Smartphone based Vehicle Tracking and Control via Secured Wireless Networks

Rajesh Borade
Department of computer engineering
Sinhgad college of engineering

Aniket Kapse
Department of computer engineering
Sinhgad college of engineering

Prasad Bidwai
Department of computer engineering
Sinhgad college of engineering

Priya Kaul
Department of computer engineering
Sinhgad college of engineering

ABSTRACT
Nowadays, automobile thefts are increasing at an alarming rate all over the world. Security of their vehicle has always been a concern to people. We are developing secured vehicle tracking and control system. In this system the user will be able to control his vehicle through an android based Smartphone. A secured mode of communication between Smartphone and vehicle is established via GSM network. Using his/her Smartphone, the owner will be able to lock/unlock the vehicle and track the vehicle in case of theft. If the GSM network is not available momentarily, a secured Bluetooth channel will be used instead. The project will be helpful in digitization of documents of Regional Transport Office.

General Terms
Regional Transport Office (RTO).

Keywords
Android, Global System for Mobile (GSM), Data Encryption Standard (DES), Subscriber Identity Module (SIM), Global Positioning System (GPS)

1. INTRODUCTION
Vehicles are expensive. Other than a house, perhaps, few purchases we make will be worth a new vehicle. And just like any other expensive asset, a vehicle brings with it a secondary cost, the risk of theft. In some laid-back parts of the world, locking the doors may be enough to ward off the threat. Everywhere else, it's a good idea to arm yourself, and your vehicle, with some security. To prevent theft, most of the vehicle owners have started using the theft control systems. The commercially available anti-theft systems have distance and security limitations. They are not portable and highly reliable. With our system, one can manage his/her vehicle via an application on a Smartphone. She/he can lock/unlock the vehicle remotely. However, if the vehicle security is still breached, the owner will be notified and he can track the current location of the vehicle.

2. OVERVIEW
There are two wireless modes of operation [6] that have been proposed for this system, Network mode and Bluetooth [7] mode. The communication between Owner's Smartphone and vehicle will be established in network mode i.e. GSM mode [2]. If GSM network is not available then automatically the system will switch to Bluetooth mode. The whole system will communicate using triple DES [1] [8] algorithm for security.

3. RELATED WORK
Triple DES uses three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits), for encryption. [1]

We can use a Smartphone to control and access a vehicle. [2] Vehicle can be protected from theft by enabling a password mechanism which prevents unauthorized access and user can be informed about the status of the vehicle. [3]

Bluetooth can be used as a short-ranged mode of communication to control the vehicle and a security algorithm can be enforced for security.[5]

The various kinds of threats to communication in Bluetooth mode which should be prevented in order to ensure secured communication as Bluetooth is an insured mean of communication which has been overcome through the security algorithm [5].

Secured communication can be used in wireless networks such as Bluetooth. [6]

4. PROPOSED SYSTEM
Following are the major components of our system:

- Server side application running on a cloud
- Database on a cloud.
- Smartphone application for the owner
- Vehicle side module
- Use of a secured communication[10] protocol which will be the most suitable among the existing security algorithms for both Network and Bluetooth mode

The proposed system is going to use the concept of cloud computing for the scalability of performance. Smartphone application on the owner side would be developed on Android. On the vehicle side, we are going to use another Smartphone as the simulation device simulating the system containing integrated GSM, GPS and SIM modules. Cloud database will result in digitization of RTO documents which will be beneficial as it will be easier to maintain records.

The proposed system is going to use Triple DES algorithm [1] [8] for encryption of control and data signals. In the Bluetooth mode, a method of key exchange algorithm will be used [4]. There are various threats to the Bluetooth communication [5] [7]. Hence, Triple DES algorithm and key exchange algorithm protects the system from these threats.

Using this system the owner can put ignition lock to the vehicle by simply disabling the internal circuit remotely. He will also be able lock or unlock the doors of his vehicle and track his vehicle anytime to ensure safety.

The overall system flow is as shown below:

1. Owner buys a vehicle with our system installed in it.
2. RTO officials make entries to the database
3. Authentication information is given to the owner
4. Authentication will be done:
   I. when GSM network is not available
   II. when GSM network is available
5. Control actions will be performed on the vehicle

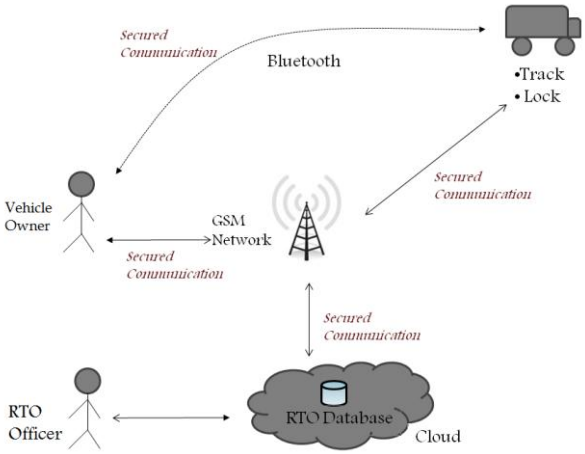


Fig. 1: Overall operation of the system

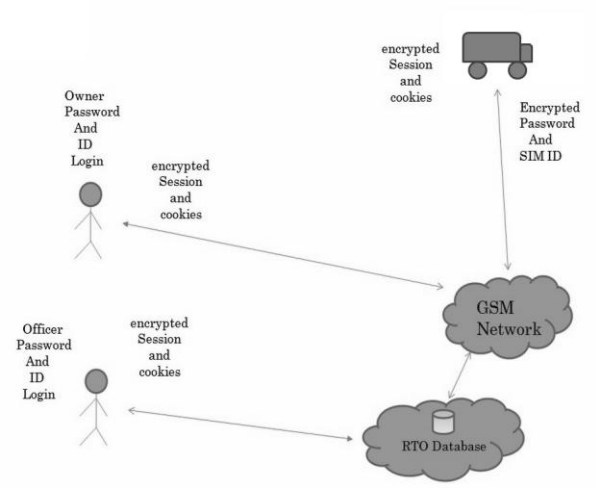


Fig. 2: Network mode operation

In fig. 1 the basic working of the system has been shown in two given modes of operation i.e. Bluetooth and GSM. The given fig. shows the communication between vehicle and owner.

In fig. 2 the communication between owner and vehicle is shown in network mode through secured path. In order to authenticate the user the database is used where the entry of user along with its vehicle is stored.

In fig. 3 the communication between owner and vehicle is shown in Bluetooth mode through secured path. In order to authenticate the user the database is used where the entry of user along with its vehicle is stored. The communication is made secured using Triple DES algorithm.

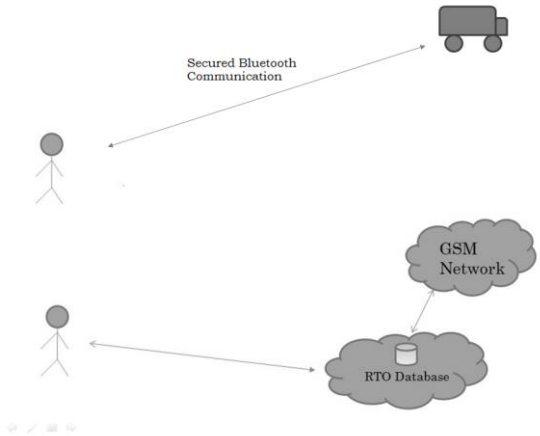


Fig. 3: Bluetooth mode operation

4.1 Comparison with existing techniques

- **Cost Effectiveness**: Todays existing security systems in most parts of the world aren't provided in ordinary vehicles. For such vehicles our system can be installed at a very low price.
- **Portable:** In our system**,** the application used to control the vehicle can be installed on any smartphone.
- **Range:** Since it is a GSM based technology, there is no range limitation unlike most other security systems which do not provide such facility
- **Future Scope:** Creation of a huge vehicle database and maintaining the location information and result in an effective fleet control or traffic management system.

5. MATHEMATICAL MODEL

Let us consider **S** as a system for Secured Vehicle Management.

S= {…

1. Identified Inputs

I= {I_1, I_2, I_3 ,……., I_n| 'I' instructions given by the user}
K= {K_1, K_2, K_3,……., K_n |'K' key used for encryption}
U= {U_1, U_2, U_3,…, U_n |'U' username for the module}
P= {P_1, P_2, P_3,……., P_n |'P' password to authenticate}
V= {P_1, P_2,……, V_n |'V' vehicle identifier for vehicle}

2. Functions performed

F={ authenticate(), lock(), unlock(), track(), update(), delete(), notify(), pair(), intiate(), encrypt(), decrypt() }

Some functions are shown as follows:

F1(authenticate(U,P)) = A'

A'= {d |'d' contains the information about success/failure of login}

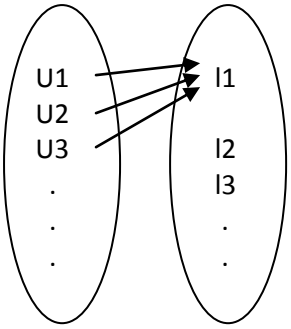


Fig. 4(A): Authenticate function mapping

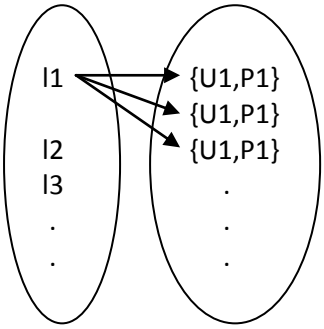
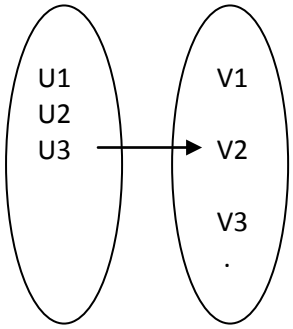


Fig. 4(B): Authenticate function mapping

F4(lock())=L'

L'= {d |'d' contains the information about success/failure of locking}



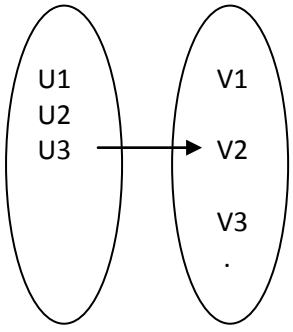


Fig. 5(A): Lock function mapping

F6(track()) = T'

T'= {d |'d' contains the coordinates of the location of the vehicle}

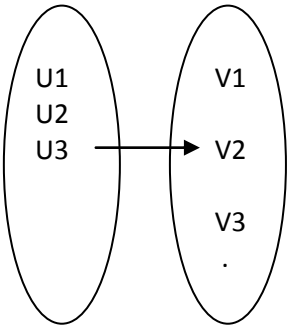


Fig. 5(B): Track function mapping

3. Output

O= {O_1, O_2, O_3…, O_n |'O' operations performed by the system}

The final system S will comprise of:

S= {I, K, U, P, O, V, A, L, U, T, PR, IN, E, DP, C, UP, D, N ...}

6. SECURITY ALGORITHM

In both modes for encryption the proposed system is going to use Triple DES algorithm [1] [8]. The high level description of this security algorithm is as:

Triple DES uses a "key bundle" which comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits).

The encryption algorithm is:

Cipher text = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$

i.e., DES encrypt with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.

Decryption is the reverse:

plaintext = $D_{K1}(E_{K2}(D_{K3}(\text{cipher text})))$

i.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.

Each triple encryption encrypts one block of 64 bits of data.

7. CONCLUSION

Thus, a system has been proposed which can effectively perform various control actions on the remote vehicle. Operations such as ignition lock, door lock can be performed remotely and securely to ensure safety. As this is being done over the GSM network there are no range limitations involved. The same operation can be performed from a short range in case of network failure using Bluetooth. The enforced security algorithm for Bluetooth makes it impossible to breach. Additionally, theft alert and dynamic location information is also provided to the vehicle owner if intrusion takes place. All the above functions are performed using a Smartphone which makes the system portable and more convenient and facilitates ease of use. Digitization of records provides efficient management for the authorities unlike the traditional paper work which is still being followed. With

such a system people can govern their vehicles with and improved accessibility and less active involvement. Such a system with high security measures, cost effectiveness and easy operability, vehicle theft rates can thus be reduced significantly.

8. ACKNOWLEDGMENT

The authors would like to thank Prof. G. T. Chavan, assistant professor, Sinhgad College of Engineering for his valuable support and guidance for the development of the project.

9. REFERENCES

[1] "Triple Data Encryption Standard", Published By Federal NIST Special Publication 800-67, Revised January 2012

[2] Amol S. Dhotre, Abhishek S. Chandurkar & S. S. Jadhav, Dept. of Electronics Engineering, Govidrao Wanjari College of Engineering, Nagpur, India, "Design Of A Gsm Cell – Phone Based Vehicle Monitoring & Theft Security System", International Journal of Electrical and Electronics Engineering (IJEEE), 2012

[3] Jayanta Kumar Pany1 & R. N. Das Choudhury, Dept. of Electronics and Communication Engineering, Raajdhani Engineering College, BPUT, Odisha, India, Dept. of Electronics and Instrumentation Engineering. ITER, SOA University, Odisha, India, "Embedded Automobile Engine Locking System Using Gsm Technology", International Journal of Instrumentation, Control and Automation (IJICA) ISSN, 2011

[4] "System And Method For Exchanging Encryption Keys Between A Mobile Device And A Peripheral Device", US Patent, US 2011/0280401 A1, November 17 2011

[5] "Studying Bluetooth Malware Propagation", Published By The IEEE Computer Society, 2007

[6] "In-Vehicle Secure Wireless Personal Area Network", Published By The IEEE, 2006, IEEE Transactions On Vehicular Technology, Vol. 55, No. 3, May 2006

[7] "Bluetooth: Technology For Short-Range Wireless Apps", Published By The IEEE Computer Society, 2001, IEEE Internet Computing, May-June 2001

[8] "Data Encryption Standard (DES)", Published By Federal Information Processing Standards, Publication, October 1999

[9] "Advanced Encryption Standard", Published By Federal Information Processing Standards Publication, November 26, 2001, First Published 1998

[10] "How You Can Use The Data Encryption Algorithm To Encrypt Your Files And Database", Published By Roy F. Van Buren Cpa Cisa , 1990