SECURING INFORMATION IN WIRELESS SENSOR NETWORKS

Prashant Sangulagi[1], Mohan G[2]

[1]Department of ECE, BKIT Bhalki, Karnataka INDIA: 585328
[2]Department of ECE, BKIT Bhalki, Karnataka INDIA: 585328

Abstract

Security in Wireless sensor Network has emerged a must required research topic for the researchers. Securing the important data without affecting its accuracy is a important task. In this paper some of the important and feasible security techniques are discussed. Some of the standard and popular encryption techniques are Digital Encryption Systems (DES) and Advanced Encryption systems (AES). Attacks considered in the WSN environment are more, some of the main type like active attacks and passive attacks. Here, attacks in WSN are discussed in details and avoidance of those attacks using encryption techniques are also discussed here. This paper also analyzes the performance of DES and AES algorithms against the attacks in WSN.

Keywords: *WSN, Network Security, Attacks, Cryptography, DES, AES.*

----------***----------

1. INTRODUCTION

The aim of this paper is to provide secure data communication using DES and AES security algorithm for wireless sensor network. Wireless sensor networks are quickly gaining popularity due to the fact that they are potentially low cost solutions to a variety real of world- challenges. Their low cost provide a means to deploy large sensor arrays in a variety conditions capable of performing both military and civilian tasks. But sensor network also introduce severe resource constants due their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network. Unreliable communication channel and unattended operation make security defences even harder. Indeed, as pointed out in wireless sensors often have the processing characteristics of machines that are decades old, and the trend is to reduce the cost of wireless sensors while maintaining similar computing power. With that in mind, many researchers have begun to address the challenges of maximizing the processing capabilities and energy reserve of wireless sensor nodes while also securing them against attackers. All aspects of wireless sensor networks are examined including secure and efficient routing, data aggregation, group formation and so on.

1.1 Issues and Challenges in Designing a Sensor Network

Sensor networks pose certain design challenges due to the following reasons:
1. Sensor nodes are randomly deployed and hence do not fit into any regular topology.
2. Sensor network are infrastructure-less. Therefore, all routing and maintenance algorithm need to be distributed.
3. Sensors usually rely only on their battery power,
4. Sensor nodes should be able to synchronize with each other.
5. Sensor network should also be capable of adapting to changing the connectivity due to the failure of nodes, or new powering up.

Organization of the paper is as follows, section two describes the overall methodology in network security, section 3 gives detailed information regarding attacks in WSN, section 4 provides information regarding cryptography and section 5 and 6 explains DES and AES algorithms and lastly section 7 concludes the paper.

2. NETWORK SECURITY

Having discussed some of the attacks that have occurred in real life, let us now classify the principles related to security. This will help us understand the attacks better and also help us in thinking about the possible solution to take them.

There are four chief principle of security. And two more, access control and availability. Which are not related to a particular message, but are linked to the overall system as a whole. We shall discuss all these security principles as follow.

2.1 Confidentiality:

The principle of confidentiality specifies that only sender and receiver should be Understand the contents of the transmitted message.

2.2 Authentication:

The principles of authentication mechanisms help establish proof of identities. The authentication process ensures that the origin of a electronic message or document correctly identify.

2.3 Integrity:

When the contents of a message are changed after the sender sends it, but before it reaches the intended receiver, we say that the integrity of the message is lost.

2.4 Non-Repudiation:

There are situation where a user sends a message and later on refuses that she had sent that message.

2.5 Access Control:

The principle of access control determines who should be able to access what. For instance, we should be able to specify that user A can view the records in a data base, but cannot update them. However, user B might be allowed to make updates as well. An access control mechanism can be set up to ensure this.

3.TYPES OF ATTACKS

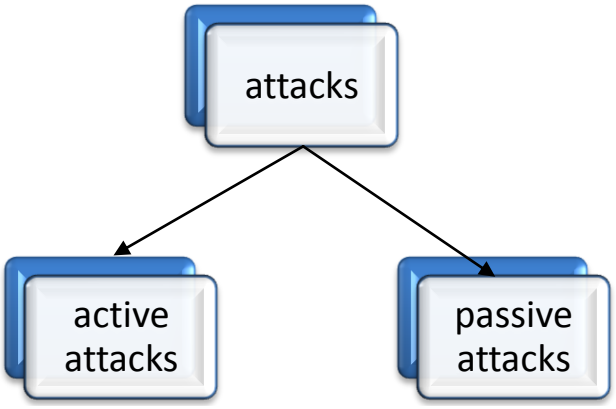

Fig. 1 types of attacks

3.1 Passive Attacks:

Passive attacks are those, wherein the attacker a indulges in monitoring data transmission. In other words, the attacker aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications to the data. In fact, this is also why passive attacks are harder to detect. Thus, the general approach to deal with passive attacks is to think about prevention, rather than detection or corrective actions. Passive attacks do not involve any modification to the contents of an original message.

3.2 Active Attacks:

Unlike passive attacks, the active attacks are based on modification of the original message in some manner or the creation of a false message. These attacks cannot be prevented easily. However, they can detect with some effort and attempts can be made to recover from them. These attacks can in the form of interruption, modification and fabrication.
In active attacks, the contents of the original message are modified in some way.

- Trying to pose as another entity involves masquerade attacks.
- Modification attacks can classified further into replay attacks and alteration of messages.
- Fabrication causes denial of service attack.

3.3 Types of Passive Attacks:

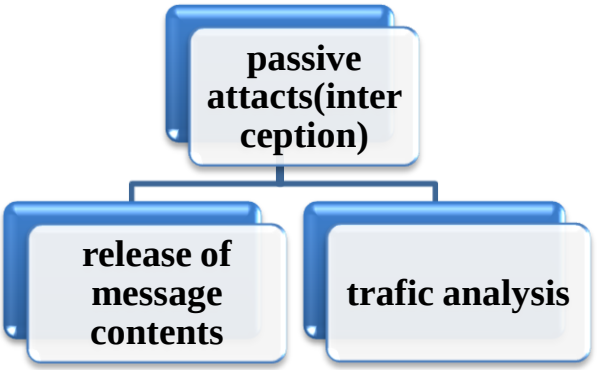

Fig. 2types of passive attacks

- **Release of Message Contents:**
  Release of message contents is quite simple to understand. When we send a confidential email message to our friend we desire that only she be the able to access it. Otherwise, the contents of the messages are released against wishes to someone else. Using certain security mechanisms, we can prevent release of message contents.

- **Traffic Analysis:**
  However, if many such messages passing through, a passive attacker could try to figure out similarities between them to come up with some sort pattern that provide her some clues regarding the communication that is taking place. Such attempts of analyzing message to come up with likely patterns are the of the traffic analysis attacks.

3.4 Types of Active Attacks:

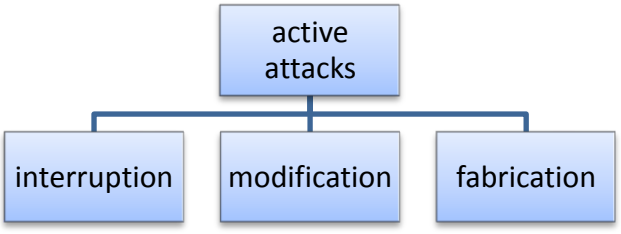

Fig 3: Types of active attacks

- **Interruption:** Interruption caused when an unauthorized entity pretends to be another entity.
- **Modification:** Modification attacks can be classified further into replay attacks and alteration of messages.
- **Fabrication:** Fabrication attacks make an attempt to prevent legitimate users from accessing some services, which they are eligible for. For instance, an unauthorized user might send too many login requests to a server using random user ids one after the other in quick succession, so as to flood the network and deny other legitimate users from using the network facilities.

4 WHAT IS CRYPTOGRAPHY?

Cryptography derived its name from a Greek word called "Kryptos" which means "Hidden Secrets".

Cryptography is the practice and study of hiding information. It is the Art or Science of converting a plain intelligible data into an unintelligible data and again retransforming that message into its original form.

It provides Confidentiality, Integrity, and Accuracy

4.1 Cryptography Algorithm

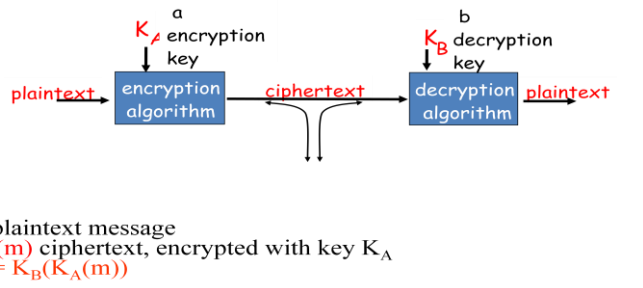

Fig 4: cryptographic components

Suppose now that "a" wants to send a message to "b". Ad's message in its original form (for example, "b", hello. "a") is known as plaintext, or clear text. "a" encrypts his plaintext message using an encryption algorithm so that the encrypted message, known as cipher text, looks unintelligible to any intruder. Interestingly, in many modern cryptographic system, including those used in the internet, the encryption technique itself is known-published, standardized, and available to everyone (for example,[RFC 1321;RFC 2437: RFC 2420; NIST 2001]), even a potential intruder! Clearly, if everyone knows the method for encoding data, then there must be some secret information that prevents an intruder from decrypting the transmitted data. This is where keys come in

5. DATA ENCRYPTION STANDARD:

The algorithm described by DES is a private-key algorithm, meaning that, both sender and receiver must know and use same private key is used for both encrypting and decrypting the data.

DES encrypts and decrypts data in 64-bit blocks, using a 64-bit key (although the effective key Strength is only 56 bits, as explained below). It takes a 64-bit block of plaintext as input and outputs a 64-bit block of cipher text. Since it always operates on blocks of equal size and it uses both permutations and substitutions in the algorithm, DES is both a block cipher and a productcipher.DES has 64-bit rounds, meaning the main algorithm is repeated 16 times to produce the cipher text. It has been found that the number of rounds is exponentially proportional to the amount of time required to find a key using a brute-force attack. So as the number of rounds increases, the security of the algorithm increases exponentially.

Steps in DES:
1. In the first step, 64-bit plain text block is handed over to an initial permutation function.
2. The initial permutation is performed on plain text.
3. Next, the initial permutation produces two halves of permuted block; say left plain text and right plain text.
4. Now, each of left plain text and right plain text go through 16 rounds of encryption process.
5. In the end, left plain text and right plain text are rejoined and a final permutation is performed on the combined block.
6. The result of this process produces 64-bit cipher text.

5.1 Advanced Encryption Standard:

The algorithm described by AES is a symmetric-key algorithm meaning that same key is used for both encrypting and decrypting the data. The AES standard is a variant where the block size is restricted to 128 bits and key size of 128, 192, 256 bits can be used.

AES is a symmetric cipher that processes data in 128-bit blocks. It supports key sizes of 128, 192, and 256bits and consists of 10, 12, or 14 iteration rounds, respectively.
Each round mixes the data with a round key, which is generated from the encryption key. The encryption round operations are presented in Fig 5.1. The cipher maintains an Internal, 4-by-4 matrix of bytes, called State, on which the operations are performed. Initially State is filled with the input data block and XOR-ed with the encryption key.

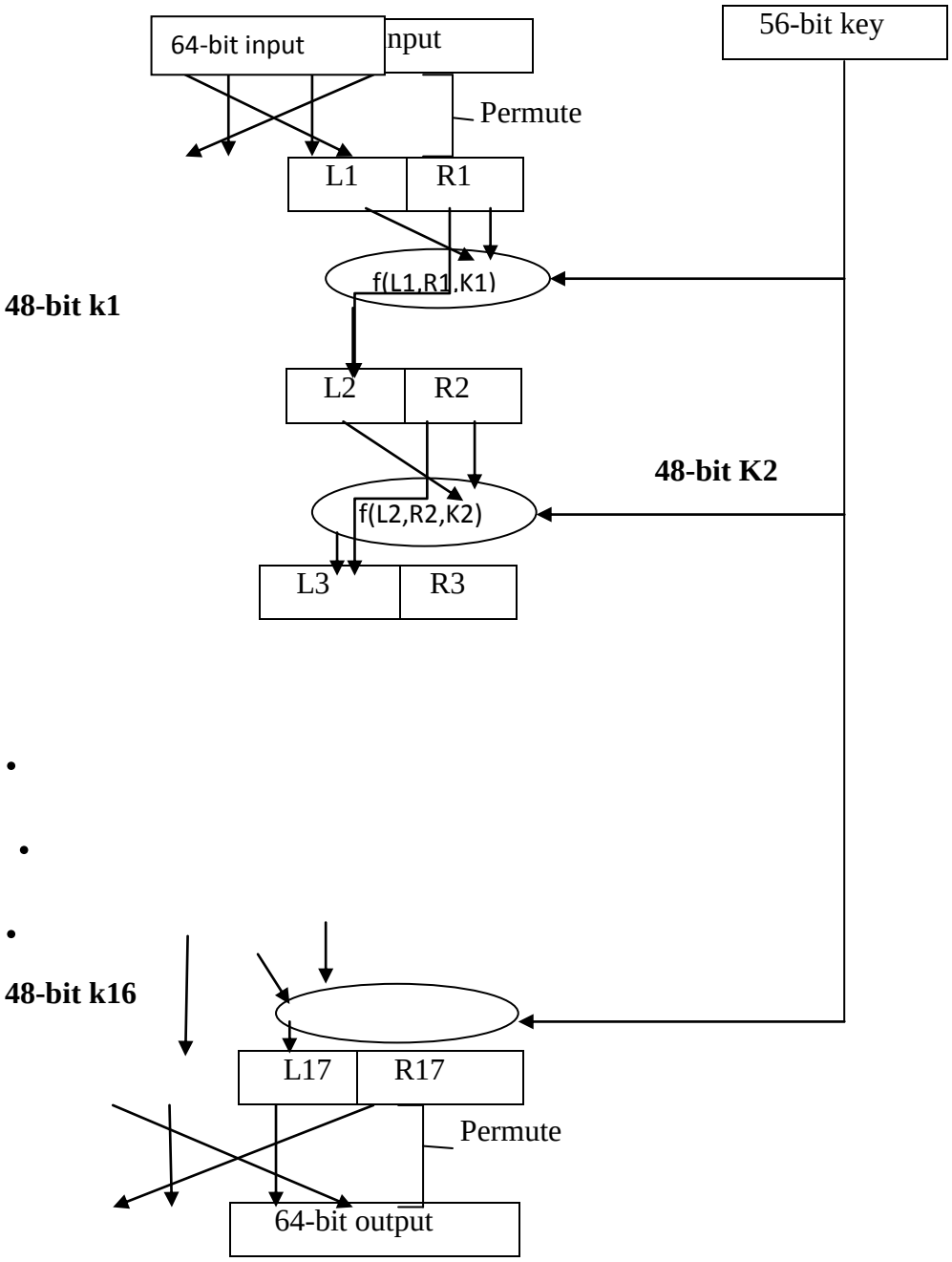

Fig. 5: Basic operation of DES

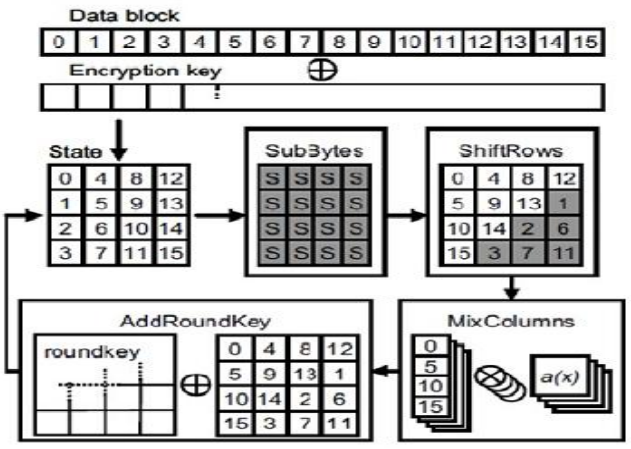

Fig 6 Round operation of AES encryption

6. ADVANTAGES AND APPLICATION

6.1 Advantages

1. Network security facilitates protection of information that is shared between computers on the network.
2. Hacking attempts or virus attacks from the internet will not be able to harm physical computers. External possible attacks are prevented.
3. Network security provides different levels of access. If there are various computers attached to a network, there may be some computers that may have greater access to information than others.
4. Private network can be provided protection from external attacks by closing them off from internet. Network security make them safe them virus attacks, etc

6.2 Applications

Sensor nodes are used in a variety of applications which require constant monitoring and detection of specific events. The most security-oriented applications of WSN are.

1. Military applications
2. Sensors are also used in environmental applications such as forest fire detection
3. Sensor can be extremely useful in medical applications.
4. Sensor also useful in commercial applications at home and industries

7. CONCLUSIONS

From this survey paper we can conclude that DES and AES are advanced security algorithm which provides secure or accurate information about sensed data in wireless sensor network. AES is a most dominant algorithm in wireless sensor network for coming decades like security oriented-applications such as military, medical, fire detection and home automations and variety of applications which require constant monitoring detection of specific event.

REFERENCE

[1]. Atulkahate, “Cryptography and network security” second edition,
[2]. James F. Kurose, “Computer networking”,
[3]. Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks”Communications of the ACM, Page53-57, year 2004
[4].Al-SakibKhan Pathan, Hyung-Woo Lee, ChoongSeon Hong, “Security in Wireless SensorNetworks: Issues and Challenges”, International conference on Advanced ComputingTechnologies, Page1043-1045, year 2006
[5]. A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public keycryptographyfor wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328