IJCES International Journal of Computer Engineering Science , Volume1 Issue 3, December 2011
ISSN : 2250:3439
https://sites.google.com/site/ijcesjournal
http://www.ijces.com/

Secure Control of Remote Electrical Devices Using Mobile SMS Services

Kishor T. Mane[1], G.A. Patil[2]
1. Asst. Professor, 2. Head and Asst. Professor
D. Y. Patil college of Engg. & Tech. Kolhapur, Maharashtra, India
1. kishormane1@yahoo.co.in, 2. gasunikita@yahoo.com

Abstract— In this paper an attempt is made to extend the capability of mobile phones for secure control of remote electrical devices using SMS services. The transmission of SMS in GSM network is not secure. It only provides the encryption between Mobile Station to Base Station Controller. The message transmitted between GSM operator networks is not encrypted and hence is not safe. Mobile SMS service has been used for control purposes in various applications; but the control operations seem not to be secured. Therefore, it is desirable to secure SMS by adding suitable cryptographic algorithm so as to perform operations securely on certain crucial remote devices.

In this system blowfish algorithm has been enhanced for its suitability to increase the security on the parameters like Avalanche effect, GA, key-size, and others. The results obtained are far better in above terms.

Keywords— SMS, GSM network, electrical device, encryption, control.

1. INTRODUCTION

Today, mobile phones are integral part of our daily lives. Due to widespread growth of wireless network and drastic reduction in call rates and handset cost, the mobile usage has percolated to all sections of the society from business magnets to skilled laborers like carpenters, masons and even dabbawalas. Millions of people all over the world are familiar with the way of usage of mobile and their services provided like music tones, capture and send images, MMS, MP3 player, Internet browsing, downloading songs, etc.

Many systems have been developed to control and operate home appliances using wireless technology. Also, systems to control remote devices exists in many specific areas like chemical industries, satellite communication systems, etc. However, this paper highlights on controlling electrical devices through the most common mechanism of SMS services provided by mobile technology, that too in a secured way.

Sending SMS over the GSM network is not secure because GSM network does not provide end-to-end encryption. The encryption is provided only between the Mobile Station and Base Transceiver Station (BTS) using the A5 algorithm. The SMS message that traverses in between the operator networks is in plaintext format. If the attacker gets an access to the BTS or other parts of GSM network, then it is easy for tapping. Since the SMS messages stored on MSC (Mobile Switching Center) are in plaintext format, operator can always read all sent messages. The attacker can tap a message and also send fake SMS. Nowadays one can send SMS with arbitrary phone number of sender. It is possible to prepay this service on certain websites [8]. To avoid this, the additional facility of encrypting the message is desired to provide end-to-end security.

The system developed to provide end-to-end message encryption can be used not only for controlling electrical devices but, can be applied to other common applications which are based on message transfers using mobile SMS services. It also provides authentication and secure message transfer between two wireless endpoints.

2. LITERATURE REVIEW

In the past, different systems have been designed for controlling electrical devices. A system for controlling the devices especially for blind or handicapped people exists [1]. The algorithm is developed to generate text message from spoken commands of user by extracting features like cepstal coefficient, short-time energy and zero-crossing rates. A multi-layer feed-forward neural network is used for recognition of suitable words. The derived text message is then sent as SMS to the mobile connected to the control system through PC. On receiving SMS, the system responds by activating appropriate ports. But, the limitation of this system is that it cannot be controlled from remote places.

An Internet application has been developed that allows local, remote monitoring and control of home appliances [2]. A fast and secure algorithm designed and proposed by Paul A. J. et. al. [6], use symmetric key algorithm which operates on block of size 128 bits and key size 128 bits.

The limitations of existing systems used for control purposes are as under:

a) Devices cannot be controlled from remote location.
b) Insecure GSM network.
c) Requirement of PC for sender to convert voice to text [1].
d) Systems are for specific purposes.
e) Cost involved in such systems is high.

Present work overcomes some of the above limitations. Blowfish algorithm has been used in many commercial applications for security purposes due to its more promising features like memory size, variable key-size and its robustness. However, Brute-force attack has been tried till 4-rounds of Blowfish algorithm. Therefore, there is a need to enhance the complexity where the present work emphasizes on.

3. SYSTEM ARCHITECTURE

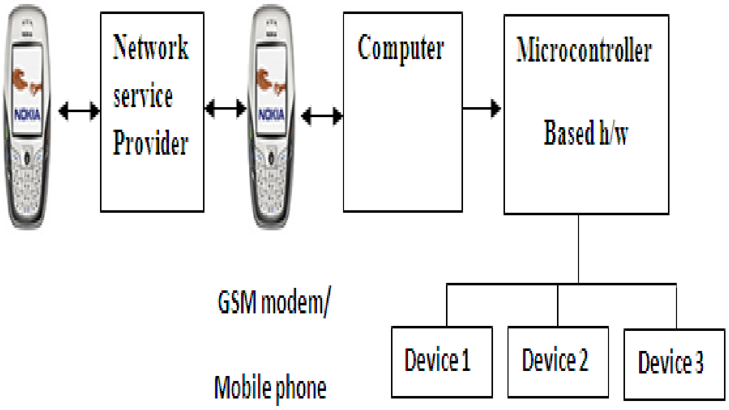

Fig.1 Architecture of proposed system

The layout of the system is as depicted in fig. 1 which conveys the mechanism of sending messages from a sender mobile handset for the purpose of performing control operation of the electrical device at a remote place. The operations are performed in a more secured way. The receiver is a GSM modem or GSM enabled mobile phone which is connected to the electrical device through a computer system and micro-controller based hardware. The security to the messages passing through the network operators between the sender and the receiver mobile devices is provided by developing enhanced version of Blowfish algorithm. Presently, emphasis is given on relay based control operations in a more secured way.

The objectives behind this research work are –

1. Provide end-to-end security over GSM network.
2. Utilize messaging service for important applications like control purposes etc.
3. Enhance the blowfish algorithm to provide better security and its use for many common purpose commercial applications.
4. Design microcontroller based hardware to apply all the above techniques and control the electrical devices connected there-on.
5. Analyze the performance of Blowfish and modified version of Blowfish algorithms on the parameters like block size, key size, memory size, Avalanche effect, GA and others.

4. MODIFIED BLOWFISH ALGORITHM

Although the fast and secure encryption algorithm [6] and blowfish algorithm [7] are implemented for mobile device applications, they do have certain limitations and brute-force attack have been attempted.

However, the combination of these two algorithms serves this purpose in better way. The techniques like substitution mapping, transposition, translation and Feistel networks make the cryptanalysis difficult by brute-force method.

The modified blowfish algorithm has the block size of 128-bits and key size of 128-bits and it occupies 6.1 KB space which helps in embedding this mechanism in any handheld devices for secured message transfer. Fig. 2 depicts the mechanism of modified blowfish algorithm.

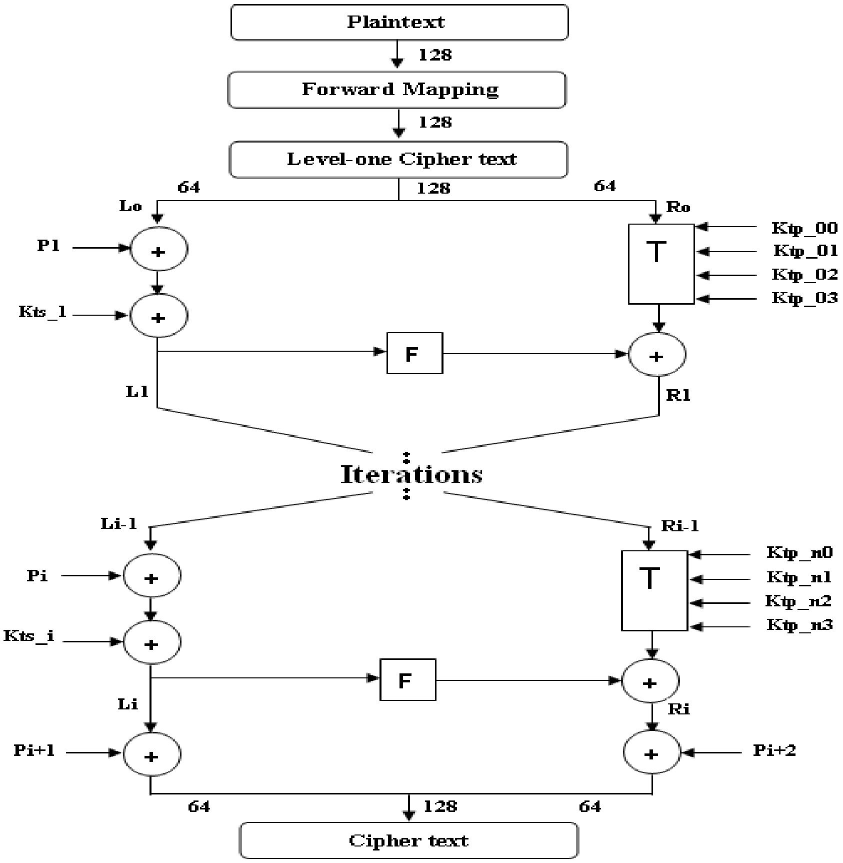

Fig. 2 Modified blowfish algorithm

The terminologies used mean the following:

L_i – Left 64-bits of i^{th} round. R_i – Right 64-bits of i^{th} round F – Feistel function

T – Transposition K_{ts_i} – Key for translation of i^{th} round.

K_{tp_ij} – Key for transposition of i^{th} round $\oplus$ - XOR operation

4.1 Encryption steps

i) Initialize matrix with given key and calculate various sub keys.
ii) Perform forward mapping [6].
iii) For 1-16 stages of encryption:

$$R_i = L_{i-1} \oplus P_i \oplus K_{ts\_i}$$

$$L_i = T(R_{i-1}) \oplus F(R_i)$$

4.2 Decryption steps

i) Perform XOR using P_{i+1} and P_{i+2}.

ii) For 1-16 stages apply key in reverse order:

$$L_{i-1} = R_i \oplus P_i \oplus K_{ts\_i}$$

$$T(R_{i-1}) = L_i \oplus F(R_i)$$

$$R_{i-1} = T^{-1}(L_i \oplus F \oplus F(R_i))$$

iii) Perform reverse mapping [6].

The J2ME wireless toolkit is used to provide GUI for user to choose the control operation of specific remote device, encrypt the user enforced information and send the message to the remote GSM modem enabled mobile device. At the receiver end, the Java packages like SMSLib, Comm are used and necessary initialization of communication with GSM device, decryption of message received, communicating with serial port of the computer system is done.

5. MICROCONTROLLER HARDWARE

The interfacing hardware required to operate electrical devices connected to the computer system through serial ports has been designed using 89C51 microcontroller. Fig. 3 and fig. 4 show the required circuit diagrams. The functioning of the 89C51 micro-controller is to decode the bit stream coming from serial port of the computer system and send the signals to the relay circuit to control the appropriate devices connected to the relays.

The code written in assembly language performs the operations of initializing communication port between the PC and microcontroller. The tools used for the purpose are Keil µVision4, universal programmer and XACCESS.

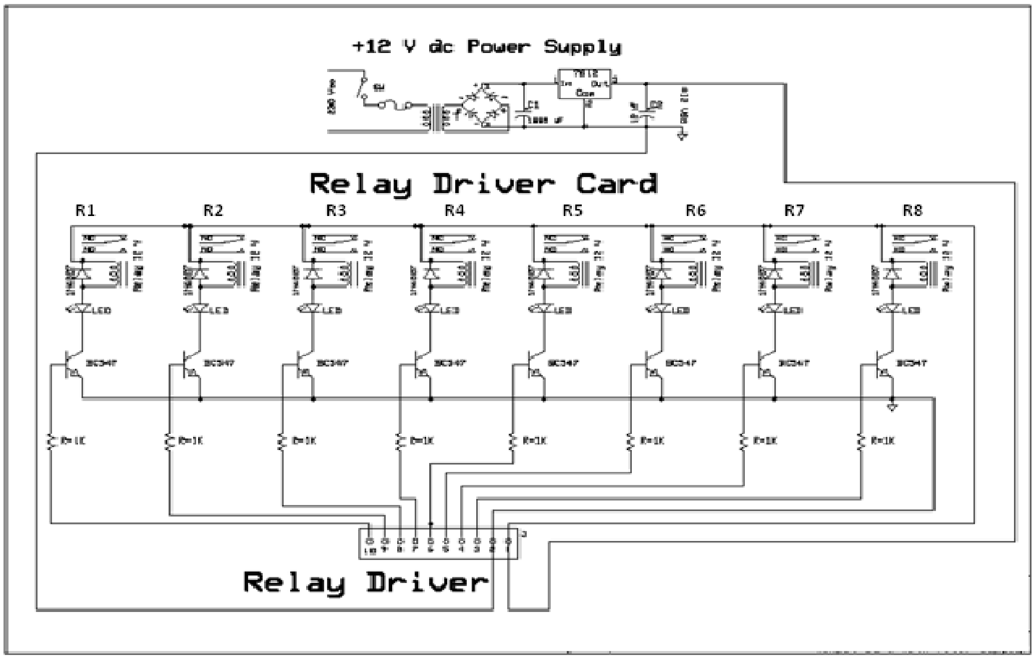

Fig. 3 Circuit diagram of CPU board in hardware

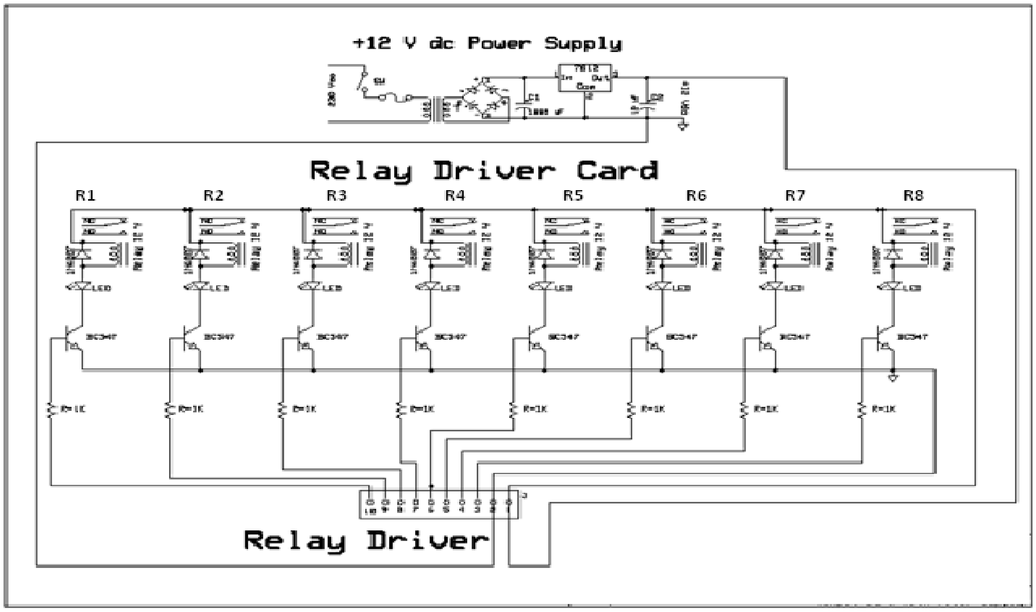

Fig. 4 Relay Driver Circuit

6. EXPERIMENTAL RESULTS

The executable version of Modified Blowfish algorithm has been embedded on mobile phone. Varieties of messages were tested for encryption, decryption and control of appropriate relays to which electrical devices are connected. The implementation of Blowfish algorithm and Modified Blowfish algorithm has been tested on the following parameters:

i) Time for encryption and decryption
ii) Throughput
iii) Guaranteed Avalanche effect
iv) Memory size required to store the executable version of the algorithm.

The throughput of encryption algorithm is calculated as the total plaintext in bytes divided by the time taken for encryption [4][5]. The Guaranteed avalanche effect is of order π. The comparison of both the algorithms is shown in table 1.

Table 1

Parameters	Modified Blowfish Algorithm	Blowfish Algorithm
Block size	128-bits	64-bits
Key size	128-bits	128- bits

Techniques	Feistel function, Substitution, Transposition, Translation	Feistel function
Total time	16.70966 ms	10.282816 ms
Throughput	975.5296 bytes/sec	1565.342 bytes/sec
Guaranteed Avalanche	Order=3	Order=1
Memory size	6.5 KB	5.3 KB

The table 1 shows that by having appropriate tradeoff amongst the parameters, the security is enhanced by looking at the guaranteed avalanche of the algorithms. The fig. 5 and fig. 6 show the avalanche effect of Blowfish algorithm and Modified Blowfish algorithm respectively.

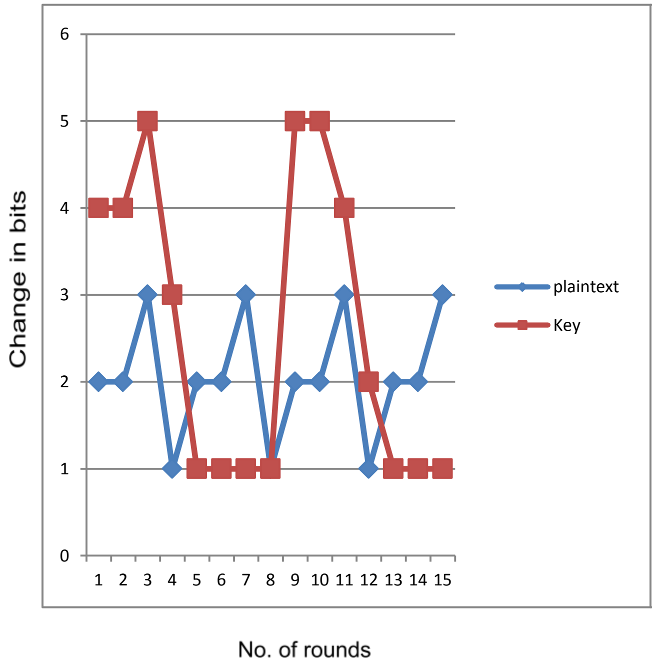

Fig. 5 Avalanche effect of Blowfish algorithm

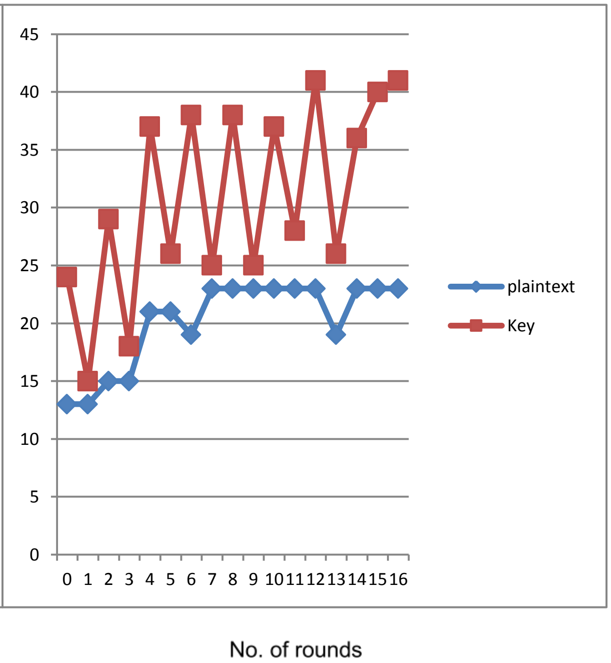

Fig. 6 Avalanche effect of Modified Blowfish algorithm

7. CONCLUSION

There has been tremendous rise in number of mobile users in the world as it provides lots of services. Hence the aim of developing new secured and authenticated system which can control the electrical devices from remote locations using mobile SMS services has been achieved. An 89C51 micro-controller was designed and programmed with the help of Universal programmer. The Modified Blowfish algorithm was found to be a suitable encryption algorithm for the above purpose. Results of this algorithm clearly show that the system provides end-to-end security and the algorithm is difficult for cryptanalysis.

The non-linear graph obtained using Modified Blowfish algorithm clearly shows that the algorithm provides greater security comparatively. The use of techniques like Substitution, Transposition, and Translation along with Feistel function increases the complexity of algorithm which makes it difficult for cryptanalysis.

The further work includes use of digital signature for checking message integrity over GSM network. One can choose different control operations other than ON/OFF for remote electrical devices.

REFERENCES

[1] Jawarkar N.P.; Vasif Ahmed; Thakare R.D. ***Remote control using Mobile through Spoken commands*** Signal Processing, communications and Networking, 2007. ICSCN apos; 07 Vol. Issue , 22-24 Feb.2007page(s):622 – 625.

[2] Nunes, R.J.C.; Delgado, J.C.M. ***An Internet Application for Home automation*** Electrotechnical Conference, 2000. ME LECON 2000. 10th Mediterranean Vol 1, Issue , 2000 Page(s):298 – 301.

[3] D.; Drahansky, M. ***SMS Encryption for Mobile Communication*** Security Technology,2008. SECTECH apos;08. Vol. , Issue , 13-15 Dec. 2008 Page(s):198 – 201.

[4] Diaa Salama, Abdul Elminaam, et.al. "***Performance Evaluation of Sym metric encryption Algorithms***" ICSNS International Journal of Computer Science and Network security, VOL.8 No.12, December 2008.

[5] Aamer Nadeem, Dr.M. Younus Javed "***A Performance Comparison of Encryption algorithm***".

[6] Paul. A. J.,Varghese Paul, P. Mythili ***A fast and secure encryption algorithm for message communication*** Information and Communication Technology in Electrical Sciences (ICTES2007).ICTES.IET- UK.

[7] Webpage: pocketbrief.net/related/Blowfish Encryption.pdf

[8] Website: http://www.smsspoofing.com

[9] Website: http://www.atmel.com

Kishor T. Mane received the BE (CSE) from Dr. J. J. Magdum college of Engg., Jaysingpur and ME (CSE) from D. Y. Patil college of Engg. & Tech., Kolhapur. He is presently working as Assistant professor in D.Y. Patil college of Engg. & Tech., Kolhapur.

G. A. Patil received BE (CSE) from PESCOE, Mandya and ME (CSE) from Walchand college of Engg., Sangli. He is working as Head and Assistant professor in D. Y. Patil college of Engg. & Tech., Kolhapur since 1992.