International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.5., 2015
(Sept.-Oct.)

RESEARCH ARTICLE

ISSN: 2321-7758

CONTROLLER INTERFACING FOR SECURING COMMUNICATION BETWEEN TWO ARMY STATIONS

UMANGI LENGRE, POONAM PARDESHI, ASHWINI MAHALE, MADHURI AHIRE, Prof. K. C. NALAVADE

Department of Computer Engineering
Sandip Institute of Engineering and Management, Nashik, India

UMANGI LENGRE

ABSTRACT

Security of data/information in the army stations is an important threat. In the early developed systems, at the time of data transmission between two army stations, it can be hacked by terrorists, spies and enemies. Cryptography is a most important system employed for this purpose. There are variant types of algorithms available for encryption and decryption of data and new algorithms are evolving. Substitution cipher is a secure algorithm used for security of data in army stations. In this paper, various techniques of security of data and one the algorithm using substitution cipher i.e. poly alphabetic are discussed.

Key words— Cryptography, security, substitution cipher, Encryption, Decryption.

1.INTRODUCTION

Now-a-days, security is one of the most important factors in our day-to-day life. It can be useful anywhere any time. In banks, shops as well as in our daily life also we need security. One can use password to his computer for securing private information. This is also one of the types of data security. If in our daily life we require security then think about security of our security system i.e. our national security (defense). Especially, at the war time the terrorists and spies tries a lot to leak information so that they can capture the important information useful to win the war. Even in business and share market the competitors try a lot to hack the site of front person but if our data will be in coded form even if they are successful in hacking they will not understand the message/data. Present techniques having many drawbacks such as, anyone can receive, transmitted encoded message then these systems never provides the applications such as

1. **Privacy:** The transmitted message must be such that only the expected receiver should able to read it. No one else should be able to receiveit.
2. **Message authentication:** In message authentication, the receiver needs to be sure about the senders existence.
3. **Integrity:** The meaning of integrity is that data arriving at the receiver exactly as it was sent. There should not be any changed absolutely.
4. **Non-repudiation:** The meaning of non-repudiation is that the receiver should able to prove that, the message it has received has come from a specific sender itself.

The method for security of data is given as follow: Spread Spectrum Technique, Cryptography technique.

1.1. CRYPTOGRAPHYTECHNIQUES

Cryptography is the science of providing security for information. It has been used consequentially as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a key element of the modern security technologies used to protect information and resources on both open and closed networks.

The usage of cryptography techniques is increasing day by day as hackers are getting strong in their field and as important information is transmitted over the internet. There is need of securing this information within the organization only.

As cryptography contains the private key generation algorithms it became easy to secure the data between the specific sender and the receiver.

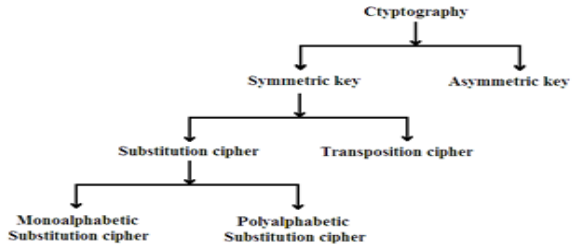

Fig1:TypesofcryptographyTechniques.

This figure 1 shows, the types of cryptography in which there are two types of cryptography one is symmetric-key and another is asymmetric-key. Again the symmetric-key is categories into two types namely substitution cipher and transposition cipher. The substitution cipher is subdivided into mono-alphabetic and poly-alphabetic substitution cipher.

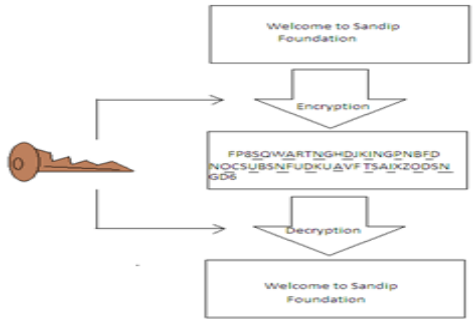

Fig 2: Cryptography Techniques

As above figure shows the process of cryptography in which it shows how the confidential data is encrypted and decrypted.

Cryptography is used to achieve following goals:-

Confidentiality: To ensure data remains private. Confidentiality is usually achieved using encryption. Encryption algorithms (that use encryption keys) are used to convert plain text into cipher text and the equivalent decryption algorithm is used to convert the cipher text back to plain text. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use a public/private key pair

Data Integrity: To ensure data is protected from accidental or deliberate (malicious) modification. Integrity is usually provided by message authentication code or hashes. A hash value is a fixed length numeric value derived from a sequence of data. Hash values are used to verify the integrity of data sent through in secure channels. The hash value of received data is compared to the hash value of the data as it was sent to determine if the data was altered

Authentication: To assure that data originates from a particular party. Digital certificates are used to provide authentication. Digital signatures are usually applied to hash values as these are significantly smaller than the source data that they represent.

2. LITERATURE SURVEY

2.1.Secure Data Retrieval for Decentralized Separation Tolerant Military Networks: A mobile nodes which contain in military environments such as a battlefield or an unfriendly regions are likely to a suffer from an intermittent networks connectivity and a constant partitions. The Disruption tolerant network (DTN) technologies are becoming a successful solutions to that allows a wireless device carried by a soldiers to communicate with each other's and an access the confidential information or a command reliably by abuse

external storage nodes. The most challenging issues for this scenario are the enforcement of authorization policy and the policies which are update for secure data retrieval.

2.2. Border Surveillance: Wireless Sensor Networks (WSN's) are based on a elementary sensors that detects the occurrences of particular events in a monitored area. The modern critical WSN applications are one can find a border surveillance applications. The first objective of the class of applications are to monitor the country border and a detect the presence of a intruders near to the border line. In this, investigate a theoretically the effects of a natural factors on dynamic deployment schemes of a tree like WSN based solutions to providing two lines of a surveillance. Parameters such as wind effect, altitude and a velocity of the airplanes from which sensors are thrown are put into an equation to optimize the coverage area and WSN connectivity.

2.3. Barrier Coverage with Airdropped Wireless Sensors: Obstacle coverage of a wireless sensor network aims at detecting intruders crossing a network. It provides a viable alternative for monitoring boundaries of fronts, country borders, coastal lines, and the perimeters of critical infrastructures. Early studies on a barrier coverage regularly is assume that sensors are deployed uniformly at random in a large area. While theoretically interesting, may be impractical in real applications. Sensors are airdropped from an aircraft along its flying route. The wind, geographic terrain, and other factors are may cause a sensor to land in a locations circuitous from its targeted landing point with a random offset. It is more realistic to assume that sensor nodes are scattered with a normal offset along the deployment line.

3. PROPOSED SYSTEM

In this paper we discussed about the architecture of our system which is implemented for the securing communication.

Fig. 3 shows the design for showing sender side and receiver side communication using the Micro-controller 89S52.Which is used with the trans receiver RF antenna for wireless communication between two stations.

The algorithms will be stored on the controller itself for proper execution of it. This is the block diagram for PC side communication hence here we used MAX 232 IC for serial communication.

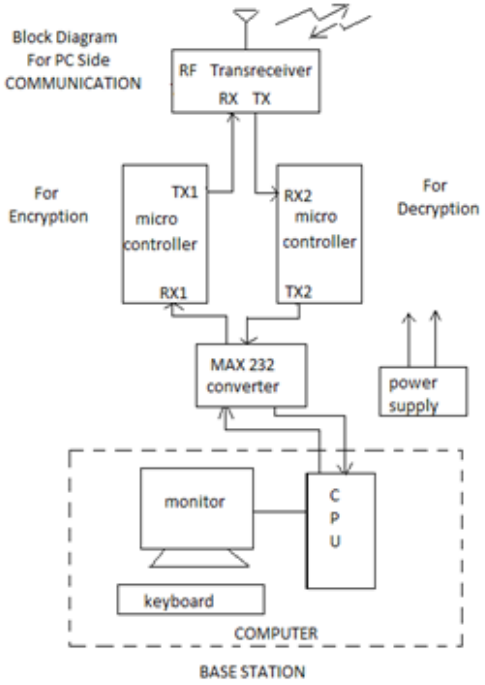

Fig 3: Block diagram of Sender and Receiver

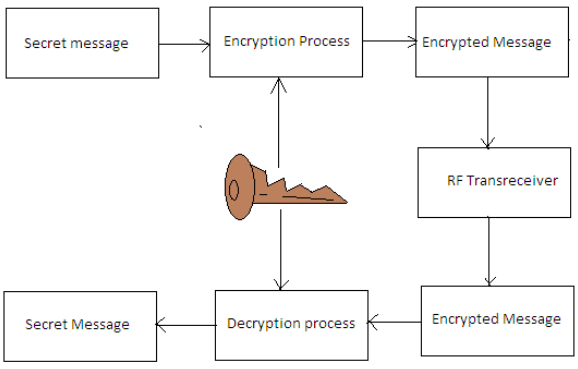

Fig 4: Block diagram of Proposed System

Figure 4 shows the encryption and decryption process of our system. Here when secrete message is sent through wireless network firstly with the help of encryption algorithm the message will be encrypted and secrete key will added in it. At receiver end the

reverse process will be applied, when receiver receive the encrypted message he/she were not able to get the message exactly hence receiver has to apply the decryption algorithm with subtraction of the secrete key from it after all this process receiver will get the original message which is sent by the sender.

The secrete key will be the unique one which is updated or modified after every one month. So, there is less possibility of hacking the secrete key. Even hacker got the key he/she need algorithm which is used for encryption and decryption.

4. SYMMETRIC KEY CRYPTOGRAPHY

It is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Comparison with public key cryptology, which utilizes two keys - one public key to encrypt messages and a private key to decrypt that message. Symmetric-key systems are simpler and faster, but main drawback is, two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be scattered in insecure way, and the private key is never transmitted. Symmetric-key cryptography is also called secret-key cryptography.

In our paper we are going to use encryption and decryption algorithm for encoding the frames. For this purpose we give a start of frame and end of frame to each slave. For example,

Slave1 start of frame: - FRZ----- (FRAME) ------91S.
SOF EOF
Slave2 start of frame: - 6R7------ (FRAME) -----OP9.
SOF EOF
Inside a frame we can have a encoding system For example, Original frame: FOUNDATION
Encoded :FEDOAXUCSNESDCVALETVCIMNOXAN
Decoded frame: FOUNDATION

So now the whole encoded frame for slave1 will be:
FRZ FEDOAXUCSNESDCVALETVCIMNOXAN91S.
SOF EOF

Here the micro controller has both the SOF (Start of frame) and EOF(End of frame) and the decryption logic it can easily decode the frame as FOUNDATION. Whereas if the frame fails in to enemy hands they cannot decode the frame because they don't have the decoding logic. Same goes for slave2.so if we know both the slaves SOF, EOF and the encoding logic inside the frame we can send an encoded frame for 'N' no of slaves. In this way when we send a frame all slave will receive it. Then scan the whole frame for SOF and EOF if they get it they accept the frame in between SOF and EOF. The rest of the frame is discarded.

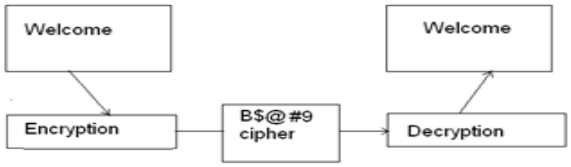

Fig 5: Secret key cryptography

Figure 5 shows the simple example of secret key cryptography. Which describes the how plain text is converted into cipher text and how it again decrypted.

5.ALGORITHM AND FLOWCHART FOR SYMMETRIC KEY

5.1.Algorithm for encryption:

Step1 : START

Step2 :Take the character from plain text and represent each letter in cipher-text by a number from 0-25 (i.e. 'a'=0,'b'=1, 'z'=25).

Step3 : Add 26 to cipher-text number.

Step4 : Subtract corresponding key from that addition. Step5 :Subtract 26 from that addition.

Step6 : write corresponding letter for above number.

Step7 : Repeat the procedure up to end of text.

Flowchart:

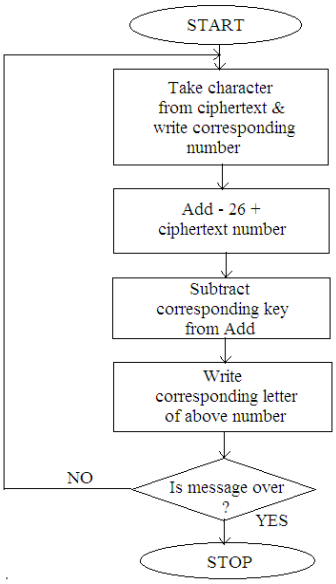

Fig 6: Flowchart for Encryption

5.2. Algorithm for decryption:

Step1 : START

Step2 : Take the character from plain-text and represent each letter. In plain-text by a number from 0-25 (i.e. 'a'=0,'b'=1…
'z'=25).

Step3 : Add the key number corresponding to plain-text number.

Step4 : If addition is > 25, subtract 26 from addition and write down letter corresponding to that number as cipher-text

Step5 : And if addition is between 0-25 write down corresponding letter as cipher-text.

Step6 : Repeat the procedure up to end of text.

Flowchart:

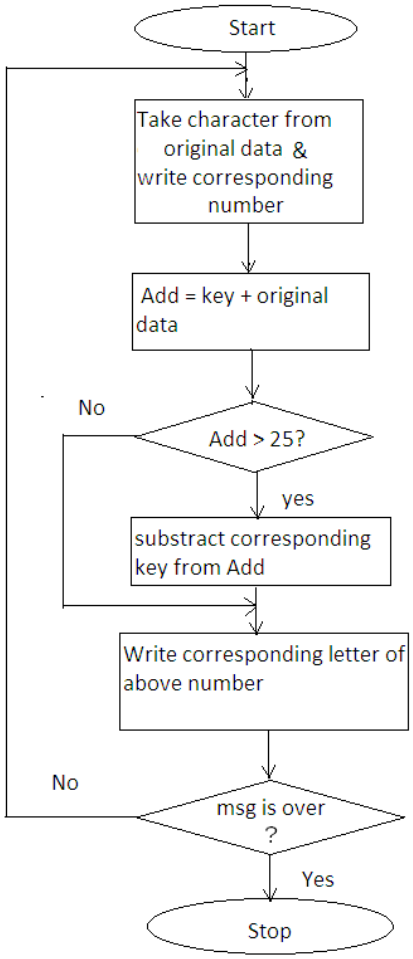

Fig 7: Flowchart for decryption

6. MATHEMATICAL MODEL

System S= Encrypted data and Decrypted data

System S= {s~, E, D, d, K, I,O}

∑Ii= {I1, I2}

∑Oi= {O1, O2}

Where, E=Encrypted data D=Decrypted data d=Original data

K=security key E=Encrypted data + key D1= Decrypted data – key D2= Decrypted data

I1= Input data converted into number (assigning a/A=0, b/B=1….. z/Z=25)

I2= number + key

O1= Output data in number format O2= Output-key

ACKNOWLEDGMENT

We are sincerely thankful to Prof. K. C. Nalavade and also Prof. U. B. Pawar, Head of Department, Department of Computer Engineering, Sandip Institute of Engineering and Management, Nashik, for their kind help and encouragement for the proposed work.

REFERENCES

[1]. Sumedha et al., International Journal of Advanced Research in Computer Science and Software Engineering 2 (12),December - 2012, pp. 105-107

[2]. Quantum Cryptography for Wireless Network Communications

[3]. Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma Faculty of Information Sciences and Engineering University of Canberra, ACT 2601, Australia

[4]. Xu.Huang,Shirantha.Wijesekera,Dharmendra.Sharma I.J. Information Engineering and Electronic Business, 2012, 2, 36-42 Published Online April 2012 in MECS (http://www.mecs- press.org/) DOI: 10.5815/ijieeb.2012.02.06