Military Technical College
Kobry El-Kobbah,
Cairo, Egypt.

15th International Conference on Applied Mechanics and Mechanical Engineering.

INTEGRATION OF CAR SECURITY LEVELS USING TRANSPONDER KEY: DOUBLE IDENTIFICATION CAR CODE

M. N. Tawfeek*, S. Shedid*, I. El-Sherif* and Y. Hendawy**

ABSTRACT

One of the main problems in the field of transportation is the diversity of the concepts of vehicle security that has been lately elaborated under continuous threat of technology spreading in a very chaotic manner, issue that opposes many obstacles when evaluating the security measure of such technique on the ground, especially when dealing with very important person (VIP) security, and its constrains. This paper aims to develop a scientific approach to integrate three levels of car security namely life saving, car theft prevention and user access security with respect to current technologies. Novel double identification code applications are introduced. The introduced applications use the traditional radio frequency car key considering Actual threats and limited budget using novel methodologies. They enhance the fixed code key security to achieve the security level of rolling code key. Experimental work has been carried out using the two standard car communication frequencies namely 315MHz and 433.9MHz simultaneously to transmit two different fixed car codes with a spatial frequency separation.

KEY WORDS

Car Security, VIP Security, Spatial Frequency, Fixed Code, Double Identification Code Key, Passive Keyless Entry, Immobilizer Systems, Hopping Frequency.

---

* Egyptian Armed Forces.
** Professor, High Institute of Technology, 10th of Ramadan city, Egypt.

INTRODUCTION

The automotive industry develops several security systems to prevent car theft relative to the car class, price and expected threats. Since there is no official standard for the theft determent systems around the world, greater challenge comes from professional thieves.

Unfortunately the higher is the security measure, the higher is the cost. Issue that handicap the car manufactures specially when developing economic class cars to compete on a global level.

Another challenge facing the automotive market is the security of VIP cars. On the one hand the theft threat is travail because the car is always guarded on the other hand cost is not considered when dealing with VIP car security but access roles of the VIP cars is the issue.

This paper objective is to define, classify car security levels and the integration between them and developing new security tools without remarkable increase in the cost. One can classify car security approaches from a wide scope into three levels.

The first approach is life saving and personal security which aim to soles protection regardless the needed cost concerning the security of very important persons. For this approach we must consider some security measures. We can summarize these measures into main categories, passive measures including shielding, night vision navigation, camouflage paint, theft belt, driver isolation screen and active measure including active armors ,active camouflage, active jamming ,artificial fog, active night vision navigation, self-inflation tires, anti-laser electro-croma mirrors and screens, air bags, active theft belt and oxygen supply.

The second approach is car theft prevention that deals with the car security taking into consideration the class of the vehicle and appropriate budget to achieve the security in need. Also it can be summarized into two main categories passive measures and active measures. Passive measures includes outer body parts design security like non standard tools, inner fixing aides, dummy parts hidden bolts and intrusion security like traditional mechanical locks, electromechanical fixed code locks and finally the inner security like steering stick lock, gear box lock, brake pedal lock electrical battery switch and ignition lock. Active measures includes outer bodies parts design security like proximity detector alarm, vibration alarm, intrusion security like electromechanical rolling code locks, and finally the inner security like electric intrusion alarm with silent GMs, SOS alarm, biometry alarm(face recognition and finger print).

The third approach is the car access control, where conditions to use the vehicle previously determined by the car owner. It can be summarized into two main categories passive measures and active measures. Passive measures includes separated intrusion and ignition keys, fuel intake throttling for maximum speed control tented rear glass owner disclaimer private number pretend outside the vehicle self adjusting car compartment key(multi user key setting) and passive trip analyzer. Active measures like GSM remote ignition and interruption, GSM tracking and AVI tracking.

MULI-FREQUENCY AUTOMOTIVE KEY THEORY

There are three distinct types of transponder car key systems [1, 2]. The single identification (fixed) code, the challenging response encrypted code and the rolling code. The single identification code is the simpler and cost effective one. It uses an alphanumeric combination of digits assigned to a particular vehicle but it achieves the lowest security level of them all. To make use of the benefits of the fixed code with a higher level of security a novel application using frequency manipulation is introduced. It is based on establishing the communication between the car lock and the car key using two fixed codes on two different frequencies simultaneously. Each frequency carries a simple identification (fixed) code.
For the traditional fixed identification code that uses "M" digits out of "N" digits codebook, the all possible code combinations "X" can be calculated as:

$$X = N^M \tag{1}$$

The probability "P" to find the correct car code by the intruder:

$$P = 1/X = 1/N^M \tag{2}$$

By using the introduced double identification method, we can recalculate the probability "P" as follows:

For the first carrier frequency F_1,

$$X_1 = N_1^{M_1} \tag{3}$$

$$P_1 = 1/X_1 \tag{4}$$

For the second carrier frequency F_2,

$$X_2 = N_2^{M_2} \tag{5}$$

$$P_2 = 1/X_2 \tag{6}$$

For the intruder, the probability "P' " to find the correct key is:

$$P' = P_1 * P_2 = 1/(X_1 * X_2) \tag{7}$$

Equation (7) shows that, using the proposed double identification method cause a significant reduction in the probability to find the correct car code rather than that for the simple identification method given at equation (2). This result shows that the double identification method achieves a higher level of security than that of the simple identification method.

Actually the probability reduction is not the only benefit gained. The proposed double identification method uses two different spatially separated frequencies; hence the intruder is forced to intercept two different frequencies simultaneously. Such interception process may be considered more complicated than that required for the simple identification code.

PROPOSED IMPLEMENTION ARCHITECTURE FOR DOUBLE IDENTIFICATION METHOD

Synchronous Transmission of Double Identification Fixed Code

In this architecture, two transmitters with two standard frequencies (315 MHz and 433.9 MHz) [1] and two fixed code encoders are embedded in one key package. When triggering the car key kit, a dual simultaneous transmission will be carried out. The spatial frequency separation between the two carrier frequencies allows simultaneous transmission with minimum interference; hence, the signal to noise ratio (SNR) at the receiver front-end shall be sufficient to correctly receiving the two identification codes.

At the receiver front-end, two receivers tuned at 315 MHz and 433.9 MHz shall be equipped to receive each code individually. Each code shall be decoded and compared to pre-stored codes A and B; the decision to unlock the car shall be made when the two codes are correct. The details for the proposed Simultaneous transmission of double identification fixed code method illustrated in Figure 1.

Dual Code Access Control Using Double Identification Fixed Code

For VIP cars, another Authentication method is required. The VIP cars are not susceptible for theft as it is always being guarded. Allowing access to the car for one person like the driver is not recommended since this may offer a chance for betrayal. So a dual authentication method should be used instead. For this reason, a dual key access control using double identification fixed code method is introduced. In this method, the presence of two authorized persons instead of one is necessary to gain access to the car. Each person has an authorization fixed code key which cannot be used solely to gain access to the car. Two receivers at the car are equipped to unlock the car only when the two authentication codes are received correctly within a short period of time which can be adjusted. Once this is done, the presence of two persons, the driver and the security guard (for example) at the same time is a must. This will help preventing any attempts to violate the indoor privacy of VIP car cabinet. The details of the proposed architecture are illustrated in Figure 2.

Asynchronized Transmission of Double Identification Fixed Code

Asynchronous transmission accomplished by integrating a timer to the embedded key package will be discussed. This timer will act as a time separator for the two transmissions with a predefined time duration adjusted in both transmitter and receiver. The receiver shall accept the first received code and increments the timer. The second code shall not be accepted unless it was received at the correct time interval. This scheme is intended to reduce the chance for the intruder to unlock the system even if he has intercepted the two fixed codes. The intruder shall be forced to know the predefined time duration to be able to unlock the system. The proposed method is illustrated in Figure 3.

For VIP cars, synchronized transmission can be used on two separated keys that τ is in the order of seconds giving a time window for the driver to activate the lock after the security guard authorization fig.5, fig.6.

RESULT AND ANALYSIS

This technique acquires both the benefit of the rolling codes lock high security without a significant increase in security budget. Further, the applied approach can be considered a novel approach thus the usage of two different standard frequencies making the fixed code lock to achieve the order of rolling codes lock by using frequency hopping technique in car theft prevention. The concept of condition and limited the car access entry using to access simultaneous or synchronized keys in integration with the DVR alarm lock control has proven its efficiency in Order to prevent illegal breakthrough, illegal access, illegal usage of the vehicle and avoiding bobby traps and bugging operation using a modest budget.

CONCLUTION AND FUTURE WORK

A novel approach technique has been applied cheap electronic technique systems to increase cars security in addition achieve economic model, then enhancing the level of fixed security code to be better than the rolling code from security point of view using frequency hopping system, and without increasing cars budget. In addition securing very important person from sabotage, this by exchange the ordinary opening system to the dual opening system, including the driver and the guard.

This approach (radio frequency identification) can be mixed with video recording systems technique to achieve maximum security benefit to users. From this approach one can separate the meaning of cars security from inside car, outside car, and the passenger safety.

REFERENCES

[1] Car security: remote keyless "entry and go", Jarno van de Moosdijk, http://www. Jarno.vandemoosdijk@os3.nl, dick.visseroos3.nl, Jun 2009. Revision 232, compiled at sun Jul, 2009.
[2] Car keys, a guide to car keys and remote controls. Car keys electronic transponder keys and remote control the AA.
[3] RF Design Consideration for Passive Entry Systems, Paul Lepek, Paul Hartanto. http://www.atml.com
[4] EM microelectronic "expertise in Automotive". http://www.emmicroelectronic.com
[5] Estimation of low frequency coverage inside car for passive access system entry A. Takacs, M. Huard, S. kessler, G. A. Chakam and E. Iardjane, ELECTRONICS LETTERS 4th June 2009.
[6] Rfid security, Gianluigi Me, Giuseppe F. Italiano, DISP, Universita deli studi de Roma "Tor Vergata".
[7] Anti theft systems, Robert F. Mangine.
[8] The problem of auto theft, Mikel Longman.
[9] An Automotive Security System for Anti-Theft, Huaqun Gu, H. S. Cheng, Y. D. Wu Institute for infocomm Research, Department of Electrical & Computer Engineering, National University of Singapore. School of Computer Engineering, Nanyang Technological University.

[10] Transponder key technology. http://www.wikipedia.transponder key technology.
[11] Keeloq Hcs4xx transponder/Encoder family. http://www.microshiptechnology.com
[12] An open Approach for designing secure Electronic immobilizers, Kerstin lemake.
[13] RFID system and security and privacy Implications, Sanjay E.sarma, Stephen A. Weis, and Daniel W.Engles Auto-ID center, Massachusetts Institute of Technology Cambridge, MA 0139. http://www.autoidcenter.org. Springer-verlag Berlin Heidelberg 2003.
[14] A New Embedded Car Theft Detection System, Zhixiong liu, School of Electrical Engineering Wuhan University, china.zxliu@whu.edu.cn
[15] Anti theft protection: Electronic Immobilizers, Kerstin lemake, Ahmed-Reza Sadeghi, and Christian stuble, Horst Gortz Institute for IT security, Ruhr University Bochum, Germany. {Lemake, sadeghi, stueble}@crypto.rub.de
[16] Digital signature transponder Ulrich Kaiser, Texas Instruments Deutschland Gmbh, 85350 freising, Germany p.kitsos.y.zhang (eds) Rfid security, techniques Protocols and sys.on.chip design Springer science 2008.
[17] Analysis of Attacks against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs, Ansaf Ibrahim Alrabady and syed Masud Mahmud, Member, IEEE. Authorized licensed used limited to McMaster University, 2005 IEEE.
[18] METHOD OF PREVENTING CAR THEFTS Cross Reference to related application Aug.9, 2000.

FIGURES AND TABLES

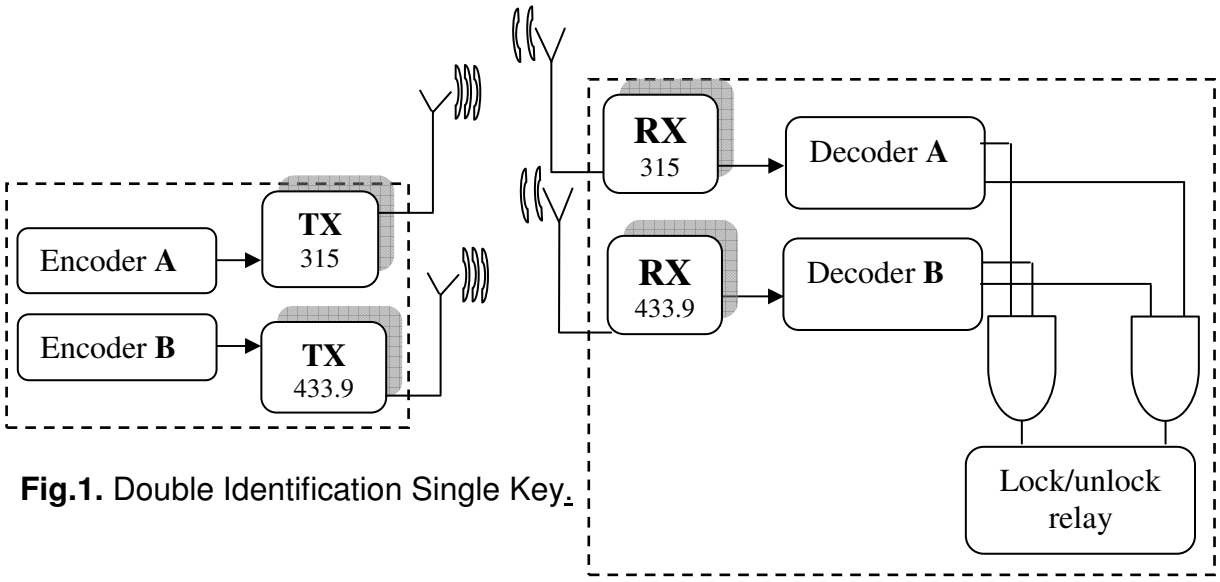

Fig.1. Double Identification Single Key.

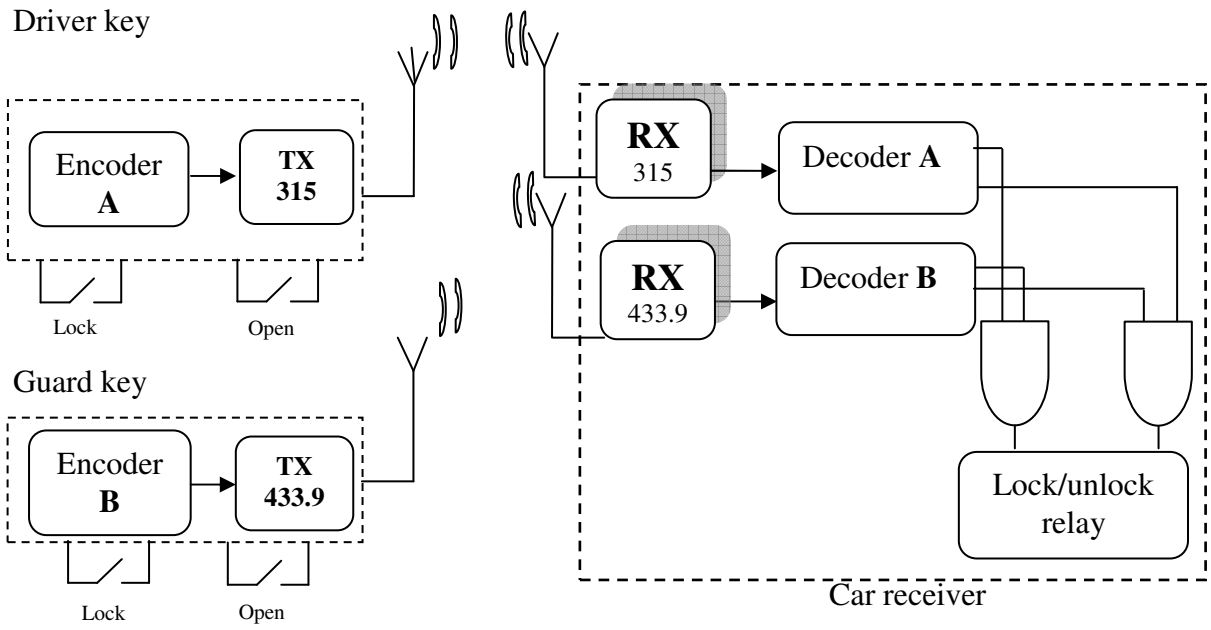

Fig.2. Double identification dual key.

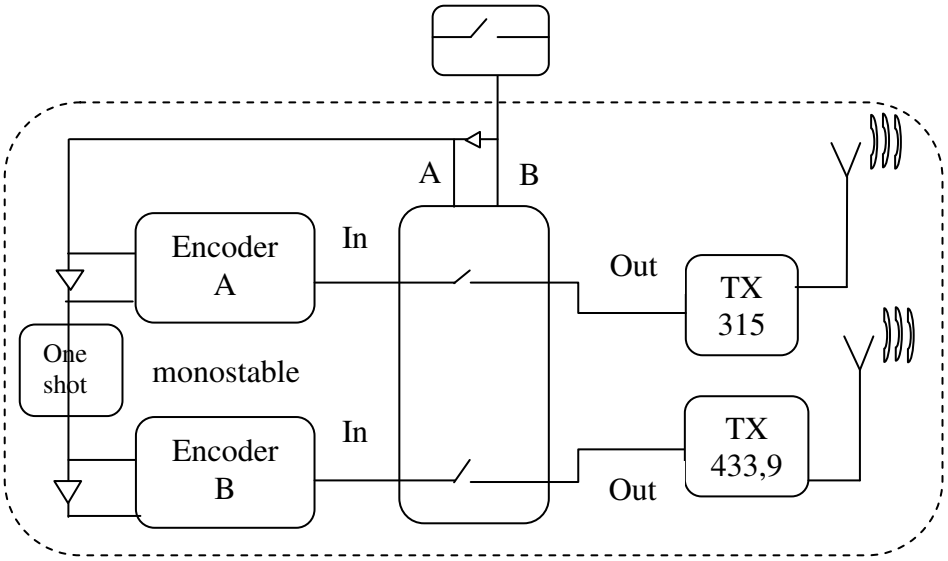

Fig.3. Synchronized transmission of double identification fixed code single key transmitter.

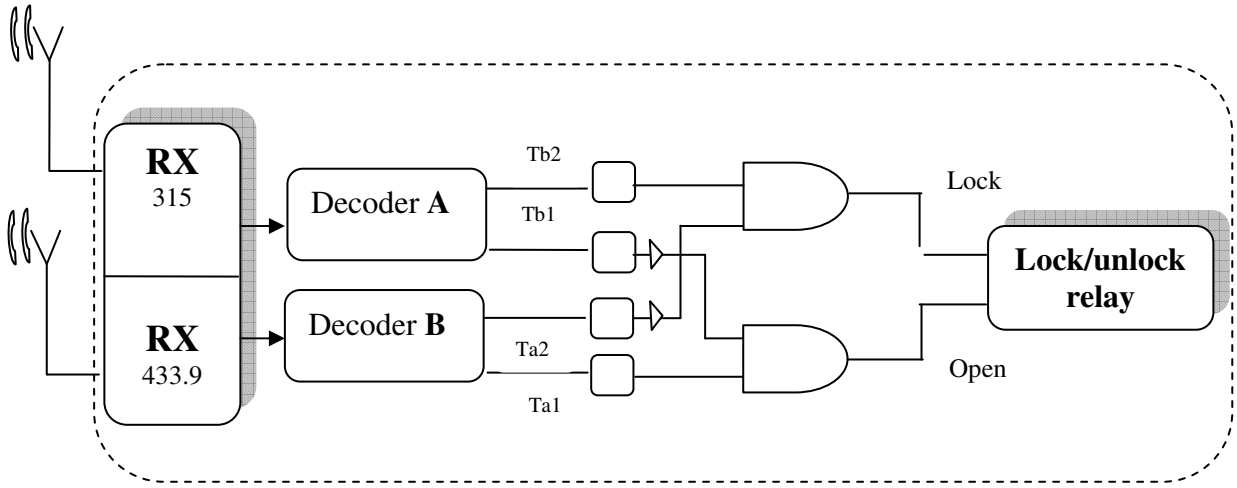

Fig. 4. Synchronized transmission of double identification fixed code single key receiver.

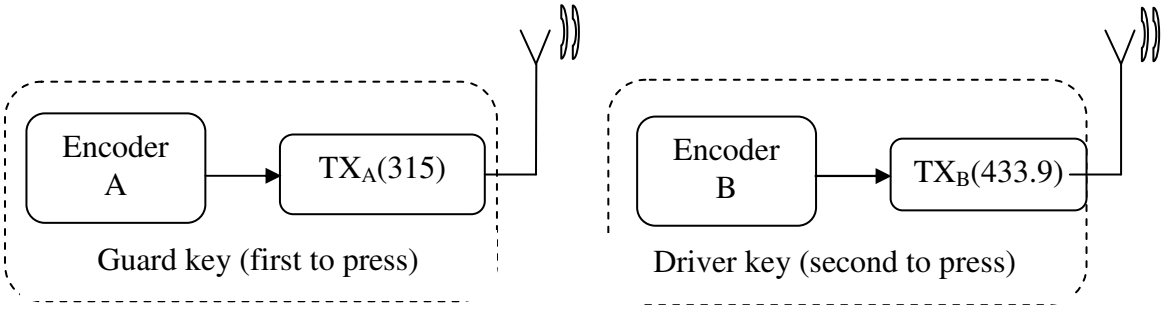

Fig. 5. Synchronized transmission of double identification fixed code dual key TX.

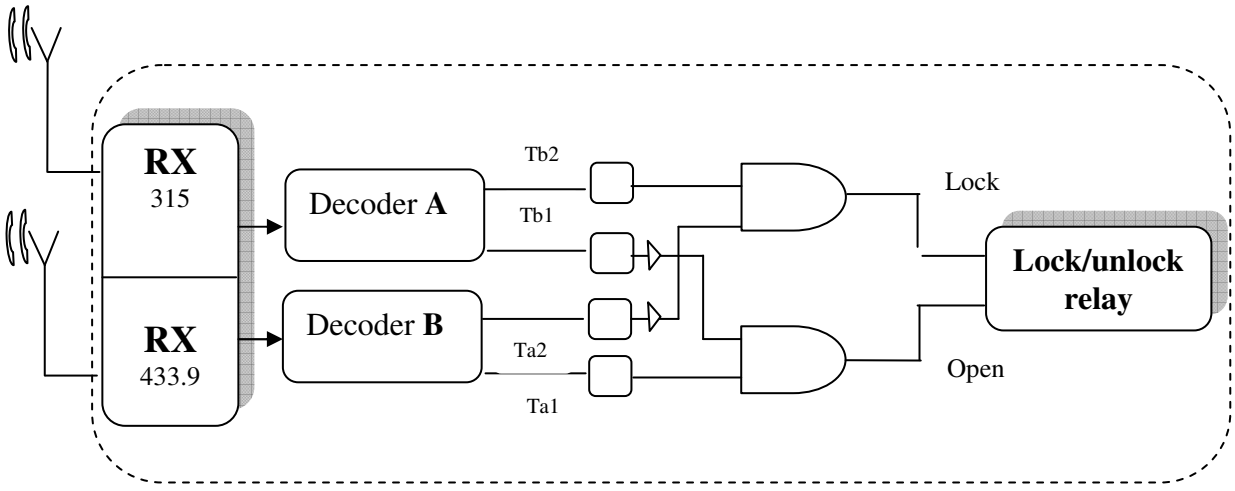

Fig. 6. Synchronized transmission of double identification fixed code dual key RX.

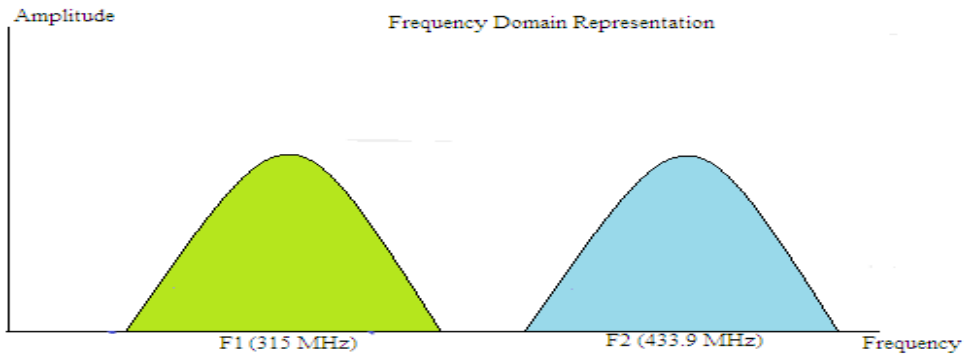

Fig. 7. Frequancey domain for the two transmitted signal (315MHz and 433.9MHz).

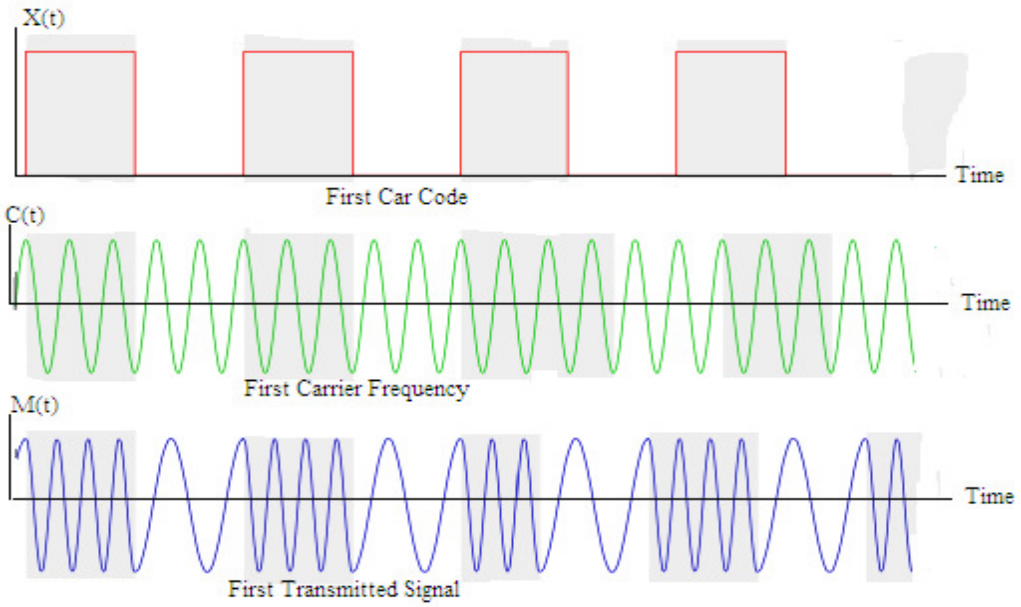

Fig. 8. Time domain for the transmitted signal**.**