International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.1, No.7, November 2012 DOI:10.15693/ijaist/2012.v1i7.58-61

Encryption of Sensor Data: A Novel Implementation

Prajakta Paturkar
ME (Perusing),
Digital Communication, II Year,
JIET, Jodhpur.

***Abstract*— Wireless Sensor Network technology is a fast growing priority area of research. It is expected that wireless sensor technology shall make inroads into many public utilities namely, disaster management, transport, process control, security, environment and wild life monitoring, etc.**

The wireless sensor networks differ from other networks in two primary aspects. The first is that unlike other networks the Wireless sensor networks have a dedicated function to perform and not any sort of information exchange. The other aspect of the network is that the nodes may or may not be accessible after deployment.

This paper describes an encryption technique, specifically suitable for wireless sensor networks. The scheme works on a public key with dynamic encryption changes. The scheme can be implemented on a FPGA and can be dynamically altered. Since the nodes in a WSN are built using microelectronics gadgets the scheme of encryption can be implemented on a single microchip with embedded resources and programmable gate array that comes on the latest programmable cores.

Index terms - Data encryption, wireless sensor network, Data security, VHDL, FPGA

I. INTRODUCTION

Wireless sensor networks offer a wide range of advantages with respect to the conventional wired networks. The prominent advantages are:

1. Unattended performance,
2. Possibility of monitoring unreachable locations,
3. Unobtrusive monitoring
4. Low deployment efforts and cost

Whereas the disadvantages are:

1. Energy constraints at node,
2. Medium access control issues,
3. Data traffic problems,
4. Node compromise and topology changes,
5. Data security

Most wireless sensors are expected to meet a unique objective. Depending on the objective and the venue over which it extends, requirements guiding the WSN architecture vary. As an example a WSN may be deployed to monitor temperature of various parts within a turbine. The requirements of this system shall be completely different from another WSN which is expected to monitor and ensure security of wild life in a sprawling forest. Most of the features that are required for ensuring QoS of the WSN are guided by the objective and venue. The intricacies of the Network design rise with criticality of the objective as well as with the size and accessibility of area of deployment.

The network design parameters that change with respect to WSN objective are:

- Security features
- Routing protocols
- RF power requirement
- Deployment strategy
- Energy resources

A WSN normally consists of three principle devices as shown in Figure 1.

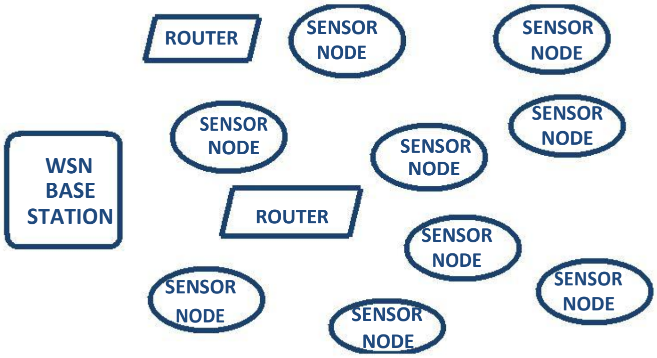


Figure 1 Devices in a Generic

The components are Server, sensor nodes and data processing nodes. The sensor node acquires environment variables from its neighborhood, converts this to digital data and transmits this information for further processing. The data processing nodes are expected to perform data aggregation, and handle routing requirements of its domain of sensor nodes. A server assimilates the data and presents it for action at a command/ control center.

Majority of the design aspects that differ in WSNs are features in the sensor node. Block schematic of a generic sensor node is shown in figure 2.

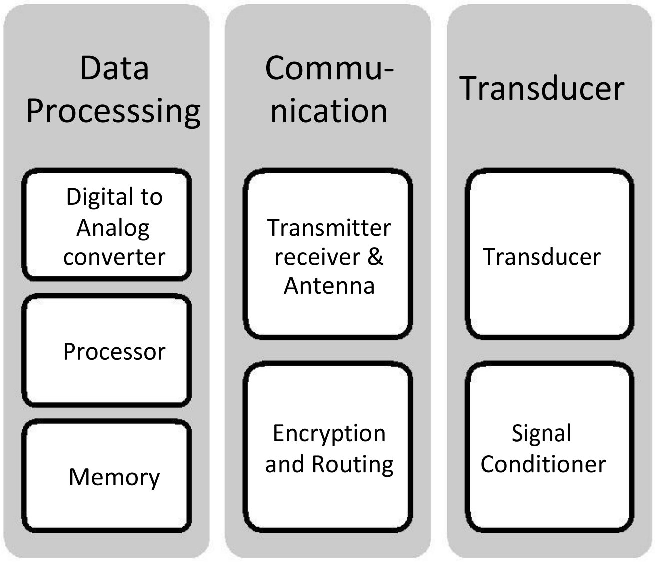


Figure 2 Block schematic of a sensor node

The sensor node consists of transducers for sensing the environment parameters, signal conditioner, analog to digital convertor, embedded controller, RF trans-receiver and battery as energy source. The embedded controller handles four processes simultaneously. These are:

1. Sense the environment parameters and digitize the data either periodically or on command or based on changes in the environment.
2. Keep track of energy resource and communicate energy criticality on priority.
3. Monitor RF input and Respond to RF network MAC requirement. Keep track of adjacent nodes within its RF reach and routing requirements for self configuration.
4. Ensure security of data via authentication and identification of malicious data packets.

In principle the processes of sensing environment and tracking energy constraint are common to all WSNs. The QoS and nature of objectives of a WSN enforce additional complexities in routing, self configuration and data security.

A. Data security

Many problems can arise due to network attacks in a general network. The degree of damage caused by such attacks varies from case to case. In general, a message leakage or alteration is a well-recognized security risk as well as privacy invasion. However, if such attack occurs on sensor network, there can be major accident causing harm to life and property.

B. Cyber Attacks and Precaution

There are two major categories of attacks -

1. Imitate: Data coming from unauthorized sources.
2. Man in between:-The data coming from source, which is on the same channel through any parallel system on same network claiming as sensor.

To avoid both types of attacks the following precautions need to be taken.

1. The sensor has to identify itself in every message.
2. All the data sent on channel or network has to be encrypted properly

The first of the requirement can be functionalized by the embedded processor by having a unique ID stored in its ROM. However, without proper encryption, even this may lose its effectiveness.

Encryption and decryption of data is thus an important aspect in secure data communication. The data usually has some secret element that can affect security of individuals or organizations like password of e-mail, ATM, system login etc. Data concealing means converting a legible form of information to an illegible form. This is essentially done for protecting the information from unauthorized access.

In **Encryption,** a readable information or simple text is transformed into unreadable form using some defined algorithm at the transmission end. At the receiver end a **Decryption** algorithm is used to decode or translate the unreadable data back to readable information. The process of encryption and subsequent decryption is secrete and known only to the identified sender and receiver.

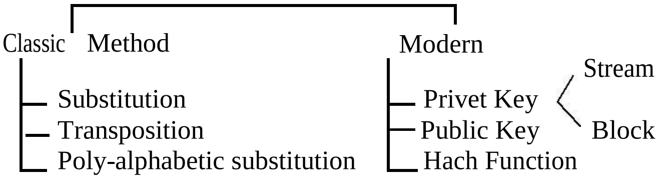
The algorithm of encryption, the key of encoding, and the algorithm of decryption are all together called as cryptography [1].

II. COMMONLY USED CRYPTOGRAPHIC ALGORITHM

In cryptography, an algorithm known as cipher is used for performing encryption and decryption. Cipher has a well-defined series of steps that are followed as a procedure to perform encryption. An alternative term also used for cipher is encipherment [1].

There are many types of cryptographic algorithms. Discussing all of them is beyond the scope of this paper. However, some main basic techniques are briefly outlined here only for introductory purpose.

Cipher can be divided in many types such as:



In this paper the technological aspects of field sensor data encryption dealt with a hardware implementable algorithm for encrypting sensor data in effective manner. In other words, the scheme of encryption described can be implemented on a single programmed chip like an embedded controller or an FPGA. Such an algorithm can have immense applications in networking of sensors [2][3].

III. Proposed Work In Cryptography

A. *Major Issues in Encryption of sensor data*

Unlike a human readout message, where typically a few characters are required for making a sensible statement, the sensor data length may range from a single bit such as the state of a switch to a large volume such as an image from camera. It is implied that the encryption scheme must take this in account. For encryption of large volume of data many ciphers exist and the ciphers implemented on a computer system can afford to be quite complex in terms of number crunching requirement. In case of sensors, particularly field-deployed sensors, the hardware and power resources are critical. The hardware should not be too bulky and the power requirement must be minimal. These two requirements are suitably available through FPGA hardware. It would always be preferable to include additional logic on the resources already available and the algorithm should use minimum resources from the given chips.

The key issue that is sought to be addressed here is encoding of data that may be of small length, typically tens of bytes (including sensor identification code), and is hardware implementable on energy efficient chips like FPGAs.

Another important issue in sensor data is the temporal aspect of the sensor data. Unlike the data in case of messages (like e-mail), the sensor data has some limited time validity. The time validity may range from a few seconds to a few days. Thereafter, the data is only of historical interest. For designing the Encryption scheme, the projection of possible auto debugging may not be required beyond this time provided the encryption method has a dynamic element, which should be reprogrammable at frequent interval.

IV. Solution Through Cryptographic Method

There are various methods of encryption that can be used and implemented through a program written in C, C++, Java, VHDL, or Verilog. The program can be written in the field and downloaded to the FPGA chip. Most of these chips are in-circuit programmable and hence the encryption key or even the complete cipher can be changed online.

For implementing the encryption scheme on practical systems the foremost consideration is network attack minimization. This can be done by using identification of sensor system and using a proper authentication ID. Every time sensor is sending data it should send its encrypted identification number and it should frequently change encryption key. After completion of one cycle of operation, the key may or not be repeated, but in one cycle operation, it will not be repeated.

The data to be transmitted by the sensor also must be encrypted along with the authentication ID. Thus when the complete information exchange is encrypted the network can be trusted in terms of security.

There are two important aspects of encrypting a message.

1. Alteration of the character set.
2. Relocating the characters within message.

Neither of two is independently sufficient method of encryption. This is so because any kind of messaging protocol shall have a predictable set of format in the original form. The statistical or syntax analysis of the messages over a set of transmissions shall give away the encryption system in absence of either of the two aspects. Alteration of characters alone shall result in a constant predictable pattern in the output and Relocation shall give away the repeating character set which can be made legible in very short time. Therefore, both these aspects need to be implemented in the encryption system.

Another aspect that should be implemented is dynamic encryption. As has been brought out earlier, a sensor is constantly sending messages on the same network and if an intruder studies a set of messages that he has managed to trap; he can analyze them and use this information some time later to manipulate the network. This can only be avoided if the encryption scheme changes with every message in a manner that is known only to the authentic transmitter and receiver system through a predefined and programmable (through in-circuit programmable chips) key.

V. Proposed Scheme

A. Novel Approach and Implementation

The paper proposes a new way of cryptography. In this process the WSN network is kept in mind which means method should be built in sufficient security so that authenticity and privacy of information is secured. It should also have low processing overheads for energy efficient implementation.

According to this scheme, the nodes of WSN are pre-programmed to hold a data file much longer than the data packet. The data file supports dynamic key for encryption then the node mainly carries out following two procedures for encryption

1. Decimation
2. Encryption

Decimation

The data slots are to be created let’s say N bits. Then these N bits are to be decimated in a predefined manner. The key to decimation can be passed through data packets.

In this paper decimation is done similar to card shuffling method. The following steps should be followed

- Remove the LSBs (M bits) from data slot of N bits and move them on the MSB.
- Remove the LSB (M bits) from modified data slot of N bits and insert it midstream defined by fraction of M.
- Repeat these steps T times.

Encryption

After decimation the new data slot can be directly XORed with the key. But for doing this also the key should be shared with the main base station in WSN. The key will be stored in ROM of the sensor node and also will be with the main base station.

The key stored should be long than the data slot let's say K bits (such that K >> N). The key is read through a pointer which calculates and points a random bit of the memory slot from where the key of N bits is to be copied in a temporary register. These N bits of the key are now XORed with the N bits of decimated data slot.

B. Algorithm proposed

1. Convert the data to digital format using analog to digital converter.
2. Make data slots of 128 (N) bits each.
3. Decimate the data using the shuffling method outlined above or any other 1:mapping scheme
4. After decimation XOR the data with key selected via the pointer.
5. Now the data is ready to be transmitted on WSN.

VII. Conclusion

The encryption suggested in this paper can implemented on in-circuit programmable chips. Hence it is suitable to use where hardware resources is a design constraint. This encryption method builds in dynamic encryption for both decimation of characters as well as character set manipulation. The processing overheads are minimal. Thus it makes a strong case for implementation on a wireless sensor network.

Acknowledgement

I thank my parents for their guidance, support and encouragement that helped me during this work. I am obliged to Prof. O P Vyas and the colleagues from Jodhpur Institute of Engineering and Technology for their constant encouragement and guidance.

References

[1] Wikipedia "Cryptography" http://en.wikipedia.org/wiki/Cipher

[2] Sudip Misra, Isaac Woungang & Subhas Chandra Misra "Guide to Wireless Sensor Networks" Springer 2009, Chapter 19, Security in Wireless Sensor Networks(Eric Sabbah and Kyoung-Don Kang) pp. 491-512.

[3] Jun Zheng &Abbas Jamalipour "WIRELESS SENSOR NETWORKS A Networking Perspective" Wiley 2009, Chapter 12, Network Security And Attack Defense (Yun Zhou and Yuguang Fang) pp369

[4] Sunder Rajan R., "An Efficient Operator based Unicode cryptography Algorithm for Text, Audio and video files", in International Conference 2008.

[5] Whitfield Diffie and Martin E. Hellman, "Privacy and Authentication: An Introduction to Cryptography" in Proc. IEEE vol. 67, no.3, pp. 397 - 427, 1979

Authors Profile

Prajakta Paturkar received the **B.E.** degree in Electronics and Communication Engineering from the Jodhpur Institute of Engg. & Tech. College, Jodhpur, Rajasthan University, Jaipur, India, in 2009.Currently doing **M.E.** in Electronics and Communication engineering (Digital Communication) in Rajasthan Technical University, Kota, India. Her research interest includes wireless sensor networks, digital communication, VLSI & FPGA.