Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Secure vehicle tracking using RFID

Ibrahim M. Alseadoon, Rabie A. Ramadan *, Ahmed Y. Khedr, Badr M. Alshammari

College of Computer Science and Engineering, University of Hail, Hail, Saudi Arabia

ARTICLE INFO

Article history:
Received 16 March 2019
Received in revised form
12 July 2019
Accepted 17 July 2019

Keywords:
Localization
Tracking
RFID
Internet of things

ABSTRACT

Localization technology such as GPS is one of the most methods used to guide drivers to their final destination. It is also used in some other applications including tracking. However, it seems that GPS technology by itself might not be sufficient especially in tunnels and mountains. First, to have a strong signal between an orbiting satellite and a GPS receiver, there must be a relatively clear line of sight. Obstructions such as buildings, trees, and large mountain passes can potentially weaken the strength of the signal from the satellites and make the positioning data less reliable. Also, GPS localization signals in most of the tracking applications sent Short Message Service (SMS) that are not never secured. Therefore, SMS signal might be intercepted, eavesdropped, replayed, and modified and this might lead to misguided vehicles, trucks, container cargos and trains. This paper concerns the security of vehicles tracking information for the sake of transportation security. This paper also suggests other localization technology along with GPS for accurate localization such as RFID in addition to proposing a lightweight security algorithm for tracking information.

1. Introduction

In 2010, Saudi Arabia Railway Organization (SRO) signed a six months' contract with German International Cooperation (GIZ) to work on a master railway plan for the Kingdom till 2040. The plan has been settled, and currently, there is an efficient railway trip between Riyadh and Dammam. The plan includes many other cities in the Kingdom including Hail. At the same time, in July 2014, the SRO invited consultants to pre-qualify for construction supervision contracts on the Saudi Landbridge railway project. The project is intended as a 950 km freight link between Jeddah on the Red Sea Coast and the capital Riyadh. The scheme would also see the existing rail link between Riyadh and Dammam on the Arabian Gulf coast upgraded, to establish a continuous 1,400 km east-west rail link across the country.

Therefore, the kingdom within a few years will have an important railway system as a transportation method around the cities. However, as it is known, these railways will be crossing through the desert may be for a large number of Kilometers, especially the new landbridge railway. Also, the carried goods vehicles might not survive for a long time; at the same time, to make sure that each cart is not opened, therefore, the kingdom within a few years will have an important railway system as a transportation method around the cities. However, as it is known, these railways will be crossing through the desert may be for a large number of Kilometers, especially the new landbridge railway. Also, the carried goods vehicles might not survive for a long time; at the same time, to make sure that each cart is not opened during the trip, there is a need somehow to secure the train through monitoring. Runtime data about the train can provide momentary help when needed.

At the same time, there are huge goods transportation by trucks moving around the country. Trucks are also crossing thousands of kilometers in desert holding goods that might not survive for a long time if something goes wrong with the truck. Thus, truck accurate tracking and monitoring might be an urgent requirement. However, the current tracking systems depend mainly on the SMS messages which is not secure by default where messages are sent in clear text.

This research investigates the security of the tracking system especially the data transferred from the vehicles to the base station without interfering, changing or even eavesdropping. It also investigates using RFID along with GPS to track and monitor moving vehicles along the roads. In addition, the

* Corresponding Author.
Email Address: ra.ramadan@uoh.edu.sa (R. A. Ramadan)
https://doi.org/10.21833/ijaas.2019.10.001
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-0281-9381

project will be utilizing the Arduino board with GPS, sensors, and GSM shields for the purpose of monitoring and transferring data.

The paper road map is as follows: Next section is the introduction to the paper; section 2 is the literature review, the used methodology is presented in section 3, the experiments and discussion are explained in section 4, and the paper is concluded in section 5.

2. Literature review

Transportation research is one of the very attracting fields. There are many issues that are considered in transportation. One of these issues is the fleet planning and roads management. Another field is the automatic signal control where signals become smart and act according to the traffic situations (Salehi et al., 2014; Padrón et al., 2014). Furthermore, there are some work has been done in buses and underground transportation schedule (Ting-ting, 2012).

Nevertheless, some transportation security issues are considered for research (Altunbasak and Owen, 2007; Buttyan and Csik, 2010; Lee and Ernst, 2011; Radhamani and Ramasamy, 2002). However, up to our knowledge, there is no study to the intrusion problem to vehicles that cross cities and an environment such as Saudi Arabia. In addition, there is a need for securing the tracking information transferred from the vehicle to the base station especially if the cellular network is used to transfer the data. Moreover, an accurate localization to the vehicles, trains, and other traveling fleet is another objective of this research. We believe that Saudi Arabia new transportation system will have Nevertheless, some transportation security issues are considered for research (Altunbasak and Owen, 2007; Buttyan and Csik, 2010; Lee and Ernst, 2011; Radhamani and Ramasamy, 2002). However, up to our knowledge, there is no study to the intrusion problem to vehicles that cross cities and an environment such as Saudi Arabia. In addition, there is a need for securing the tracking information transferred from the vehicle to the base station especially if the cellular network is used to transfer the data. Moreover, an accurate localization to the vehicles, trains, and other traveling fleet is another objective of this research. We believe that Saudi Arabia new transportation system will have special characteristics that need to be considered. This research is considered as a start point in this regard.

RFID has been used in many applications including building securities and tollways (Infanta and Hemalatha, 2013; Kamarulazizi and Ismail, 2010), it consists of readers and tags. Tags are classified into passive and active tags. The passive tags contain no power source while the active tags have their power sources. In passive tags, the power is generated from the reader while in active tags, there is an associated power with the tag. RFID is used for instance in attendance systems where each employee may hold a tag and wirelessly the reader can identify him/her (Lim et al., 2009; Ramadan, 2009). RFID is also proposed to be used for pilgrim identification where the tag is attached to a simple device such as watch (Mohandes, 2008).

One of the interesting security algorithms proposed for Internet of Things (IoT) is SIT (Usman et al., 2017). As stated in the original algorithm, it is 64 bits' key and only 5 rounds. The 5 rounds are shown in Fig. 1. Also, the key expansion process is shown in Fig. 2.

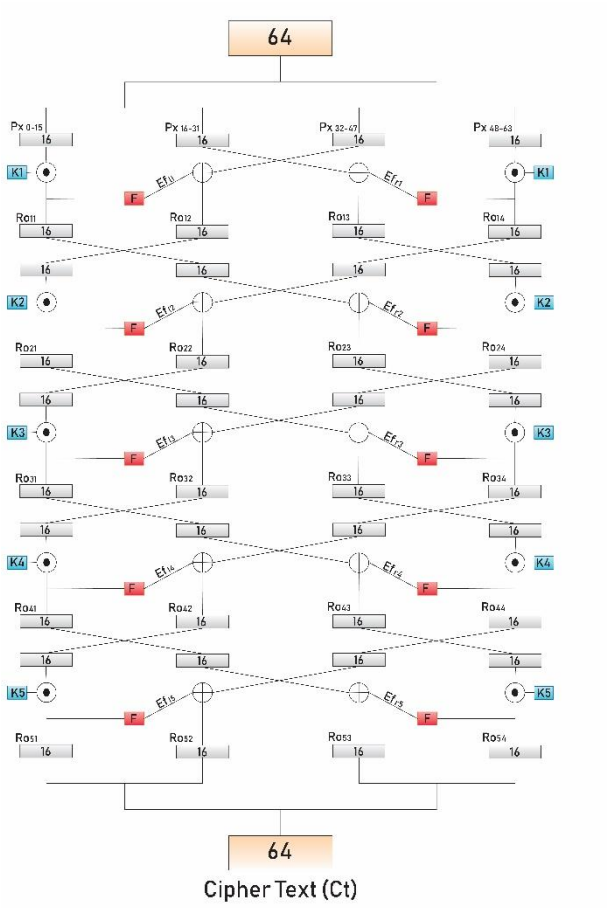

Fig. 1: SIT five rounds (Usman et al., 2017)

This paper investigates the best method to keep the vehicles safe, monitored all the time, and promptly send alarms to the main center or to the police for emergency response if something goes wrong.

3. Methodology

To tackle the secure vehicle monitoring problem, our proposed framework consists of the following components

3.1. Server software

The server will be on the base station for monitoring the vehicles around their way to the destination. The server involves an SMS receiver for receiving the vehicles SMS message. It also contains the decryption algorithm for deciphering the received SMS messages

3.2. On vehicle client

The client in this context is not just softwareWe propose to utilize the Arduino board to act as a client The board will be mounted with GSM and GPS shields and connected to IR sensors and RFID tag. A SIM card is attached to the GSM shield for data transferThe GPS shield is also used to report the location of the vehicle along the road.

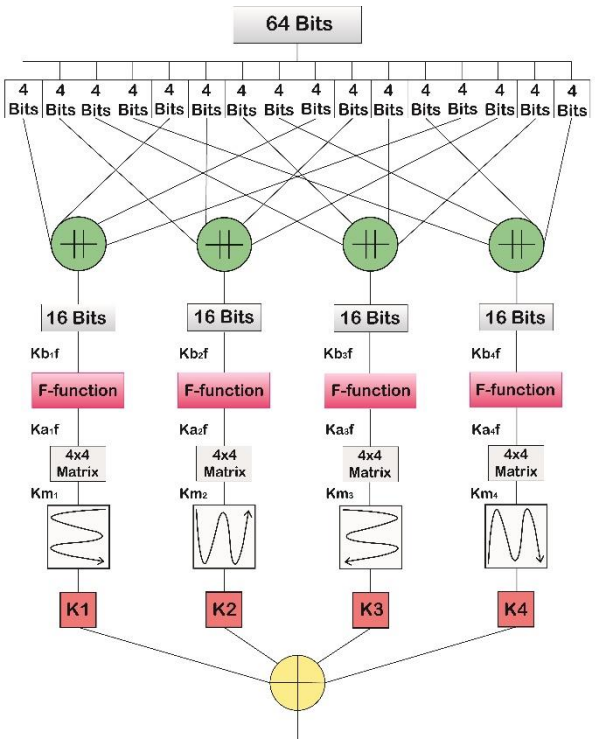

Fig. 2: Key expansion (Usman et al., 2017)

3.3. RFID set

RFID set consists of three parts which are RFID tag, RFID reader, and another Arduino board with GSM shieldThe RFID tag is always in the vehicle where the RFID reader will read it, it identifies the vehicleThe RFID reader will be deployed at certain known places on the road where cellular networks signals are guaranteed with high strengthThe RFID reader is attached to the Arduino board for reporting the read RFID tagsThe Arduino board is associated with GSM shield for reporting the read tags and location of the RFID reader as soon as it receives them through SMS. The distance between two readers will be a reasonable indicator of the vehicle's location

3.4. Security algorithm

The security algorithm is the one used to encrypt/decrypt the tracking informationWe realized that using an Arduino board, our choices will be limited to lightweight security algorithms due to the processing and memory limitations of Arduino. We adopted the SIT algorithm developed in (Usman et al., 2017) to be developed in the Arduino board. The algorithm helped to secure the transmitted information from the Arduino board to the software server.

4. System architecture

In this section, we explain how the system is constructed and tested. The main idea, shown in Fig. 3 and Fig. 4 is to construct a localization system based on the previous description. The implemented system consists of two main modules, the Sender and the Receiver.

4.1. Sender module

As can be seen in Fig. 3, the RFID tag is programmed to include a specific tag in the vehicle/train. Also, the board and the RFID readers are set to have the SIT security algorithm implemented on them. The distance between the boards is considered for different distances such as 1km, 2km, 4km, 6km, 8km, and 10km. the reason behind making such distances is to measure the performance of the overall system. In addition, SIM module is deployed on the board for sending and receiving messages.

Fig. 3: Hail railway suggested system

After initial testing, we noticed the following two problems:

1. Buffering problem: Since the system is based on the SIM messages, in certain areas, the cellular network was not available, or its signal was very week. Therefore, a buffering system is implemented on the Arduino board to keep the messages until the network is back. However, buffers are implemented to fit only five messages due to the limited board storage.
2. System overloading: During the initial testing, we noticed that sending a large number of messages overloads the system. Therefore, we had to limit the number of messages to be sent from the board to the receiver module. Also, we implemented a remote configuration to the sender part to set the allowed number of messages per hour. This requires the deployment of another SIM module on the receiver module.

The other part of the system, the receiver, has the following components:

- The receiver hardware
- The receiver software
- Content-Based filtering
- GUI module

As can be seen in Fig. 4, the first component of the receiver is the receiver hardware followed by the software for receiving the encrypted messages. The received message is decrypted and sent to the next component for content filtering and recognition. After all, the information is presented according to the interface requirements.

One of the problems faced during building the system is that the RFID tag size is 112 bits in addition to GPS information. Also, the GPS information could best fit in 8 bytes, 64 bits, storage. In addition, there is a GSM header that is mostly 23 Bytes of header data to be included in the message, shown in Fig. 5. This header will not be encrypted. Thus 112 bits plus the 64 bits will be the GSM payload and they will be encrypted using SIT algorithm. Therefore, the message to be sent from the Arduino board to the receiver would be divided in a chunk of 64 bits.

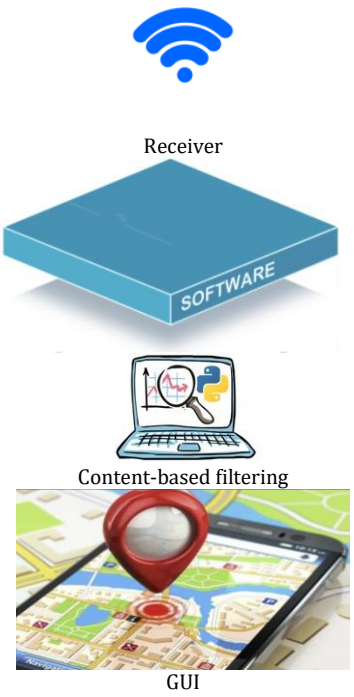

Fig. 4: Receiver module

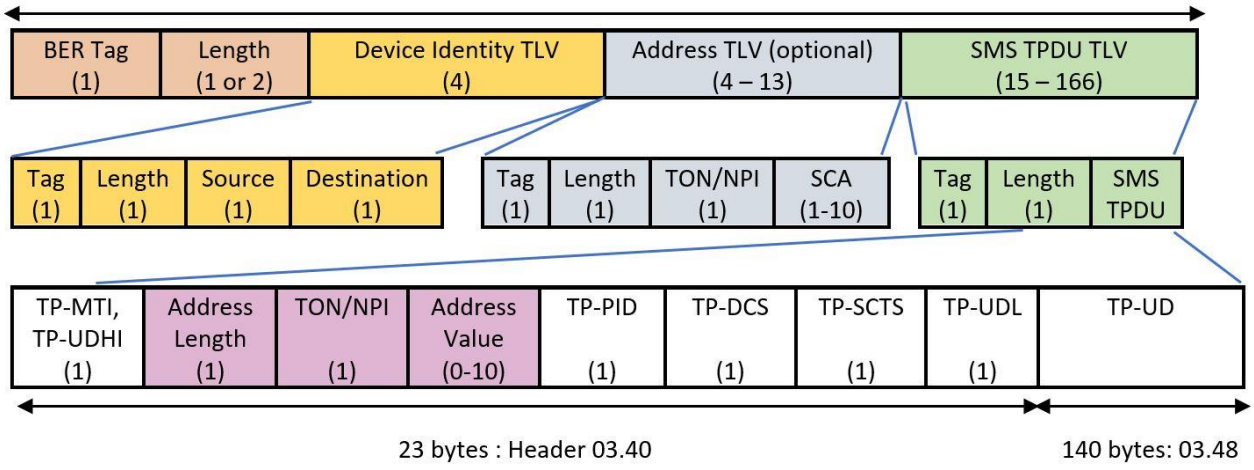

Fig. 5: GSM structure

5. Experimental results and discussion

In this section, we are not testing the security of SIT because it is already tested on its original paper, but we are testing its performance as well as the performance of the whole system. One of the important performance measures is the execution time, memory, and delay. SIT is implemented using C/C++ on the Arduino Uno board.

Compared to the previously implemented version of the SIT algorithm, we got better footprint in terms of memory and execution time. For instance, the execution time for the encryption and decryption were 0.122 ms and 0.156 ms, respectively in Core i7@3.7 GHz. In addition, the memory, surprisingly, 22 bytes which is almost the same number of bytes used by its original implementation. Therefore, our implementation to SIT is within the footprint of the previously implemented versions. Our implementation is comparable also to similar algorithms like AES, TEA, PRINCE, RC4, and IDEA in terms of the required memory and code size in which all of these algorithms work with 64 bits block size and different key sizes. Table 1 shows the comparison between such algorithms and our implementation to SIT. Table 2 shows a comparison between different ciphers.

The other part of the evaluation would be the overall system. Testing the overall system includes the RFID tags and reader, sending time, receiving time, and content-based filtering. The RFID reader was tested for 4 different speeds, as shown in Table 2, 50 mph, 75 mph, and 100 mph, 125 mph, and more than 125 mph.

Another important measure is the time used to encrypt and decrypt each message. We have to divide each message into 3 chunks of 64 bits. Therefore, the time used for encryption and decryption of a message could be as follows:

- Encryption time per message = 0.122 * 3 ms
- Decryption time per message = 0.156 * 3 ms

As can be seen, it is within what is considered a reasonable time.

Table 1: RAM and code size comparison

Algorithm	RAM	Code Size (byte)
AES	-	1570
TEA	24	648
PRINCE	24	1574
RC5	72	3288
IDEA	-	596
SIT	22	826
Our implementation	22	795

Table 2: Comparison between different ciphers

CIPHER	DEVICE	Block Size	Key Size	Code Size	RAM	Cycles (enc)	Cycles (dec)
AES	AVR	64	128	1570	-	2739	3579
HIGHT	AVR	64	128	5672	-	2964	2964
IDEA	AVR	64	80	596	-	2700	15393
KATAN	AVR	64	80	338	18	72063	88525
KLEIN	AVR	64	80	1268	18	6095	7658
TEA	AVR	64	128	648	24	7408	7539
PRINCE	AVR	64	128	1574	24	3253	3293
SKIPJACK	Power TOSSIM	64	80	5230	328	17390	-
RC5	Power TOSSIM	64	128	3288	72	70700	-
PRESENT	AVR	64	128	1000	18	11342	13599
SIT	**ATmega328**	**64**	**64**	**826**	**22**	**3006**	**2984**

Table 3: RFID speed and detection

Speed	Detection
50 mph	detected
75 mph	detected
100 mph	detected
125 mph	detected
More than 125 mph	Less detection

6. Conclusion

The problem of vehicles/trains tracking using GPS might not be efficient. We proposed a modified tracking system with RFID technology is included. Also, the tracking system without any security consideration could be easily hacked and controlled. In this paper, we proposed a complete system for vehicle tracking using GPS and RFID technology. The overall system is secured using a lightweight security algorithm with only five rounds. The system is tested, and the system problems were overcome.

Acknowledgement

This research was supported by Research Deanship, University of Hail, KSA.

Compliance with ethical standards

Conflict of interest

The authors declare that they have no conflict of interest.

References

Altunbasak H and Owen H (2007). An architectural framework for data link layer security with security inter-layering. In the 2007 IEEE SoutheastCon, IEEE, Richmond, USA: 607-614. https://doi.org/10.1109/SECON.2007.342975

Buttyan L and Csik L (2010). Security analysis of reliable transport layer protocols for wireless sensor networks. In the 8th IEEE International Conference on Pervasive Computing and Communications Workshops, IEEE, Mannheim, Germany: 419-424. https://doi.org/10.1109/PERCOMW.2010.5470633

Infanta J and Hemalatha M (2013). Enhancing building security with RFID and ZigBee. International Journal of Engineering and Technology, 5(1): 265-272.

Kamarulazizi K and Ismail DW (2010). Electronic toll collection system using passive RFID technology. Journal of Theoretical and Applied Information Technology, 22(2): 70-76.

Lee JH and Ernst T (2011). Security issues of IPv6 communications in cooperative intelligent transportation systems (poster). In the IEEE Vehicular Networking Conference, IEEE, Amsterdam, Netherlands: 284-290. https://doi.org/10.1109/VNC.2011.6117112

Lim TS, Sim SC, and Mansor MM (2009). RFID based attendance system. In the IEEE Symposium on Industrial Electronics and Applications, IEEE, Kuala Lumpur, Malaysia, 2: 778-782. https://doi.org/10.1109/ISIEA.2009.5356360

Mohandes M (2008). An RFID-based pilgrim identification system (A pilot study). In the 11th International Conference on Optimization of Electrical and Electronic Equipment, IEEE, Brasov, Romania: 107-112. https://doi.org/10.1109/OPTIM.2008.4602508

Padrón G, García C, Quesada-Arencibia A, Alayón F, and Pérez R (2014). Using massive vehicle positioning data to improve control and planning of public road transport. Sensors (Basel, Switzerland), 14(4): 7342-7358. https://doi.org/10.3390/s140407342 **PMid:24763212 PMCid:PMC4029661**

Radhamani G and Ramasamy K (2002). Security issues in WAP WTLS protocol. In the IEEE International Conference on Communications, Circuits and Systems and West Sino Expositions, IEEE, Chengdu, China, 1: 483-487. https://doi.org/10.1109/ICCCAS.2002.1180664

Ramadan RA (2009). Leveraging RFID technology for intelligent classroom. In the 4th International Design and Test Workshop, IEEE, Riyadh, Saudi Arabia: 1-6. https://doi.org/10.1109/IDT.2009.5404113

Salehi M, Sepahvand I, and Yarahmadi M (2014). TLCSBFL: A traffic lights control system based on fuzzy logic. International Journal of u-and e-Service, Science and Technology, 7(3): 27-

34.
https://doi.org/10.14257/ijunesst.2014.7.3.03

Ting-ting C (2012). Study of an underground-based cyclic timetable impact on arrangement for bus schedule reliability. In the International Conference on Information Management, Innovation Management and Industrial Engineering, IEEE, Sanya, China: 3: 503-506.
https://doi.org/10.1109/ICIII.2012.6340028

Usman M, Ahmed I, Aslam MI, Khan S, and Shah UA (2017). SIT: A lightweight encryption algorithm for secure internet of things. International Journal of Advanced Computer Science and Applications, 8(1): 402-411.
https://doi.org/10.14569/IJACSA.2017.080151