A new security architecture for mesh networks: Application to sensor networks and ZigBee standard

AKLI M. REDJEDAL[1,2], KHALED GARRI[1],
SAMIA BOUZEFRANE[1] and PASCAL THONIEL[2]

[1]**CEDRIC Laboratory, Conservatoire National des Arts et Mtiers**
292 rue Saint Martin, 75141, Paris Cdex 03, France

[2]**NTX Research SA**
111 avenue Victor Hugo, 75116 Paris - France

***Abstract*—The IEEE 802.15.4 specification proposes a new protocol dedicated to network small devices with low power consumption and personal area. This specification includes a number of security options that reduce safety. In this paper, we highlight a new technique for ZigBee networks to improve safety and security.**

***Index Terms*—IEEE 802.15.4, Zigbee Standards, Sensor Networks, Key management, Security, Authentication.**

I. INTRODUCTION

The 802.15.4 specification describes the communication protocols between small wireless devices so that they communicate with each other with low cost. These protocols are intended for the development of applications on a dedicated system on chip. These applications often use embedded devices controlled by a 8 or 16 bits microcontroller. Because of limited resources and energy, the software that runs on these devices should be simple and small, and the devices shall manage their low energy by minimizing the amount of data transmitted. On the other hand, many applications need to handle security issues such as privacy, integrity, etc.

ZigBee specification, still under consideration, is a high-level library using the 802.15.4 API to export these specific services. Designed for low power consumption and low flows, ZigBee is a mesh, self-organizing sensor networks. With the benefits of high availability, low cost and low resource, ZigBee is ideal for commercial, industrial or residential applications.

In this paper, we propose a cryptography-based XC technologies for the safety of the ZigBee networks. The proposal helps to reduce the response time, resource requirements and complexity of the system, while keeping the network secure.

- Samia Bouzefrane is Associate Professor at the CEDRIC Lab of CNAM, samia.bouzefrane@cnam.fr.
-Pascal Thoniel, is CEO & CTO of NTX Research, thoniel@ntx-research.com
-Khaled Garri, is PhD student at CNAM Paris, khaled.garri@gmail.com
-Akli M. Redjedal, is Master student at CNAM Paris, redjedal.akli@gmail.com

II. ZIGBEE SECURITY

A. Specifications

A ZigBee security protocol should provide a basic security services:

- Identification and Authentication: Is the process of claiming/getting respectively proving/verifing the identity of a user, process, or device, as a prerequisite for granting access to resources in the network.
- Authorization: is the process of granting specific access rights to resources of the network.
- Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. *A loss of confidentiality is the unauthorized disclosure of information* [1].
- Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. *A loss of integrity is the unauthorized modification or destruction of information* [1].
- Protection against replay: Prevent an opponent to replay a legitimate message sent between two allowed nodes, the receiver will receive the new because it has a valid MAC.

Current ZigBee security [2] uses advanced encryption standard, AES for encryption, with other mechanisms to improve security. But the symmetric security scheme does not take full advantage of the strengths of public key cryptography without involving the trust center, like in the session key process and in the digital signature. Due to strict security requirements, the ability of ZigBee communication devices to authenticate each other is required. Some recent work has proposed using the public key for the safety of ZigBee ([3], [4]) or identity-based cryptography [5], based on public key cryptography [6], using each entity id as a public key.

B. Trust Center

The cornerstone of classic security architecture for ZigBee networks is the Trust Center (TC). TC is typically an application running on a ZigBee device, that is unique in every ZigBee network. As a key central component of ZigBee security, the TC is assumed to run on a more powerful device (e.g. a coordinator) rather than a regular ZigBee end device. TC :

- Stores the keys for the network.
- Uses the security services to configure a device with its key(s).
- Uses the security services to authorize a device onto the network.

The first task of the TC is to create and distribute the Network Keys (NK). TC is fully responsible for creating and distributing the NK, therefore there is no role of the devices in NK establishment.

C. Key management

The NK is the mere mandatory key in a ZigBee network. The NK is a common key shared among all the devices (nodes) and used to secure broadcast communications. A device shall acquire a NK via key-transport or pre-installation (for example, during factory installation). The details of the NK update protocol is given in the specification and explained in [24]. It is assumed that when TC updates the key, all the devices in the network successfully update their keys. Compromise of a NK affects all the devices in a network. Two more types of security keys may exist in a ZigBee network depending on the security configuration :

- Master Key (MK),
- Link Key (LK). Unlike NK, those keys are pairwise shared.

Link Keys are secret session keys used between two communicating ZigBee devices. This key is unique to a pair of devices that are communicating with each other and is derived from their respective MK. A device shall acquire LKs either via key-transport, key-establishment, or pre-installation.

Broadcast communications are secured by means of a 128-bit NK shared amongst all devices in the network. Unicast communication between application peer entities is secured by means of a 128-bit LK shared by two devices.

In order to mitigate the risk of using a compromised security key in a ZigBee network, the key should be updated fairly often. On the other hand, this operation is computationally expensive and we would not like to perform it too often. Unfortunately, the ZigBee specification does not give any advice on this how and when the key shall be updated?. In brief, all the specification documents of ZigBee leave the important key update issue to the implementations. Three approaches are possible :

- Time-based key update,
- Leave-based key update,
- Join-based key update.

III. A new security architecture for ZigBee

In this study, we develop a New Security Architecture (NSA) for ZigBee and addressed the major issue of the current centric model/scheme. We focused on technical cryptographic and key management issues across the scope of systems and devices found in the ZigBee network. We present alternatives to existing security standards, methods, or technologies, and their optimal adaptations for the ZigBee network.

- How is it possible to manage security in a mesh network like ZigBee?
- Without unsortable maze of provisioning and managing shared secret keys.
- without resorting to the centralization of key security.
- without being dependent on a classic PKI solution and suffering its drawbacks and disadvantages.

Our solution is based on :

- in-built ”mesh” security architecture,
- XC dissymmetric key management rather than symmetric (only two XC matrices per entity),
- innovative asymmetric key management dedicated to specific purposes but without the complexity of PKI.

A. XC technology to encrypt data

XC matrices are dedicated to encrypt session keys or small size secrets. XC matrices are not suited to encrypt huge amount of data stored or flowed. In that last case, XCC (XC Confidentiality) is used as a part of a hybrid crypto-system in combination with a symmetrical algorithm like AES.

In 1996, NTX Research uses the coding tables by inventing matrix authentication protocol in challenge-response. The coding tables are dictionaries of characters pseudo-randomly generated that allow users to communicate in challenge-response mode based on the principle of the ”naval battle”. The challenge corresponds to the table coordinates randomly selected and the response is the value found in the table using the coordinates of this challenge (see Fig. 1).

B. XC Authentification (XCA)

Authentication is the process of confirming a claimed identity. All forms of authentication are based on something you know, something you have, or something you are. XCA authentication based on XC table is strong because it combines two factors:

- What I own: a physical element (owned by the user), all these materials can be used alone or in combination to authenticate. There is no limitation, only the ability to store a flat file!
- What I know: The secret code XCA, unlike other solutions, is not stored electronically. It is only in the brain of the user and therefore cannot be divulged without his consent.

In our case, the secret codes used in the challenge-response authentication process are (see Fig. 2):

- The secret code of the user is ”+1,+1”
- The secret code of the server is ”+2,+2”

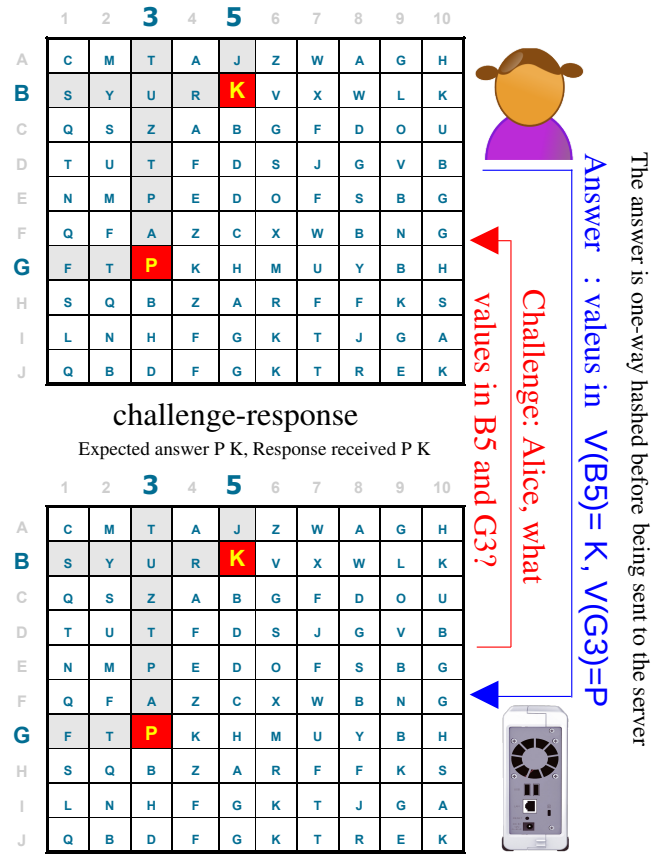

Fig. 1. XC technology with challenge-response protocol

The challenge is generated pseudo-randomly by the server: for example, ”B5”. This challenge is sent to the user on the client side:

- The user is asked to enter his secret code (+1,+1)
- The local applet/midlet transforms the initial challenge ”B5” to ”C6” (B+1= C, 5+1= 6)
- The value found in the coordinates ”C6” in user table is stored in the authenticator ”K”.
- The answer ”K” is sent to the server. This is One Time Password (OTP).

Then, the server reads from its own table the value with the appropriate coordinates, that is:

- The server reads from its memory the secret code of the administrator (2 +2), which transforms the initial challenge ”B5” to ”D7” (B 2 = D, = 7)
- The server found in coordinates ”D7” of the table stored in the user side the value ”K”.
- If the user response matches with the server response, the user is authenticated.

The secret codes are not stored anywhere in the information system, and do not transit in the network because they are memorized only by the users (5 alphanumeric characters are sufficient) and are not shared. Moreover, there is no repudiation because the server ignores the secret code of the user. In fact, if the support containing the table is stolen, the hacker cannot find the secret code of the user. Hence, the values computed in the table are wrong, and the hacker cannot

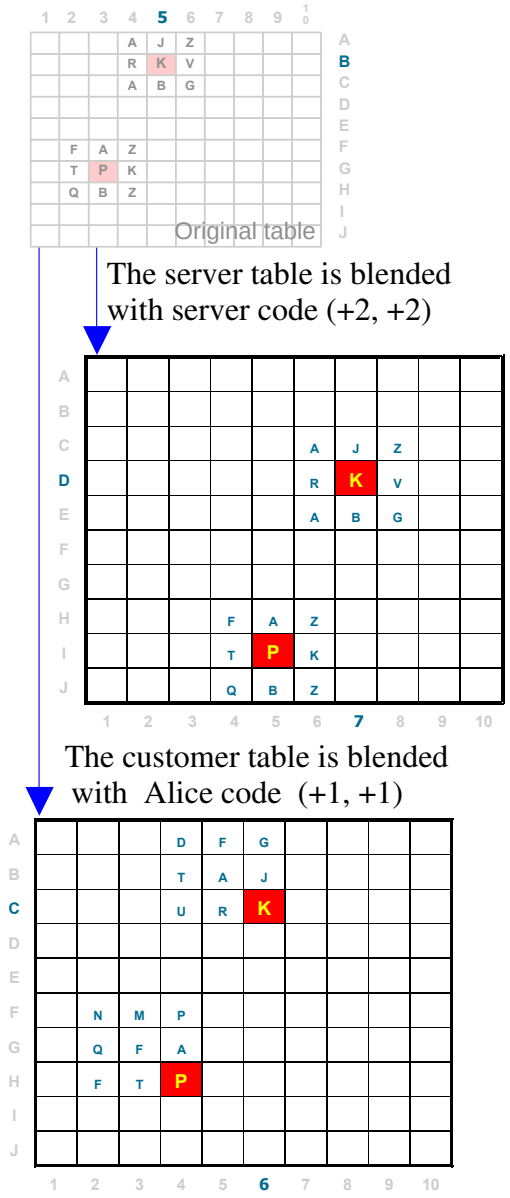

Fig. 2. Authentication process based XC technology and secret code

test all the combinations without detecting it by the server.

C. XCA: economic benefits and security

The authentication solution XCA works according three modes: web-web, web-mobile and mobile-mobile. This solution does not require a specific operating system or additional hardware to be installed on PCs, mobile or smartphones, as it is 100 % software compatible with all physical authenticator.

The security level can be adjusted depending on the issues and the maturity of consumers (medium, high, very high). It ensures both of security against eavesdropping and the security against the loan, the loss or theft of the authenticator (inviolable secret code).

Like for credit-card purchase, the user/customer:

- can choose his secret code without size or characters constraint.
- can change his secret code at any time ”offline”.

- can receive an option to alert code under constraint, totally undetectable when the stakes are important.

IV. Conclusion

In this paper, we propose to apply XC matrix for providing security in ZigBee networks. The paper presents some features of ZigBee network and its current security issues. It then summarizes some characteristics of XC cryptography and proposes an idea to use XC matrix for providing authentication process in ZigBee networks. Unlike symmetric key schemes, the use of XC cryptography has the advantage of public-key cryptography, which is more efficient in term of key management. It also helps to provide identification and non-repudiation, which is very important for critical applications. Unlike public-key cryptography, XC cryptography is simpler regarding key management and thus, is optimized in resource-sensitive environment like ZigBee.

References

[1] *Standards for Security Categorization of Federal Information and Information Systems*. National Institute of Standards and Technology (NIST).

[2] Z. Alliance, *ZIGBEE SPECIFICATION*, January 17, 2008. [Online]. Available: http://www.zigbee.org/Specifications.aspx

[3] M. Blaser, "Industrial-strength security for zigbee: The case for public-key cryptography. embedded computing design," 2005.

[4] ——, "Securing zigbee: Building robust, reliable sensor networks," p. v12 n2 p18, 2006.

[5] S. T. Nguyen and C. Rong, "Zigbee security using identity-based cryptography," in *ATC*, 2007, pp. 3–12.

[6] S. Goldwasser, "New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a match made in heaven)," in *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 1997, pp. 314–. [Online]. Available: http://dl.acm.org/citation.cfm?id=795663.796386