Indian Journal of Science and Technology, *Vol 8(28), DOI: 10.17485/ijst/2015/v8i28/74872, October 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secure and Authenticated Vehicle Navigation System

Dalip[1]*, Vijay Kumar[2] and Rohit Vaid[2]

[1]Department of Information Technology, MMEC, Maharishi Markandeshwar University, Mullana - 133207, Haryana, India; dalipkamboj65@gmail.com
[2]Department of Computer Science and Engineering, MMEC, Maharishi Markandeshwar University, Mullana - 133207, Haryana, India; dean.acadaffairs@mmumullana.org, rohitvaid@mmumullana.org

Abstract

Background/Objectives: Although, several security mechanisms have developed for vehicle navigation system yet there is a need of more advancement in existing or development of new security architectures. The main objective of this paper is to provide security and authenticity for vehicle navigation system. **Methods/Statistical Analysis:** Existing cryptography algorithms and fault tolerance technique helps to designed novel secure architecture. A fault tolerance based mathematical model is used for system analysis. The inputs for the system are latitude, longitude and digested engine number. **Findings:** It has been observed that designed system is able to provide the correct information in spite of corrupted signal is sensed at destination end (at server side). **Application/Improvements:** Designed secure and authenticated architecture which improve fault tolerance by applying fault tolerance technique on digested information and also reduces server overhead.

Keywords: Fault Tolerance, GPS Receiver, Message Digest, Navigation System, Secure and Authenticated

1. Introduction

Global Positioning System[13] (GPS) and Global System for Mobile Communication (GSM) based tracking systems are used to track the vehicle around the world. There are two modules namely vehicle location tracking and information storage. The GPS receiver retrieves the location information of tracking vehicle and java enabled mobile sends this information to the server side through SMS. Nowadays, communication among devices and the people is increasing fast. Secure communication of the digital information is very important between the devices as attackers can perform various types of attacks including interception, modification, fabrication, and interruption etc. during the time of information transmission. There are several principals of security are confidentiality, Integrity, authentication, non repudiation, access control and availability are followed as shown in Figure 1. Symmetric and asymmetric, two types of cryptography algorithms are used to protect the information. The symmetric cryptography algorithms uses single key for encrypting and decrypting the data e.g. Data Encryption Standard (DES), Double DES (2DES), Triple DES (3DES), International Data Encryption Algorithm (IDEA), RC4 and RC5. Two keys are used in asymmetric cryptography algorithms, one for encryption and the other for decryption e.g. RSA and DSA. GPS receivers and java enabled mobile with SIM card are used as hardware in the designed system. The authentication problem is solved using message digest algorithm and the problem of loss of integrity is solved using asymmetric cryptography algorithm. Engine, chassis and registration numbers uniquely identify the vehicles, in our research work we apply message digest algorithm on engine number to prevent fabrication attack. The delivery of faulty packets can be minimized by reducing the packet size. Compression of the packet is done by using message digest concept to improve the fault tolerance.

Many researchers have implemented secure systems for vehicle tracking based on hardware and software, but

*Author for correspondence

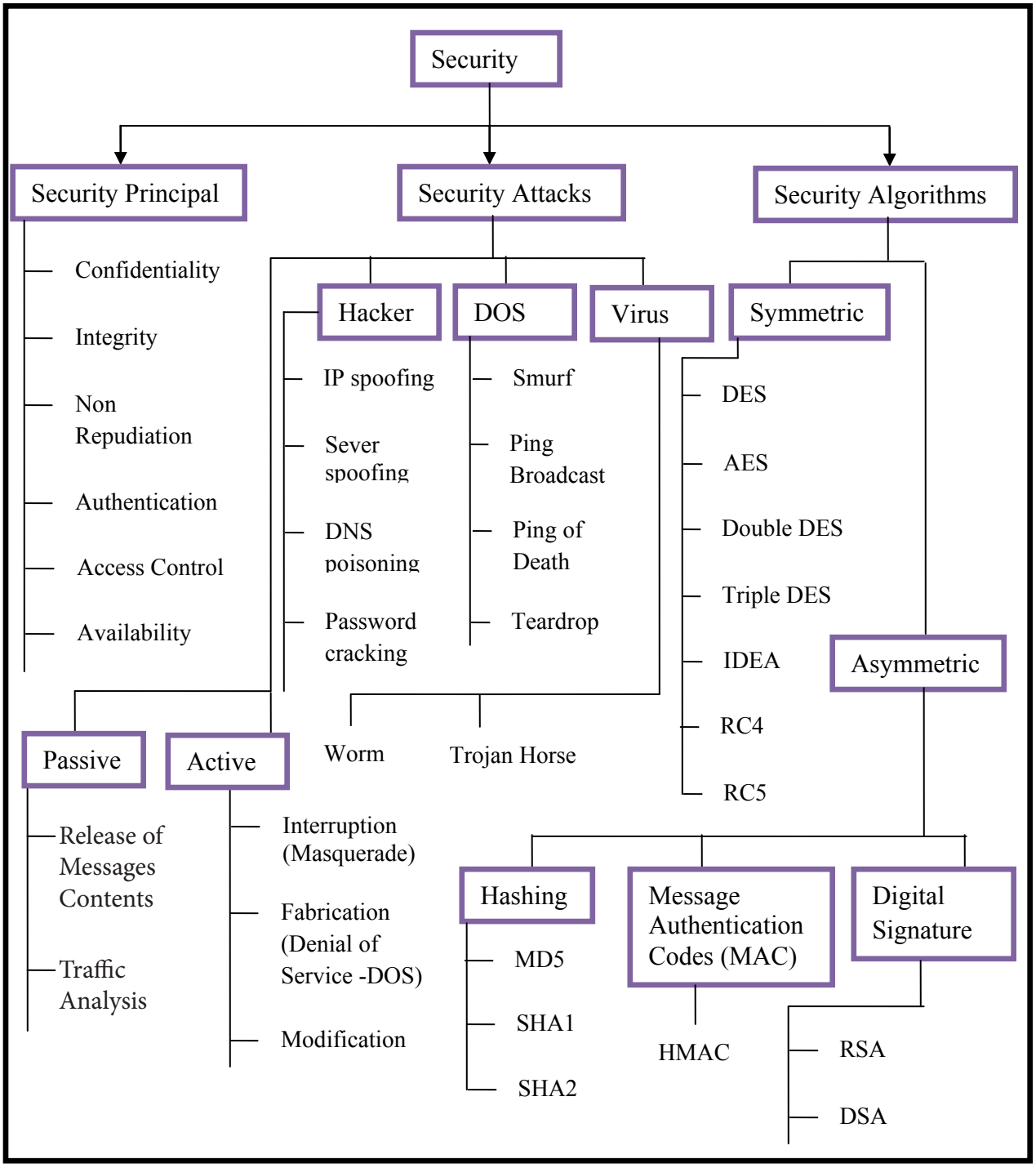

Figure 1. Overview of security principal, security attacks and security algorithms[11].

the literature of this article shows software based secure architectures. The security objectives, security attacks and various cryptography algorithms are shown in Figure 1. Jattala I. et al. introduced a Secure[1] Automotive Telemetric System (SATS). The encrypted information is transmitted between SATS and the tracking server. The security of TCP/IP socket (primary communication channel of SATS) is done by SSL/TLS protocol and of SMS (secondary or backup communication channel) is made by using AES-256 encryption algorithm. Constantinescu

Z. et al. presented a system[2] which provides safety of drivers and passengers from accidents related to tracking system and intentional situations, events like criminal acts by other person, any malicious intention and deliberate causations. The core security technologies and mechanisms[3] along with detailed description of business models, vehicular applications relying on IT security was provided by Wolf M. et al. in 2007. An analysis of different attacks on navigation system is done by Becker G. T. et al. and authentication mechanism was discussed for vehicle[4] tracking systems, based on Timed Efficient Stream Loss-Tolerant Authentication (TESLA) algorithm. Han K. et al. purposed a three tired mechanism[5] and architecture to securely integrate external devices with the devices placed in vehicles. The architecture is divided into three modules: user devices, Electronic Control Units (ECUs) on vehicle network and gateway. Three tier architecture of this authentication protocol provides secure communication between in-vehicle network and external network. A secure, safe and comfortable mobility system was designed by Yano A. et al. to reduce congestion[6] by using smart phones, advance mobile communication and by connecting the vehicles to internet. An intelligent transportation system was introduced to provide a secure, cost[7] effective architecture for vehicle tracking by using existing infrastructure. Wullems C. et al. and Rouf I. et al. proposed authentication[8] schemes[9] which provide authenticity, integrity, privacy and security, the performance of this system is calculated by software simulation. A trusted platform for inter-vehicle communication[10] was implemented by Schweppe H. et al. which were also used to securely store cryptographic material to perform cryptographic operations. TPM-based secure[14] architecture for Vehicular Ad hoc Network (VANET) is designed by Suresh J. S. et al. The deployment of base station does not require along the road for this architecture. The literature review specifies that researchers have designed various software based secure architecture to protect the communication between hardware devices and users, but none of them provided this kind of architecture for information security with fault tolerance[12]. Asymmetric cryptography algorithm is used to achieve our research goal.

The rest of the paper is organized as follows. The section I describes the related work for security in vehicle navigational system. The section 2 presents system requirements of proposed system. The secure system architecture is provided in section 3 and the section 4 shows the query system. Results and discussions are presented in section 5. Finally section 6 discusses the conclusion and future work of the paper.

2. System Requirements

The major hardware requirements of the system include GPS receivers, Java enabled GSM mobile phones, and TTL Bluetooth, GSM modem and the software requirements is Microsoft Visual Basic 6.0. In our research work the idea of taking Java enabled mobile with SIM card is to do programming in J2ME according to system requirements to set the criteria for sending SMS.

3. System Architecture

Figure 2 shows the secure architecture for vehicle location tracking and information storage. Some software and hardware tools are required to implement system architecture. System architecture is able to create a secure communication between the levels discussed below:

- Vehicles to server.
- Sever to users.

The idea behind this architecture is simple which uses SMS for communication between involved parties. GPS receivers and Java enabled GSM mobile phones with SIM cards are placed in vehicles, interconnected via TTL Bluetooth. The location information from satellites is received by GPS receivers and sent to server side through SMS. If SIM card is portable then unauthorized person can replace it and wrong navigational information will produce regarding particular vehicle. The fabrication and modification attacks can affect the information, so it is must to provide a secure communication among the involving hardware, software and users. Security is implementing by using asymmetric cryptograph algorithms. A fingerprint or message digest of vehicle engine number is generated with secret key K1 and encryption of location information like latitude, longitude with public key PK1 is done using RSA algorithm. Encrypted information is sent to server side through SMS with the help of J2ME program. At server side, the server program matches the Message Digest (MD_1) in database, if exact match is found then the information will be accepted and updating the received SMS information in database is done corresponding to that mobile number from which SMS is received otherwise fault tolerance

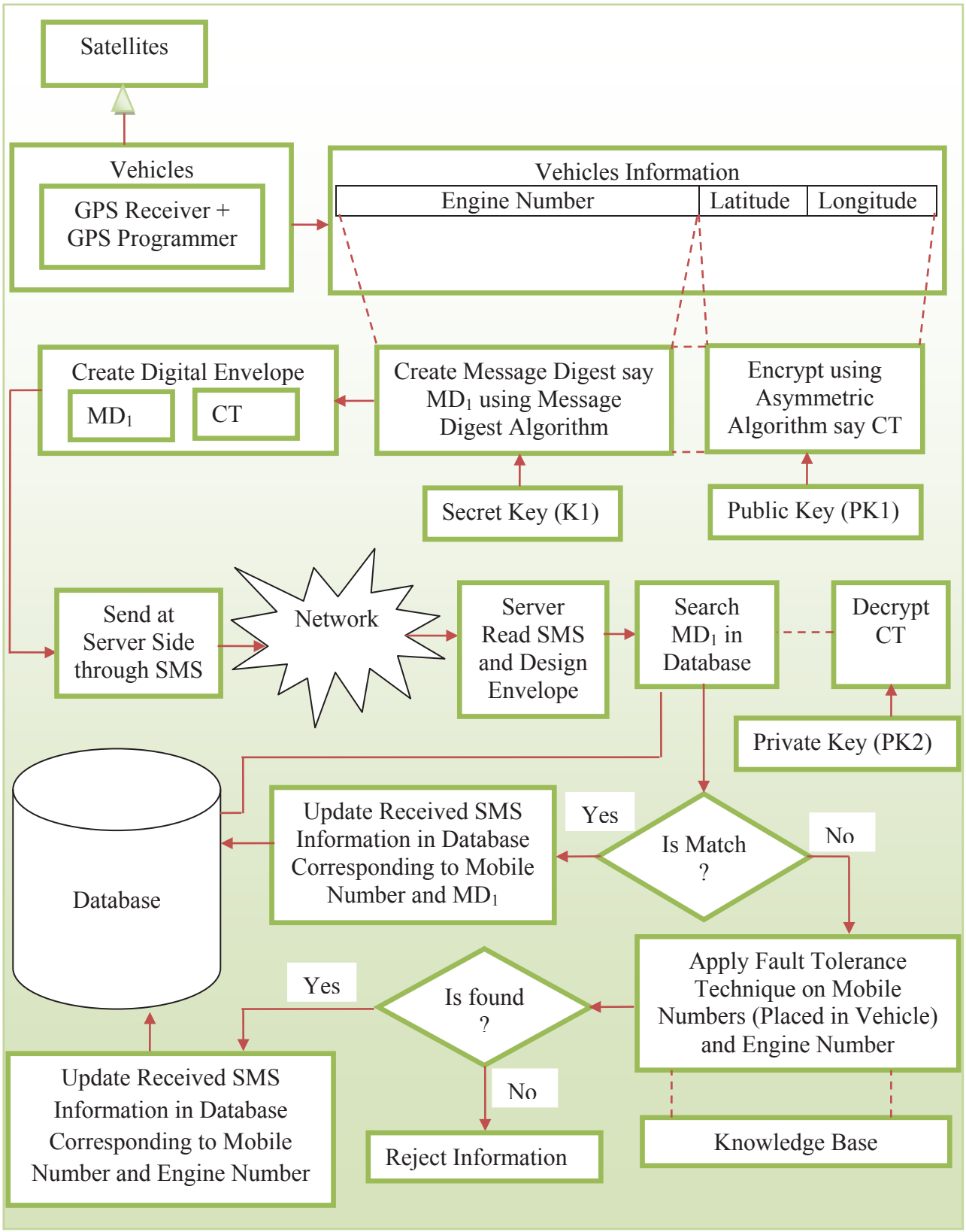

Figure 2. Secure architecture for vehicle to server.

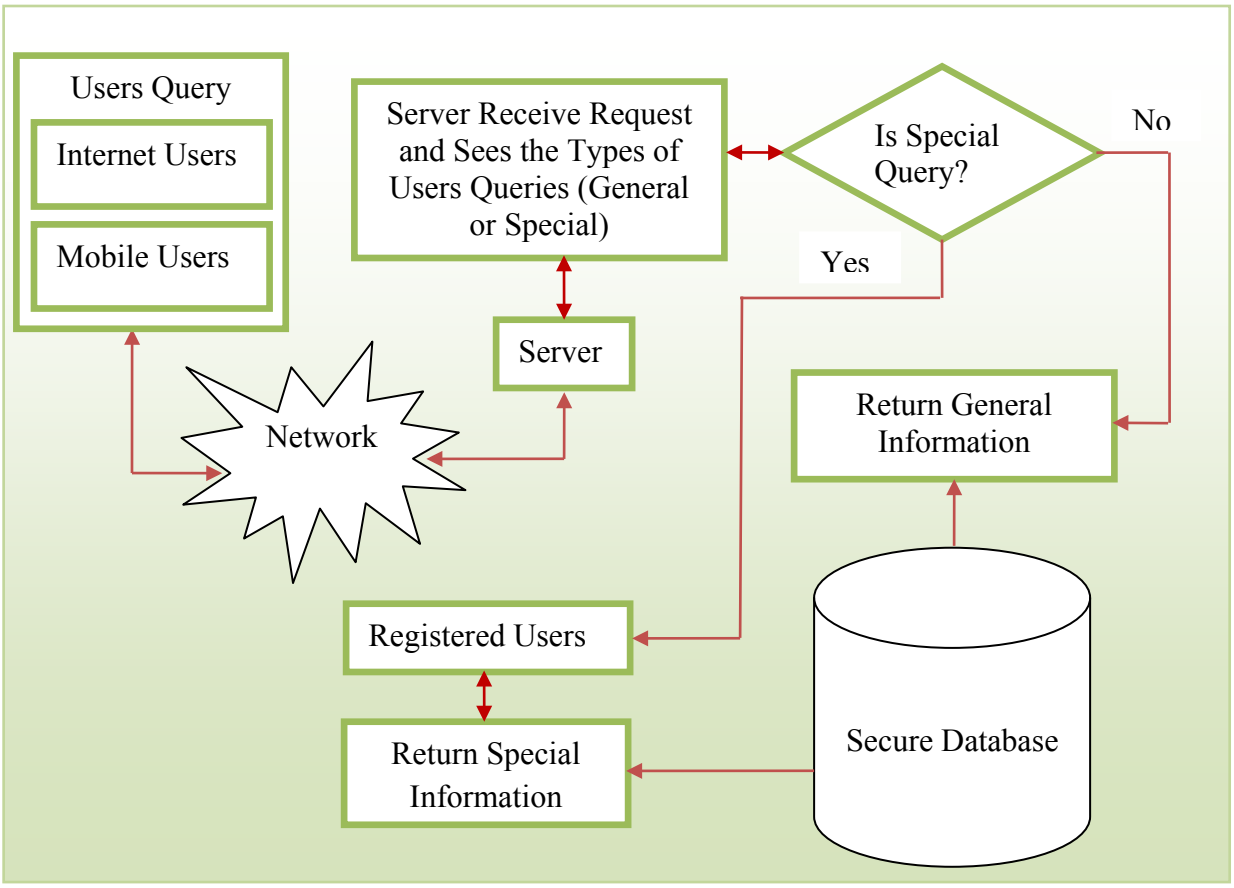

Figure 3. Secure information exchange between (server to users) and (users to server).

technique will apply on the digested message. In case, if associated message is found corresponding to original message then updating of the received SMS information will be done in database corresponding to the mobile number and the engine number otherwise it will reject the information. This mechanism provides the solution of fabrication attack and protects the location information from attackers.

4. Query System

The user's quires are divided into two parts:

- General query.
- Special query.

The general quires for the vehicle navigational systems are the arrival and departure time of buses, list of routes, list of available toll plaza on the route etc. and special queries are location information, list of stops of particular buses. In case of general query the system users have no need to register for accessing general information of the vehicles but in special queries system users have to do registration before accessing private information of vehicles as shown in Figure 3.

5. Results and Discussion

For system analysis, first of all mobile number and engine number is converted into binary form whenever messages arrive at the server side. The associated messages size should be less than original message size.

Example 1:
Original Message (Mobile Number) Associated Message (Digested Engine Number)

Mob_1= [1 0 1 1 0 1 1 0] Eng_1= [1 0 1 1]
Mob_2= [1 1 0 0 1 1 0 0] Eng_2= [1 0 0 1]
Mob_3= [0 0 1 1 0 0 1 1] Eng_3= [0 0 1 1]

Bi-Polar forms (Replace -1 at the place of 0)

Mob'_1 = [1 -1 1 1 -1 1 1 -1] Eng'_1 = [1 -1 1 1]

Mob'_2 = [1 1 -1 -1 1 1 -1 -1] Mob'_1 = [1 -1 -1 1]

Mob'_1 = [-1 -1 1 1 -1 -1 1 1] Mob'_1 = [-1 -1 1 1]

Calculates weight matrix by matrix multiplication of Eng'_K with the transpose of (Mob'_K) where k = 1 to n

$$\text{Weight Matrix (WM)} = \sum_{k=1}^{n} \left(Mob_k^{'}\right)^T Eng_K$$

$$\begin{bmatrix} 3 & -1 & -1 & 1 \\ 1 & 1 & -3 & -1 \\ -1 & -1 & 3 & 1 \\ -1 & -1 & 3 & 1 \\ 1 & 1 & -3 & -1 \\ 3 & -3 & -1 & 1 \\ -1 & -1 & 3 & 1 \\ -3 & 1 & 1 & -1 \end{bmatrix}$$

$$\text{Output} = \text{O (NET)} = \begin{cases} 1, \text{ if } NET > 0 \\ 0, \text{if } NET < 0 \\ \text{Previous Output, if } NET = 0 \end{cases}$$

Associated message Eng_1 (Engine number) corresponding to original message Mob_1 (Mobile number) which is transmitted from vehicles is computed as:

NET = Mob'_K. WM = [4 -10 12 8]

Output = M (NET) = [1 0 1 1] = Eng_1 (1)

NET = Eng'_K. WM = [3 -3 3 3 -3 3 3 -3]

Output = M (NET) = [1 0 1 1 0 1 1 0] = Mob_1 (2)

From the equation (1) and (2) it's quite clear that the correct delivery of information is sent and no one has change the content of message but in case, if attacker changes the fourth bit [1 0 1 0] shown as:

NET = Eng'_K. WM = [2 -2 2 2 -2 2 2 -2]

Output = M (NET) = [1 0 1 1 0 1 1 0] = Mob_1

The above output shows that information is received successfully in spite of corrupted signal due to missing bit at fourth position. The proposed architecture of system provides a secure communication between the vehicle and the server. It stored authenticated and secured information into database despite of modifying information by hackers. The message digest concept minimize server overhead by reducing the packet size from their normal size. It has also been observed that designed system is able to provide the correct information in spite of corrupted signal is sensed at destination end (at server side).

6. Conclusion and Future Work

Our result shows, the proposed secure and authenticated architecture minimizes the server overhead by reducing the size of sending packets by applying message digest technique. The concept of using message digest is to provide authenticity and to reduce the chance of missing bits from sending packet due to small size of the packet. It secures the location information from modification and provides protection against fabrication and modification attacks. In future we can improve the security of our system by using latest security mechanism and faults can be reduced.

7. References

1. Jattala I, Durrani S, Farooqi J, Junjua G, Shafique A, Hussian F, Mahmood H, Ikram N. Secure Automotive Telematics System (SATS). IEEE; 2103 Sep 10-12. p. 262–7.
2. Constantinescu Z, Vladoiu M. Challenges in safety, security, and privacy in the development of vehicle tracking systems; 2013. p. 1–6.
3. Wolf M, Weimerskirch A, Wollinger T. State of the art: Embedding security in vehicles. EURASIP Journal on Embedded Systems. Hindawi Publishing Corporation; 2007. p. 1–16.
4. Becker GT, Lo S, Lorenzo DD, Qiu D, Paar C, Enge P. Efficient authentication mechanisms for navigation systems: A radio-navigation case study; 2009. p. 1–12.
5. Han K, Potluri SD, Shin KG. On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks. Philadelphia, PA, USA: ICCPS'13. Apr 8-11, ACM; 2013. p. 160–9.
6. Yano A, Honda T, Hayashi A, Miyazawa H, Sawajiri H. Car information system for added value in connected cars. Hitachi Review. 2014; 63(2):128–32.
7. Hoh B, Gruteser M, Xiong H. Enhancing security and privacy in traffic-monitoring systems. IEEE CS and IEEE Com Soc; 2006.
8. Rouf I, Miller R, Mustafa H, Taylor T, Oh S. Security and privacy vulnerabilities of in-carwireless networks: A tire pressure monitoring system case study. US National Science Foundation under grant CNS-0845896, CNS-0845671, and Army Research Office grant W911NF-09-1-0089; 2010. p. 1–16.
9. Wullems C, Pozzobon O, Kubik K. Signal authentication and integrity schemes for next generation global navigation satellite systems. Munich, Germany: Proceedings of the European Navigation Conference GNSS; 2005.
10. Schweppe H, Roudier Y. Security issues in vehicular systems: Threats, emerging solutions and standards. EURECOM, SAR-SSI; 2010. p. 1–5.

11. Kahate A. Cryptography and network security. Tata Mcgraw Hill Education Private Limited. 2008.
12. Kumar V, Patel RB, Singh M, Vaid R. A neural approach for reliable and fault tolerant wireless sensor networks. Int J Adv Comput Sci Appl. 2011; 2(5):113–37.
13. Dalip KV. Effect of environmental parameter on GSM and GPS. Indian Journal of Science and Technology. 2014; 7(8):1183–8.
14. Suresh JS, Jongkun L. A TPM-based architecture to secure VANET. 2015; 8(15):1–6.