WIRELESS SENSOR NETWORKS BLOCK-CIPHER DESIGN FOR SECURITY

Brindha G MCA., (M.Phil.,)[*]

GopikaaRani N MCA., (M.Phil.,)*

Tharika B M.Sc.,(M.Phil.,)*

Abstract –

Wireless **S**ensor **N**etworks **(WSNs)** are exposed to a variety of attacks. The quality and difficulty of attacks are increasing day by day. The future work aims at showing how the difficulty of modern attacks is growing accordingly, leading to a similar rise in methods of resistance. Limitations in computational and battery power in sensor nodes are constraints on the diversity of security mechanisms. We must apply only suitable mechanisms to WSN where our approach was motivated by the application of an improved Feistel scheme. The modified accelerated-cipher design uses data-dependent permutations, and can be used for fast hardware, firmware, software and WSN encryption systems. The approach presented showed that ciphers using this approach are less likely to suffer intrusion of differential cryptanalysis than currently used popular WSN ciphers like DES, Camellia and so on.

Keywords: Security, Cipher, Wireless sensor network (WSN), Feistel scheme.

[*] MPhil Scholar, KG college of arts and science, Saravanampatti, cbe-641 035.

INTRODUCTION

The goal of information security is to provide information safety and integrity. Information transfer through wireless sensor network (WSNs) needs to be protected from misuse.

Modern security methods need to guarantee the safety of data transmission with respect to security needs, i.e., confidentiality, integrity and availability (CIA). Providing information security in WSN is also necessary especially for those security-sensitive applications and is one of the major concerns of our proposal.

There are many counter measure methods that have been extensively studied to provide WSN communication security. These defenses are ineffective against attacks from compromised servers due to the WSN level constantly increasing, and attacks are becoming more and more complicated.

WSN has some restrictions when it comes to its applications, like limited power supplies, low bandwidth, small memory sizes and limited energy, which make it more vulnerable. And as information becomes more valuable and costly, intruders use more complicated methods in attacking WSN, this eventually makes the security issue highly sensitive. Due to the increase in new trends of attack, previous security methods cannot combat or resist modern attacks. We present additional steps to create efficient security mechanisms for WSN, with limited resources.

Our study shows that new and more stable security approaches need to be put in place to provide information safety taking into consideration the following attributes: availability, confidentiality, integrity, authentication and non-repudiation. We propose to use a modified accelerated-cipher using permutation.

The concept of ‘data-dependent’ (DDP) is an approach used in many information security systems today Moldovyan and Moldovyan. Confronting the key challenges, we follow this approach by using a Feistel scheme approach to present our improved cipher block using DDP. By cryptanalysis realization, it is necessary to consider differential and linear properties of individual round transformation of crypto primitives of block ciphers. This method allows us to create more stable secure mechanisms against modern types of attacks and also to provide a highly accelerated security program within small sensor devices. In this paper we use a controlled permutation boxes based method for block cipher against modern crypto attacks such as differential cryptanalysis in WSN. The proposed cipher has free key preprocessing which provides high performance.

In frequent keys exchange. In our work we show the effectiveness of using DDP in cipher design for WSN. DDP-based ciphers demonstrate better experimental results than others.

ATTACK THREATS

Crypto attack methods are very complicated. They combine mathematics, information science and even electronics with unusual thinking. WSN block cipher design needs to consider stability against analytical crypto-attacks. The practice in past years has shown us differential cryptanalysis and linear cryptanalysis (LCA) where the most powerful analytical crypto analysis methods were used. The main content of DCA is the propagation analysis of the influence of modifications in the plaintext on the modification in cipher text(propagation properties). Using DCA as a method of complex attack with complicated mathematical methods can be one way of verifying the stability of block ciphers.

In the realization of block cipher cryptanalysis it is necessary to consider the differential and linear properties of individual round transformation crypto primitives of blocks. The cases are complicated to element addition on stable round transformation which sometimes might give negative results for a given cipher algorithm. Block cipher designers who are trying to use theoretical computing constructions that provided distinctness in the evaluation of block ciphers in modern cryptanalysis methods, should give consideration before putting all these into action.

In spite of DCA and security precautions there are many more threats to new modern networks. One of the main challenges is the design of these networks and their vulnerability to securirty attacks, which leads to network destruction and poor performance. Every year the attack complexity increases as can be seen in.

Every year not only are the quantity and complexity of new threats rapidly increasing but also their apperance and momentum. Resistance against them is becoming more and more complicated. The malicious are using more of these security vulnerabilities especially to attack WSN due to the weakness in wireless security.

EFFICIENCY OF EXISTING WSN ALGORITHMS

We outline briefly the drawbacks of existing algorithmic methods which are being used in many current technologies:

- Widespread algorithms (end to end, single destination transmission, IP surface);
- Probabilistic broadcasts (discrete effort:does not handle disconnection);
- Scalable reliable multicast (multicast over a wired network, latency-based extinction);
- SPIN (propagation protocol: does not address maintenance costs);
- Public-key cryptography (too expensive);
- Fast symmetric-key ciphers (must be used sparingly)

On designing WSN protocol it is necessary to consider all specific features of WSN. For example, communication bandwidth is extremely limited in these networks: each bit transmitted consumes about as much power as executing 800~1000 operational mandate, and as a outcome, any message augmentation caused by security mechanisms comes at a significant cost. However, we present sets of requirements for WSN protocols.

We use these requirements as the highlight in facilitating the design of our new improved cipher:

- ✓ Low maintenance overhead (minimize communication when everyone is up to date);
- ✓ Rapid propagation (when new data appear, they should propagate quickly);
- ✓ Scalability (protocol must operate in a wide range of densities, and cannot require a priori density information);
- ✓ Technical cryptanalysis stability (high-frequency influence of sensors with the purpose of information distortion. Some of the previous methods allow us to get the key's round value. Latest research shows that block ciphers are resistant to this kind of attack).

TECHNIQUES

The presented techniques are based on an original Feistel scheme which due to its significant properties can be used in WSN security applications. The modified Feistel scheme design can meet today's security challenges and generates high-quality results.

Feistel Scheme

All of WSN's block ciphers are designed using a 16-round Feistel data block encoding scheme realized by two sub-blocks of data transformation using the round encoding function. Like many other symmetric block ciphers, DES is also a Feistel network.

In a Feistel network the plaintext is divided into two halves from the first round of computations which is repeated a number of times(i.e., in subsequent rounds). Generally the output of the ith round is determined from the output of the previous round in the following way:

Li=Ri-1,(1)

Ri=Li[]F(Ri-1,ki),(2)

Where F() represents the round function; ki is the key for the ith round; Li and Ri are the left and right input data bits of the ith round, respectively.

The advantage of a Feistel scheme is that the block cipher used is very difficult to breach by proportional of one round key(2m) enumeration. So it is necessary to determine the requirements for one round cipher transformation during the Feistel scheme design. We briefly indicate below the essential design needs:

- Increase size of the transcriptive block to 128 bits and more;
- Increase the round key size;
- Provide round key elements inseparability within the limits of one algorithm round;
- Use the special methods which avoid mathematical and technical analysis especially the addition of some transformations at the beginning of the algorithm and after the last round.

Before implementing Feistel scheme to network security we would also like to ananlyze the pros and cons of this approach for a network as follows:

Advantages of a Feistel schemes to networks:

(1) In a Feistel scheme we can encode and decode in one operation sequence. Encoding an algorithm modification is achieved by queuing a round of sub-keys using modification.

(2) It minimizes software coding.

Disadvantages of a Feistel approach to networks:

(1) In a Feistel scheme we have two parts, left and right, but only one part of the block is used for coding in one round.

For **Example,** if the block on the right side (R) is used for the first time in coding, the second one on the left side (L) is only used for exchanging places, and thus not all parts of the block are participating in the coding process.

(2) Transformation is very simple because the round function F depends only on two parameters (L and round key Ki).

For understanding our presentation we give further destabilizations in this paragraph, giving a Feistel scheme as one of the standards we elaborate in detail how a Feistel scheme works. The right part R' of transcriptive data L'||R' is a result of group operation XOR([]), where Ki F is a round function, i is a round quantity and Ki is a round key(). Ki R'=R[] F L.

This Feistel scheme appeared long before modern crypto-attacks as the original cipher using a block structure. Its modified version is applied further to limited resource devices as well as embedded devices.

From the original standard version it is seen that the unmodified version does not meet the new security requirement paradigm. The latest record in cracking DES set by the Electronics Frontier Foundation's "Deep Crack", is 22 h and 15 min. It involved about 100 000 PCs on the Internet. It was performed as a 'known cipher text attack' based on a challenge from RSA Laboratories.

The task was to find a 56-bit DES key for a given plaintext and a given cipher text. It is well demonstrated.

Theoretical Approach Of CPB To Our Methodology

In our work we propose to use controlled permutation boxes for implementation of a Feistel shceme design for WSN security. DDP can be performed with the so-called 'Controlled Permutation Boxes' (CPBs) which are fast even if implemented in cheap hardware. CPB is one part of the comprehensive forthcoming start of controlled operations in security applications. The main content of this concept is to create substitution and permutation elements of block ciphers. They provide highly accelerated program realization nonlinear transformations with a small volume of modifications. These transformations are realized by the whole large size data block at once and are managed by transcriptive data and the algorithm's keys dynamically. CPB mechanisms and their implementation in block cipher methods provide high stability of such algorithms in modern crypto-attacks such as differential cryptanalysis.

WSNs use the block-algorithm encryption for data transfer. The quality of these algorithms dep-ends on indexes of binary information 'disp-ersion' and 'interfusion' which provide inter-change of substitution and permutation trans-formaions. In the modern block ciphers these transformations are used by applying two types of crypto primitives:

(1) Special nonlinear S-box given at the table view. S-boxes provide a degree of non-linearity for each block and a degree of error propagation. But the small size of S-boxes also makes

it difficult for the encoding data block to achieve high indexes for the following parameters: nonlinearity degree, error propagation degree and guessing correlation level.

(2) Standard arithmetic or algebraic operations realized with computer commands. Arithmetic operations are effective in software implementation and not complicated in hardware implementation. They have high correlation insusceptibility for all encoding blocks but a low degree of nonlinearity and error propagation.

This modern approach does not guarantee maximum security when using a Feistel scheme as it has some disadvantages. Attempting to solve this problem we employ controlled operations to make an important adaptation of controlled permutation boxes. Controlled operations are described as simpler operations 'multiples' that are selected depending on some controlling code. CPBs are an alternative to traditional S-boxes and common mathematical operations that generally use a block cipher synthesis. Thus the availability of special crypto primitive creations is becoming obvious. These crypto primitives combine and optimize the advantages of block cipher substitution transformations.

CONCLUSION

In this paper we have presented an advanced improved Feistel cipher based scheme which can be used in WSN block-cipher design for security by using CPB crypto primitives. Also we have shown how new generation attacks are increasing with how new generation attacks are increasing with time, becoming complicated and mitigating against WSN and other fields. In comparison our analysis verified that there is less probability of code breakage with a modified Feistel scheme.

Our study argues that there is a benefit in using an improved Feistel scheme for WSN security, as it is much easier to encrypt the data packet than to encrypt the data stream, which most of the encryption standards are being used for at present. However, an improved Feistel scheme can attain high and stable WSN security using block-ciphers compared to differential cryptanalysis. Due to the use of energy-efficient sensors, the security design of the modified ciphers is appropriate. This work serves as a notification and milestone in attracting more attention to WSN security and DDP-based block-cipher applications information.

REFERENCES

1. Biham, E., Shamir, A., 1993. Differential cryptanalysis
2. Bilstrup, U., Sjoberg, K., Svensson, B., Wiberg, Capacity Limitations in Wireless Sensor Networks
3. Bodrov, A.V., Moldovyan, A.A., Moldovya DDP-based ciphers: differential analysis of Spectr-H64
4. Goots, N.D., Moldovyan, A.A., Moldovyan, N.A., 2001
5. Pister, K., Hill, J., Woo, A., Hollar, S., Culler, D., Szewczyk, R., 2000. System architecture directions for networked sensors.