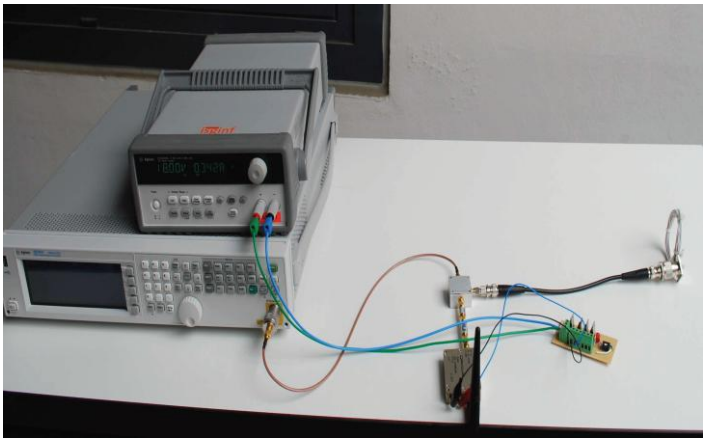


Figure.3 (b) Car side.

Implications of the Relay Attack on PKES Systems

As this messages sent over UHF it will reach the car even if the car is within a hundred meters 11. The car will therefore unlock. Once that the attacker has access to the car, the signals from within the car are relayed and the key will now believe it is inside the car and emit the *allow start* message. The car can now be started and driven. When the attacker drives away with the car, the relay will no longer be active. The car may detect the missing key; however, for safety reasons, the car will not stop, but continue running. Similarly, the car might detect a missing key for several other reasons including if the key battery is depleted. Some car models will not notify the user if the key is not found when the car is on course, while some will emit a warning beep. None of the evaluated cars stopped the engine if the key was not detected after the engine had been started. This attack therefore enables the attackers to gain access (open) and to get authorization to drive (start and drive) the car without the possession of appropriate credentials.

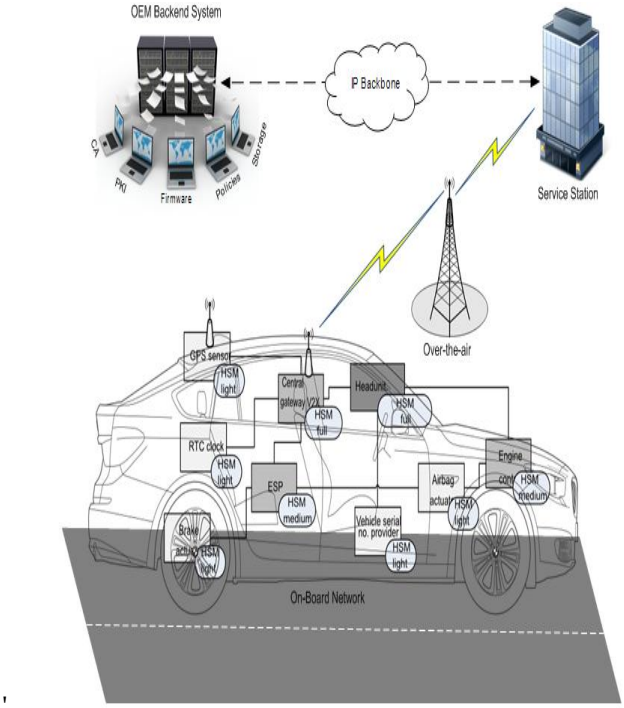


Figure 4 PKES system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

The practical risks of such attacks are reported to be reduced as the attacker needs access to the ODB-II communication port, which requires being able to open the car. There lay attack we present here is therefore a stepping stone that would provide an attacker with an easy access to the ODB-II port without leaving any traces or suspicion of his actions. Moreover, as the car was opened with the original key if an event log is analyzed it would show that the car owner did open the car.

Countermeasures

In this section we discuss countermeasures against relay attacks on PKES systems. We first describe immediate countermeasures that can be deployed by the car owners. These countermeasures largely reduce the risk of the relay attacks but also disable PKES systems. We then discuss possible mid-term solutions and certain prevention mechanisms suggested in the open literature. We finally outline new PKES system that prevents relay attacks. This system also preserves the user convenience for which PKESsystems were initially introduced.

V. RESULTS AND DISCUSSION

The Car Section consists of Arduino, DC Motor, GSM, GPS and Virtual Terminals. The Car can be driven with the help of DC motors. The virtual terminal is used to transfer and monitoring the data sends by car. The Gsm is connected to Car to indicate the Status of the Car.Gps is used to locate the Car.The simulation can be done with the help of Arduino Uno.

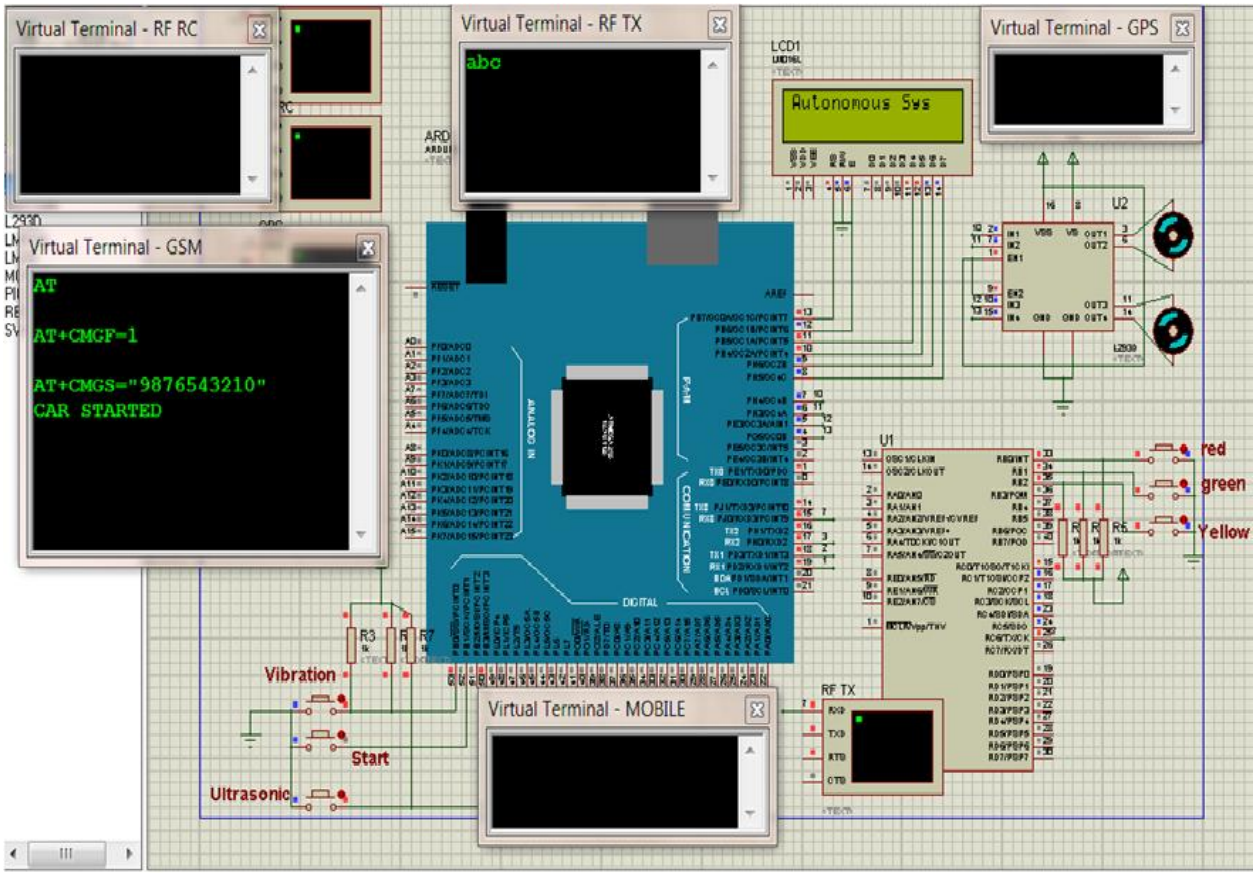


Figure 5 Simulation result

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

VI. CONCLUSION

In this paper, we have introduced and discussed security needs for wireless vehicle-to-infrastructure and vehicle-to-vehicle communication. We have adapted a well-known tax-anomy to the vehicle setting and discussed for each of five defense-in-depth layers the specific applicability and considerations of each layer. The main challenge ahead is the creation of lightweight defense mechanisms. We stress the importance of timely research and deployment of defensive mechanisms in all layers of defense.

REFERENCES

[1] *http://www.mercedes-benz.com/*.
[2] *http://en.wikipedia.org/wiki/Smart key*.
[3] *http://en.wikipedia.org/wiki/Keyless Go*.
[4] *http://vintrack.com/SIU.html*.
[5] Ettus research llc. http://www.ettus.com/.
[6] A. Alrabady and S. Mahmud. Some attacks against vehicles'passive entry security systems and their solutions. *VehicularTechnology, IEEE Transactions on*, 52(2):431 – 439, March 2003.
[7] A. Alrabady and S. Mahmud.Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs.*IEEE Transactions on Vehicular Technology*, 54(1):41–50, January 2005.
[8] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin,and M. Szydlo. Security analysis of a cryptographicallyenabledRFID device.In *Proc. of the 14th USENIX Security Symposium*, Berkeley, USA, 2005.USENIX Association.
[9] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT '93*, pages 344–359, Secaucus, NJ, USA,1994. Springer-Verlag New York, Inc.
[10] S. Capkun, L. Butty´an, and J.-P.Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proc. of the ACM Workshop on Security of AdHoc and Sensor Networks (SASN)*,Washington, USA, October 2003.
[11] S. Capkun and J.-P.Hubaux. Secure positioning in wireless networks. *Selected Areas in Communications, IEEE Journalon*, 24(2):221–232, February 2006.
[12] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore. So near and yet so far: Distance-bounding attacks in wirelessnetworks. In *Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS)*,2006.
[13] N. T. Courtois, G. V. Bard, and D. Wagner. Algebraic and slide attacks on KeeLoq. In *Fast Software Encryption: 15thInternational Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, pages 97– 115, Berlin, Heidelberg, 2008. Springer-Verlag.
[14] B. Danev, H. Luecken, S. Capkun, and K. Defrawy.Attackson physical-layer identification.In *Proc. of the 3th ACMConference on Wireless Network Security (WiSec)*, pages89–98.ACM, 2010.
[15] Datagram. Lock picking forensics. Black Hat USA Briefings, 2009.
[16] Y. Desmedt, C. Goutier, and S. Bengio.Special uses and abuses of the Fiat-Shamir passport protocol. In *CRYPTO*, pages 21–39, 1987.
[17] P. Dodd. *The low frequency experimenter's handbook*.Herts : Radio Society of Great Britain, 2000. ISBN : 1-872309-65-8.
[18] S. Drimer and S. J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *Proceedingsof 16th USENIX Security Symposium*, Berkeley, CA,USA, 2007. USENIXAssociation.
[19] M. Flury, M. Poturalski, P. Papadimitratos, J.-P.Hubaux,and J.-Y. Le Boudec. Effectiveness of Distance-DecreasingAttacksAgainst Impulse Radio Ranging. In *3rd ACM Conferenceon Wireless Network Security (WiSec)*, 2010.
[20] F.-L. W. Frank Stajano and B. Christianson. Multichannel protocols to prevent relay attacks. In *Financial Cryptography*,2010.
[21] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch,H. Poor, and Z. Sahinoglu. Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks. *Signal Processing Magazine, IEEE*, 22(4):70–84,July 2005.
[22] G. Hancke. Practical attacks on proximity identification systems (short paper). In *Proc. of the 27th IEEE Symposium onSecurity and Privacy*, 2006.
[23] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *SecureComm '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 67–73, Washington, DC, USA, 2005. IEEE Computer Society.
[24] G. P. Hancke, K. Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers& Security*, 28(7):615–627, 2009.
[25] Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006.