IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 9, PP 83-86

RF Based Secure Coded Communication System

Aditya Shah[1], Shahbaz Shaikh[2], Divyesh Parmar[3],
Sarang Kulkarni[4]
Department of Electronics, Atharva College of Engineering, India

Abstract: *The project is designed to send secured messages by using an encryption from a computer keyboard connected to the transmitting unit via RF technology. The message is retrieved at the receiver end only upon entering the secret code used by the transmitter. Thus, complete secrecy is maintained in this communication process. This system has a secret code attached to the transmission. The message typed in by the user is transmitted to the receiving end through RF transmitter. At the receiving end the RF receiver is integrated with a code and display system. User at receiving end can only view the message if he enters the right code.*
Keywords *- Encryption, Decryption, Keil compiler, Microcontroller, Secrecy.*

I. Introduction

Secure communication is when two entities are communicating and do not want a third party to listen in. For that they need to communicate in a way not susceptible to eavesdropping or interception. While standard secrecy methods such as cryptography protect the contents of the message from being accessed by unauthorized users, covert communication conceals the existence of the communication to prevent unauthorized users to detect the communication. Secure communication includes means by which people can share information with varying degrees of certainty that third parties cannot intercept what was said. Other than spoken face-to-face communication with no possible eavesdropper, it is probably safe to say that no communication is guaranteed secure in this sense, although practical obstacles such as legislation, resources, technical issues (interception and encryption), and the sheer volume of communication serve to limit surveillance. With many communications taking place over long distance and mediated by technology, and increasing awareness of the importance of interception issues, technology and its compromise are at the heart of this debate.

The proposed system is designed to be used for secret code transmissions needed in military, government or other sensitive communications. User may type his message through a computer keyboard. This is then processed by an 8051 microcontroller and delivered to the receiver end wirelessly. This system has a secret code attached to the transmission. The message typed in by user is transmitted to the receiving end through an RF transmitter. At the receiving end the RF receiver is integrated with a code and display system. User at receiving end can only view the message if he enters the right code. On entering the right code, the transmitted message is displayed on an LCD display.

For example in military operations, secrecy is of paramount importance. So when there is a need for sending any secret message, one can type the message through a computer keyboard interfaced with the system comprising of a 8051 family microcontroller and a RF transmitting module.

Radio Frequency Identification (RF-ID) is a wireless system that automatically identifies tracks and manages objects via a fast connection between the object and a RF-ID reader. RF-ID principles are described in a publication entitled "Radio Frequency Identification—RF-ID: A Basic Primer", published by the Automatic Identification Manufacturers (AIM) web site (http: //www.aimglobal.org), Oct. 23, 2001 and fully incorporated herein by reference. The object includes a transponder, active or passive, which when in the presence of an electromagnetic zone created by the reader broadcasts an object identity signal. The reader senses and decodes the broadcast signal to identify the object. The object identity is achieved by a connectionless communication that is a connection without a logical connection between the reader and the object. However, the RF-ID reader can not conduct interactive sessions between the object and the reader.

II. System Description

A. Working principle:-

RF Secure Coded Communication System. The proposed system enables users to send secret codes by enteringmessages through computer keyboard and sending the code through RF transmitters. This secret code sent is received through an RF receiver. It will be decoded when the receiver enters the same secure code as that with the transmitter. Secure communication services is based on the GSS-API (Generic security services-application programming interface), which was largely developed in the IETF.

NOTE: Interoperability is only possible between communicating peers using GSS-API implementation that supports the necessary interoperable cryptography algorithm and protocol. GSS-API allows peer to negotiate a common security mechanism (if the possess one, thereby enabling interoperability.)

B. Block Diagram :-

I. Transmitter Section

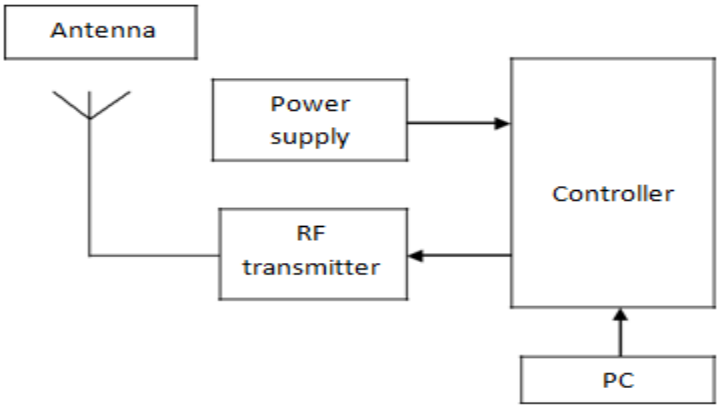

Fig 1. Transmitter Section

II. Receiver Section

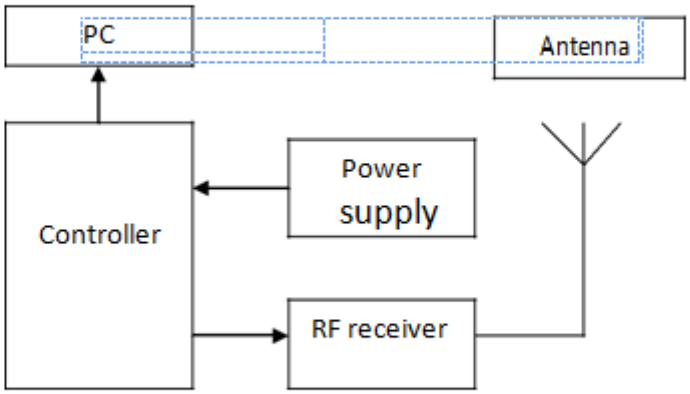

Fig 2. Receiver Section

C**. System Explanation :-**

I. MAX232N:

The MAX232 is a dual driver/receiver that includes a capacitive voltage generator to supply TIA/EIA-232-F voltage levels from a single 5-V supply. Each receiver converts TIA/EIA-
232-F inputs to 5-V TTL/CMOS levels. These receivers have a typical threshold of 1.3 V, a typical hysteresis of 0.5 V, and can accept ±30-V inputs. Each driver converts TTL/CMOS input levels into TIA/EIA-232-F levels. The driver, receiver, and voltage-generator functions are available as cells in the Texas Instruments Lin ASIC library.

II. RS232 Cable:

The RS232 connector was originally developed to use 25 pins. In this pin-out provisions were made for a secondary RS232 communication channel. In practice, only one communication channel with accompanying handshaking is present. I have never seen a computer or serial device where two RS232 ports were implemented

on one DB25 connector. For that reason the smaller 9 pin version is more commonly used today. The diagrams show the signals common to both connector types in black.

III. Antenna:

An antenna is a metallic structure that captures and/or transmits radio electromagnetic waves. Antennas come in all shapes and sizes from little ones that can be found on your roof to watch TV to really big ones that capture signals from satellites millions of miles away. The antennas that Space Communications and Navigation (SCAN) uses are a special bowl shaped antenna that focuses signals at a single point called a parabolic antenna.

IV. Micro Controller:

A Micro controller is a self-contained system with peripherals, memory and a processor that can be used as an embedded system. Most programmable micro controllers that are used today are embedded in other consumer products or machinery including phones, peripherals, automobiles and household appliances for computer systems. Due to that, another name for a micro controller is "embedded controller." Some embedded systems are more sophisticated, while others have minimal requirements for memory and programming length and a low software complexity. Input and output devices include solenoids, LCD displays, relays, switches and sensors for data like humidity, temperature or light level, amongst others. Types of Micro controllers: There are several different kinds of programmable micro controllers at Future Electronics. We stock many of the most common types categorized by several parameters including Bits, Flash size, RAM size, number of input/output lines, packaging type, supply voltage and speed. Our parametric filters will allow you to refine your search results according to the required specifications.

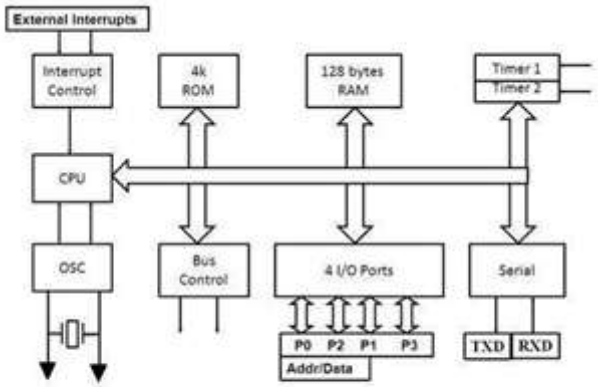

Fig 3. Block diagram of Microcontroller

V. Future Scope

The scope of GSS-API addresses protection of communication between distributed application, which does not comprise and interface to other non communication oriented security facility within hosts. Use of GSS-API is relevant to communication software and to those components of distributed application that implement application protocol. Generally, use of GSS-API sequencing facility is most appropriate when GSS-API is called from protocol modules who's message exchanges assume ordered sequences, semantics rather than a datagram environment.

VI. Conclusion

RF based secure communication is being developed by many organizations and utilized by many amputees. Many authors have presented issues and challenges in this technology. Research is being carried on this field to enhance this technology further. In this system it is possible to secure the messages sent to another user. In the future, it is possible to improve the system by making it a two way communication protocol.

Acknowledgements

We would like to express our deep gratitude to our guide Prof. Sarang Kulkarni for taking time from his schedule and provide us guidance, support, enthusiastic encouragement and useful critiques of this research. We have benefitted a lot from his immense experience and knowledge.

We are thankful to our college principal Dr. Shrikant Kallurkar, Head of Department of Electronics Prof. Disha Bhosle and all staff members of Electronics department who have provided us various facilities and have guided us whenever required.

References

[1] D. P. Agarwal and Q-A. Zeng, Introduction to Wireless and Mobile Systems (2nd Edition, published by Thomson, April 2005) ISBN 978-0-534-49303-5.
[2] J.K. and K. Ross, Computer Networking (2nd Ed, Addison Wesley, 2003) ISBN 978-0-321-17644-8.
[3] Soltani, R.; Bash, B.; Goeckel, D.; Guha, S.; Towsley, D. (September 2014). "Covert single-hop communication in a wireless network with distributed artificial noise generation". 2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton): 1078–1085. doi:10.1109/ALLERTON.2014.7028575.
[4] The schematics are illustrated in U.S. Patent 613,809 and describes "rotating coherers".
[5] Bash, Boulat A.; Goeckel, Dennis; Towsley, Don (September 2013). "Limits of Reliable
[6] Communication with Low Probability of Detection on AWGN Channels". IEEE
[7] Journal on Selected Areas in Communications. **31** (9): 1921–1930. ISSN 0733- 8716. doi:10.1109/JSAC.2013.130923.