International Journal of Electronics Engineering, 2(1), 2010, pp. 111-113

Implementation & Analysis of Security Protocols for Wireless Sensor Network

Afrin Zahra[1], M. Nizamuddin[2] & Z.A.Jaffery[3]

[1]*ECE Deptt., Al-falah School of Engineering & Technoplogy, Faridabad- Haryana, India*
[2]*Electrical Engineering Deptt., F/o Engineering & Technology, Jamia Millia Islamia, New Delhi, India*

Abstract: The main goal of this paper work is to provide the flawless security protocols to the wireless sensor networks by using the RC5 cryptographic, and learn and understand the application of Image Processing for Biometric Application. First of all, in this paper we have the concise survey on sensor network constraints, security requirements, attacks and defensive measures which was read and understood in order to obtain enough knowledge about it. To illustrate the utility of our security building blocks, an authenticated routing scheme and a secure node-to-node key agreement protocol has been proposed. These elements are universal and apply easily to other sensor networks. Since primitives are solely based on fast symmetric cryptography, and use no asymmetric algorithms, in the absence of other constraints, how it is be possible to encrypt and authenticate all sensor readings. Since the data authentication, freshness, and confidentiality properties require transmitting mere bytes per unit, it is feasible to guarantee these properties on a per packet basis, even with small no of packets.

Keywords: RC5 Cryptographic, SNEP & µTESLA Security Protocols.

1. INTRODUCTION

The field of wireless sensor networks offers a rich, multi-disciplinary area of research, in which a variety of tools and concepts can be employed to address a diverse set of applications. Smart environments represent the next evolutionary development step in building, utilities, industrial, home, shipboard, and transportation systems automation. Like any sentient organism, the smart environment relies first and foremost on sensory data from the real world. Sensory data comes from multiple sensors of different modalities in distributed locations. The challenges in the hierarchy of detecting the relevant quantities, monitoring and collecting the data, assessing and evaluating the information, formulating meaningful user displays, and performing decision-making and alarm functions are enormous. The information needed by smart environments is provided by Distributed Wireless Sensor Networks, which are responsible for sensing as well as for the first stages of the processing hierarchy. Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium.

2. TYPES OF ATTACKS ON WSNS

2.1. Passive Information Gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

2.2. Subversion of a Node

A particular sensor might be captured, and information stored on it (such as the key) might be obtained by an adversary. If a node has been compromised then how to exclude that node, and that node only, from the sensor network is at issue (LEAP [1] defines an efficient way to do so).

2.3. False Node and Malicious Data

An intruder might add a node to the system that feeds false data or prevents the passage of true data. Such messages also consume the scarce energy resources of the nodes. This type of attack is called "*sleep deprivation torture*" in [2].

2.4. The Sybil Attack

In a Sybil Attack [3], a single node presents multiple identities to other nodes in the network. They pose a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. Authentication and encryption techniques can prevent an outsider to launch a Sybil Attack on the sensor network.

*Corresponding Author: zarreen_aijaz@yahoo.co.in, scs_manit@yahoo.com

2.5. Sinkhole Attacks

In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Effectively, the adversary creates a large "*sphere of influence*" [4], attracting all traffic destined for a base station from nodes several hops away from the compromised node.

2.6. Wormholes

In the wormhole attack [5], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them.

3. IMPLEMENTATION OF SNEP & µTESLA SECURITY PROTOCOLS

3.1. SNEP: Confidentiality, Authentication, Integrity and Freshness

SNEP uses encryption to achieve confidentiality and message authentication code (MAC) to achieve two-party authentication and data integrity. Apart from confidentiality, another important security property is semantic security, which ensures that an eavesdropper has no information about the plaintext, even if it sees multiple encryptions of the same plaintext [6].

3.2. RC5 Cryptographic

We have chosen RC5 as cryptographic primitive, with this techniques security systems can become an integral part of practical sensor networks. In this paper, the security of RC5 against differential and linear cryptanalysis has been focused.

We observe that the lengthy analysis of the Data Encryption Standard [7] prior to publication, though not public, resulted in an algorithm that has resisted attack.

RC5 is a parameterized algorithm, and a particular RC5 algorithm is designated as

RC5 – w/r/b.

We summarize these parameters below:

w The word size, in bits. The standard value is 32 bits; allowable values are 16, 32, and 64.

RC5 encrypts two-word blocks so that the plaintext and cipher text blocks are each 2w bits long.

r The number of rounds. Allowable values are 0, 1... 255.

b The number of bytes in the secret key K. Allowable values of b are 0, 1, ..., 255.

3.3. RC5 Consists of Three Components

A key expansion algorithm, an encryption algorithm, and a decryption algorithm, these algorithms use the following three primitive operations (and their inverses).

(1), Addition of words modulo 2w, denoted by \+".

(2), Bit-wise exclusive-OR of words, denoted by +

(3), Rotation: the rotation of x to the left by y bits is denoted by x <<< y.

Note that only the log2 (w) low-order bits of y affect this rotation.

3.4. Key Expansion Algorithm

In Key expansion, the key-expansion algorithm expands the user's key K to fill the expanded key table S, so that S resembles an array of $t = 2(r + 1)$ random binary words determined by K. It uses two\magic constants" and consists of three simple algorithmic parts.

The two word-size magic constants Pw and Qw are defined for arbitrary were follows:

P_w = Odd ((e – 2)2^w)

Q_w = Odd ((¢ – 1)2^w)

Where

e = 2:718281828459….. (base of natural logarithms)

¢ = 1:618033988749…. (golden ratio);

4. IMPLEMENTATION

In Key expansion algorithm,

Step one: The first algorithmic step of key expansion is to copy the secret key K [0, …, b-1] into an array L[0,…, $c – 1$] of $c = [b/u]$ words, where $u = w/8$ is the number of bytes/word. This operation is done in a natural manner, using u consecutive key bytes of *K* to fill up each successive word in L, low-order byte to high-order byte. Any unfilled byte positions of L are zeroed.

In the case that $b = c = 0$, we reset *c* to 1 and *L* [0] to zero.

Step Two: The second algorithmic step of key expansion is to initialize array S to a particular fixed (key-independent) pseudo-random bit pattern, using an arithmetic progression modulo 2w determined by the \magic constants" Pw and Qw. Since Qw is odd, the arithmetic progression has period 2w.

Create an expanded key table, $S[0...t – 1]$ have *t* entries, $t = 2(r + 1)$ *w*-bit words

Initialize array S

$S[0] = P_w$;

For $i = 1$ to $t – 1$ do

$S[i] = S[i – 1] + Q_w$;

Step Three: The third algorithmic step of key expansion is to mix in the user's secret key in three passes over the arrays S and L. More precisely, due to the potentially different sizes of S and L, the larger array will be processed three times, and the other array may be handled more times.

Mix the secret key into table, S

$i = j = 0$; $A = B = 0$; do 3 * max (t, c) times:

$A = S[i] = (S[i] + A + B) <<< 3$;

$B = L[j] = (L[j] + A + B) <<< (A + B)$;

$i = (i + 1) \bmod (t)$;

$j = (j + 1) \bmod (c)$;

The key-expansion function has a certain amount of "one- wayness": it is not so easy to determine K from S.

Encryption:

$A = A + S[0]$;

$B = B + S[1]$; $i = 1$ to r do for

$A = ((A \text{ xor } B) <<< B) + S[2*i]$;

$B = ((B \text{ xor } A) <<< A) + S[2*i + 1]$;

5. CONCLUSION

It is concluded that the RC5's algorithm provides good security against the four main attacks. Although it's a simple encryption/ decryption algorithms and still under scrutiny by other cryptanalysis attack.

RC5 is a fast block cipher designed to be suitable for both software and hardware implementation. It is a parameterized algorithm, with a variable block size, a variable number of rounds, and a variable-length secret key. This provides the opportunity for great flexibility in both the performance characteristics and the level of security.

REFERENCES

[1] Sencun Zhu, Sanjeev Setia, Sushil Jajodia. "LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks", *In The Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003.

[2] Sasha Slijepcevic, Miodrag Potkonjak, Vlasios Tsiatsis, Scott Zimbeck, Mani B.Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor Networks", *In The Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'02)*, 2002.

[3] J. R. Douceur, "The Sybil Attack," in1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[4] Chris Karlof David Wagner, *In Secure Routing in Wireless Sensor Networks: Attacks and Counter Measures*.

[5] Y.C. Hu, A. Perrig, and D.B. Johnson, "Wormhole Detection in Wireless Ad hoc Networks", *Department of Computer Science*, Rice University, Tech. Rep TR01-384, June 200_

[6] Shafi Goldwasser and Silvio Micali, "Probabilistic Encryption", *Journal of Computer Security*, 28:270–299, 1984.

[7] B. Kaliski and Y.L. Yin, "On Differential and Linear Cryptanalysis of the RC5 Encryption Algorithm", *Advances in Cryptology - Proc CRYPTO '95*, LNCS 963, pp. 171 - 184, Springer Verlag, 1995.