Vehicle Position And Break-Down Tracking Using Anonymous Signal Transmission Over A Secure Channel.

K. Megha Nandi Vardhini, Manjula Srinivas

Abstract— Tracking vehicles in a large vehicular network is a vital area of focus today. Departments like traffic regulation bodies, police authorities, and other government agencies are very interested in a service that can provide them with the live vehicle position information as that knowledge can be applied in various applications like criminal run out situations or traffic rule violation regulation and many others. But such information that has to be transmitted from the vehicle itself shall be reliable by being tamper proof and also not be available to anti-social elements as that instead of solving the situation spoils it.Thus we propose a system Anonymous Signal Transmission where both secrecy and reliability are merged to their optimum mixture by being pretty scalable to the size of the network.

Index Terms— Vehicle Tracking, Anonymous Beaconing, Crypto Application, Traffic violation regulation, Vehicular Networks, Vehicle Breakdown Tracking.

1 Introduction

VEHICLE tracking is a vital point of interest today. Various government agencies are interested in this kind of a service.

Situations like police department searching for a batch of culprits running away in a vehicle, Traffic department watching out for vehicles who break traffic rules and speed limits, or a situation where an ambulance stuck up in a traffic jam and many other to quote can be helped by providing a system that can keep track of the vehicles movement and position or geo-location.

For a system to keep track of the vehicle's position the most used and possible solution is to fit the vehicle with an arbitrary device that keeps sending some signal from that vehicle to a centralized tracking system and that signal shall encapsulate the vehicle's vehicle number and its geo-location over time.

The challenge in this kind of a system is majorly its reliability. As the device that we place if tampered then the vehicle will send information as guided by the driver and it leaves enough room to impersonate and makes it unreliable.

One more is that the signal transmitted from this device if attacked may give access to the driver's information to unauthorized users which compromises the driver's privacy and security.

- *K. Megha Nandi Vardhini, pursuing MTech (CSE), Vitam College Of Engineering, Anandapuram, Visakhapatnam, AP, India. PH: 9581062251, E-mail: nandu544@gmail.com*
- *Majula Srinivas, MTech (CSE), Assistant Professor, CSE Department, Vitam College Of Engineering,Anandapuram,Visakhapatnam, AP, India. PH:* 9490707850, E-mail: manjulasrinivas2005@gmail.com

And usage of any complicated cryptographic algorithm will lead to long time complication and this makes the information being unusable as it is no more live. Thus in this paper, we propose a novel vehicle data transmission protocol called the anonymous signal transmission.

The rest of the paper is organized as the section 2 speaks about background information, section 3 speaks about protocol and implementations, followed by experimental observations and simulation results in section 4, that followed by the conclusion and references sections.

2 Background Information

2.1 Vehicular Network

The term vehicular network means that a group of vehicles can communicate with one another and can forward that communication slot a designated server.

In this paper, we consider a network of devices called Road Side Units (RSU) established on either side of the road and that can communicate the data packets to a centralized server operated by a government agency called Local Authority (LA).

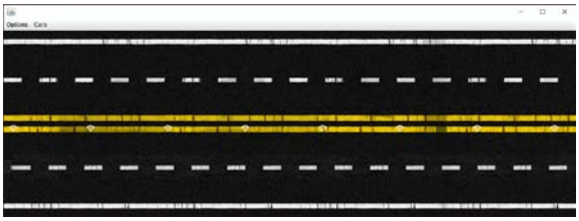

Fig. 1.Road and RSU's established

It is also considered that each vehicle is capable of sending signals wirelessly to these RSU's and these RSU's will, in turn, forward them to the LA.

2.2 The Signal Transmission

As per the consideration, the vehicle shall compose a signal and transmit to the RSU nearby. Or in the case of an RSU is not found in the transmission range, then that signal is received by another vehicle passing nearby and that forward to another RSU or another vehicle what so ever is found nearby. And thus the network is never broken, and no data packet is lost.

3 Anonymous Signal TraNsmission System

3.1 The Procedure

The proposed method of document is as follows

A. Vehicle Trip Registration Phase.
B. Vehicle Movement Tracking Phase.
C. Vehicle Trip Completion Phase.

3.2 Vehicle Trip Registration Phase.

This phase occurs every time a vehicle starts a new trip may it be short or long. As soon as the vehicle is about to start its trip, it has to register itself with the LA server. As a result of which the LA server receives a vehicle registration number and sends the vehicle with a secure one-time transmission key.

This transmission key is a tuple of three components, the secure random unique id assigned to that vehicle by the LA. This unique id is valid only for that trip and other two components are two random large prime numbers that serve as transmission encryption keys.

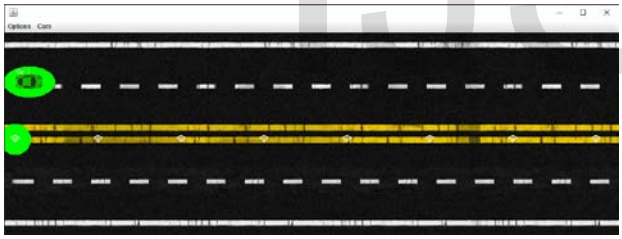

Fig. 2.Vehicle Registration Phase.

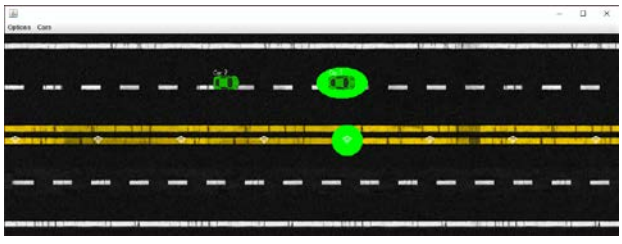

Fig. 3.Vehicle Signal Transmission.

3.3 The Vehicle Movement Tracking Phase

While the vehicle is in movement, it is bund to transmit a signal called the beacon after every fixed span of time period called time interval.

This beacon transmission if accomplishes vehicle original registration number, it will be vulnerable and it makes the drivers and vehicles privacy and security at risk.

Thus this signal is made anonymous. This means the vehicle registration id is not encapsulated in the beacon but, it contains the Unique Id sent to it by the LA at the time of registration. And to enable trustworthiness, the geolocation is encrypted by triple DES algorithm before encapsulating in the beacon using the key couple generated at the time of vehicle registration.

Such generated beacon is passed to the nearby RSU or another nearby passing vehicle. This signal will be ultimately routed to the LA. The LA retrieves the keys from the stored repository from the received UID and using those keys, the Triple DES is again applied to retrieve the signal encapsulated geo-location.

If in case any vehicle fails to transmit the signal within the expected time interval, then that vehicle is supposed to be a break -down.

3.4 Vehicle Trip Completion Phase

This phase is where the vehicle sends the trip to halt signal so that the server can deallocate the uids and can reuse them in providing any other vehicle registration.

3.5 Triple DES

Triple DES stands for **Triple Data Encryption Algorithm.** Is a cryptographic lightweight algorithm for an atmost symmetric cryptographic algorithm.

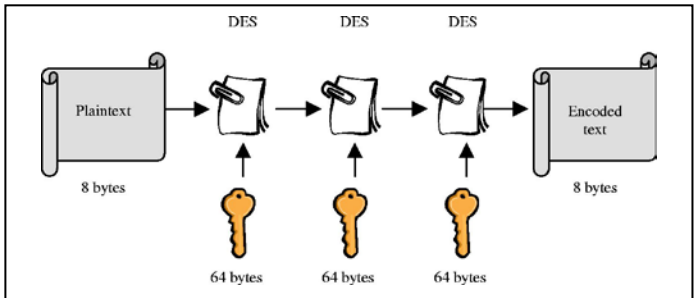

Fig. 4. DES Algorithm in short

The triple DES Encryption will happen as below:

1. The plaintext blocks are first encrypted using Single DES by key K1
2. This output is decrypted using Single DES by key K2
3. This output is again encrypted using Single DES by key K1.
4. This outputted cipher is final.

The triple DES Decryption will happen as below:

1. The plaintext blocks are first decrypted using Single DES by key K1
2. This output is encrypted using Single DES by key K2
3. This output is again decrypted using Single DES by key K1.

4 Results And Inferences

4.1 Conducted Experiment

We have implemented the above procedure using java swings and java networking procedure.

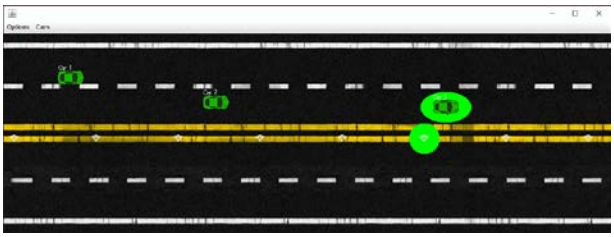

Fig. 5. Screen Showing Vehicle Movements

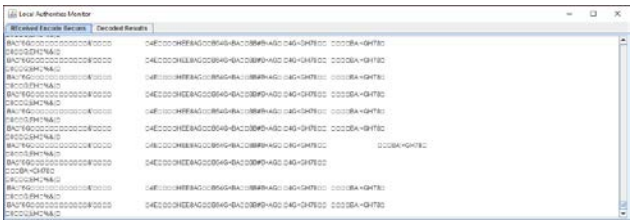

Fig. 6. Screen Showing Encrypted Beacons.

Fig. 7. Screen Showing Decrypted Beacons.

4.2 Graph depicting Time Complexity

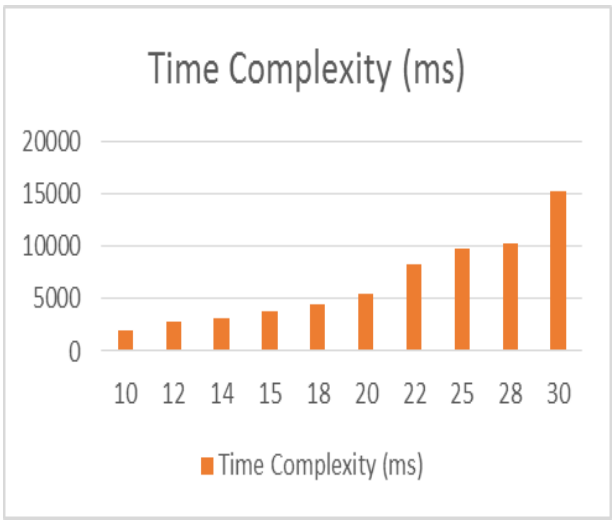

Fig. 8. Time Complexity

.

5 Conclusion

The vehicle tracking system is a very important service to various government agencies and this needs to be trustworthy, temper proofed and shall be transmitted in such a way that the drivers and vehicles information shall not suffer from privacy nd security risk.

As an attempt to design a protocol that is lightweight and secure we have designed a secure anonymous signal transmission system over a secure triple-DES algorithm channel and have implemented in a simulation environment and tested with varied vehicle count for time and security complexity.

References

[1] DSRC Message Set Dictionary, http://standards.sae.org/j2735_200911

[2] ETSI TS 102 637-2: Intelligent Transport Systems (ITS) .– Vehicular Communications .– Basic Set of Applications .– Part 2: Speci□cation of Cooperative Awareness Basic Service, 2011.

[3] Thales ISS, Thales, Jan. 2011 [Accessed July 2012].

[4] B. Wiedersheim et al., ."Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change Is not Enough," IEEE WONS, 2010. Kranjska Gora, Slovenia, 2010.

[5] E. Schoch, F. Kargl,"On the Ef□science of Secure Beaconing in VANETs," ACM WiSec, 2010. 111-116

[6] IEEE 1609.2 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, 2006.

[7] W. Dif□e, M. Hellman,"Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, vol. 67, no. 3, pp. 397.– 427, Mar. 1979.

[8] M. Röckl, K. Frank, T. Strang, M. Kranz, J. Gacnik, J. Schomerus,"Hybrid Fusion Approach combining Autonomous and Cooperative Detection and Ranging methods for Situation-aware Driver Assistance Systems," IEEE PIMRC, 2008.

[9] J. Eriksson, S. Krishnamurthy, M. Faloutsos,"TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks," IEEE ICNP, 2006.