CERTIFICATELESS SCHEME BASED NTRU CRYPTOSYSTEM FOR AD-HOC UWB-IR NETWORK

Jamel Miri[1], Bechir Nsiri[1], and Ridha Bouallegue[2]

[1]National Engineering School of Tunis, Sup'Com, Innov'Com Laboratory, Tunisia
[2]Sup'Com, Innov'Com Laboratory, Tunisia

Email: jamel.miri@laposte.net, bechirnsiri@gmail.com, ridha.bouallegue@supcom.tn

ABSTRACT

From the radar and military research world's, the Ultra-WideBand Impulse Radio (UWB-IR) was adopted in the telecommunications world in the 1990'. Currently, the UWB-IR technology is an interesting candidate for close range Wireless Sensors Networks (WSNs). It is particularly attractive for industrial sensor networks due to its resilience to multipath interference, simple transceiver circuitry, accurate ranging ability, and low transmission power. In order to secure data and communications in the Ad-Hoc UWB-IR networks, UWB-IR requires suitable encryption protocols. In this paper, we review and summarize the IEEE 802.15.4 security sub-layer protocol of UWB-IR based Symmetric Key Cryptography scheme. Then, we highlight the different vulnerabilities and weaknesses present in this type of scheme. Finally, we prove, after a deep examination of multiple Public Key Cryptography (PKC) schemes, that the certificateless one is the most suitable for Ad-Hoc UWB-IR networks characterized by nodes mobility. Indeed, we have also evaluated and analyzed the different public key cryptosystems (PKCS) and concluded that NTRU is the most optimum public key cryptosystem to be used with the certificateless scheme in order to secure data and communications in Ad-Hoc UWB-IR Networks. This is due to the fact that it is the fastest PKCS to provide different security levels at a high speed with very constrained resources.

KEYWORDS

Ad-Hoc Networks, Certificateless, NTRU, Public key cryptography, Public key cryptosystems, Ultra-WideBand Impulse Radio.

1 INTRODUCTION

The Ulra-WideBand (UWB) technology is fairly new in the field of wireless communications. It was originally used for military radar and imaging systems. Its use for military application is very obvious due to its characteristics of low detection and interception probabilities, which allows secure transmission. Nowadays, Ad-Hoc UWB-IR networks are used to establish communications between different groups of soldiers during tactical operations.

In 2002, the FCC authorized the unlicensed commercial use of UWB spectrum. Since this date, there has been a great interest to apply UWB-IR technology in wireless communications. In terms of wireless communications, UWB transmission can be generally divided into two main categories: low data-rate (LDR) for long-link-distance applications, and high data-rate (HDR) for short-link-distance applications [1]. In terms of standardization, UWB-IR technology was standardized as an alternative to ZigBee physical layer with the standard IEEE 802.15.4a-2007 [2]. It was also

standardized in 2012 as a possible physical layer for BAN networks with the IEEE 802.15.6 standard [3].

Like all WSNs, the Ad-Hoc UWB-IR networks are more vulnerable to different types of attacks (mainly active and passive) than the wired networks due to the lack of central coordination and shared wireless medium. Active attacks disrupt the operation of the network. Passive ones refer to attempts made by malicious nodes to perceive the nature of activities and to obtain information transacted in the network without disrupting its performance. The major security issues that exist in Ad-Hoc UWB-IR networks are as follow: Denial of service, resource consumption (Energy depletion, Buffer overflow), host impersonation, information disclosure and interference.

The major issue when implementing a symmetric key cryptography (SKC) in any type of network including Ad-Hoc UWB-IR one is the secure exchange of different symmetric keys (n nodes require $n.(n-1)/2$ keys). In fact, Public Key Cryptography (PKC) overcomes this weakness. Thus, it provides a robust security model. However, the only requirement is to select the best Public Key Cryptography scheme and optimum Public Key Cryptosystem (PKCS) algorithm for such resource constraint sensor network environment that has less communication as well as less computational overhead. Furthermore, the packets must be lightweight in order to decrease the large amount of time needed to transmit large files [4]. Indeed, we prove that the Certificateless scheme based NTRU public key cryptosystem is the optimum way to implement public key concept in Ad Hoc UWB-IR environments.

This paper is organized in the following manner. The next section gives a brief review of the security of IEEE 802.15.4 protocol based upon Symmetric Key Cryptography (SKC) scheme and the problems associated with the use of Ad-Hoc UWB-IR Networks. Section 3 gives a servery of the commonly used Public Key Cryptography (PKC) schemes and demonstrates how the Certificateless (CL) scheme is the best security solution for Ad-Hoc UWB-IR wireless networks on harsh environnements. Finally, section 4 evaluates and compares the security level of Public Key Cryptosystems (PKCS) and proves how the NTRU is the most efficient and optimum algorithm for CL-PKC in the Ad-Hoc UWB-IR Networks.

2 IEEE 802.15.4 SECURITY OVERVIEW

The IEEE 802.15.4 MAC sub-layer can provide security services when it is requested by higher layers. Thus, security services, including access control, data encryption, frame sequential freshness, and integrity can be provided. Also, the used protocol provides different security modes such as ACL, secured, and unsecured modes. However, there is no implementation of security measures in the unsecured mode.

Indeed, the IEEE 802.15.4 offers three different security levels. These levels are depicted in Fig 1: the CTR security level provides confidentiality; the CBC-MAC security level provides authentication and replay detection; and, finally, the CCM security level provides authentication and confidentiality. Furthermore, there are three fields related to the security in the IEEE 802.15.4 MAC frame:

- Frame Control (MAC Header).
- Auxiliary Security Control (MAC Header).
- Data Payload (MAC Payload field).

The Auxiliary Security Frame Fig 2 has 3 subfields :

- Security Control (1 Byte): defines the protection type.
- Frame Counter (4 Byte): replaying protection of the message.
- Key Identifier (0-9 Byte): specifies the used key information.

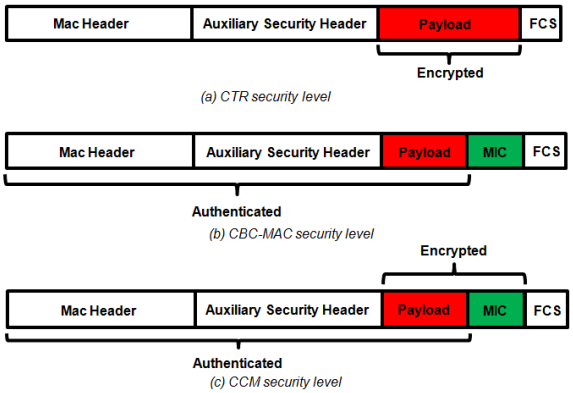

Fig. 1. MAC Frame IEEE.802.15.4.

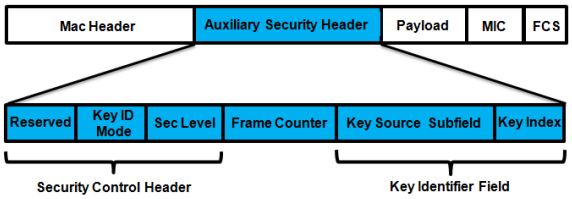

Fig. 2. Auxiliary Security Frame for IEEE.802.15.4.

2.1 ACCESS CONTROL LIST MODE

In Access Control List (ACL) mode, a node can communicate with some other network nodes previously selected by it. The communication is achieved using the maintained ACL. Each record contains the PAN identifier, the 64 bit extended address, the short address, the security suite and the related keying material of the device. The address of a source node of an incoming message is compared with ACL. The result can be passed to the higher layers which decide whether to accept or reject the message.

2.2 SECURED MODE

In Secured mode, different combinations of security options can be used. ACL functionality and cryptographic protection can be combined by MAC sub-layer on incoming and outgoing frames. The Advanced Encryption Standard (AES) algorithm is used. The security measures can be selected considering the following:

- **Access Control**: This service is as described above for ACL mode, but the messages which come from unauthorized sources cannot be passed to the higher layers.
- **Encryption**: Data is encrypted at the source and decrypted at the destination using the same key. The devices, which have the correct key, can only decrypt the encrypted data. Command, data and beacon payloads can only be encrypted.
- **Integrity**: A Message Integrity Code (MIC) can be added to a message. This integrity code allows the detection of any message tampering by devices which don't use the correct encryption or decryption key.

– **Sequential Freshness**: A frame counter can be added to a message. A device can determine how recent a received message is. Some appended values are compared with stored values in the device. The order of messages is checked. This procedure protects against replay attacks.

2.3 SECURITY SUITES FOR UWB-IR

Security is handled at the MAC layer. The application specifies its security requirements by setting the appropriate control parameters into the radio stack. Indeed the security is not enabled by default. An application must explicitly enable it. The acknowledgement packets don't support security, other packet types can optionally support integrity and confidentiality protection. An application has to choose the security suites to enable the type of security protection to protect the transmitted Data packets. Each security suite offers a different set of security properties and different packet formats. There are eight different security suites defined in IEEE 802.15.4, we can classify them into four categories by the properties they cover:

– No security (NO SEC).
– Encryption only (CTR).
– Authentication only (CBC MAC).
– Encryption and authentication (CCM).

The authentication category comes in three variants related to the size of the Message Integrity Code (MIC) it offers. Each variant is a different security suite. In fact, the MIC can be either four, eight, or sixteen bytes long. Table 1 summarizes all possible security suites used within the IEEE 802.15.4 standard.

Table 1. Security suites and options for IEEE 802.15.4 .

Security Level Identifier	Security Suites	Data Confidentiality	Data Authenticity
0x00	Null	OFF	NO (M=0)
0x01	AES-CBC-MIC-32	OFF	YES (M=4)
0x02	AES-CBC-MIC-64	OFF	YES (M=8)
0x03	AES-CBC-MIC-128	OFF	YES (M=16)
0x04	AES-CTR	ON	NO (M=0)
0x05	AES-CCM-32	ON	YES (M=4)
0x06	AES-CCM-64	ON	YES (M=8)
0x07	AES-CCM-128	ON	YES (M=16)

The IEEE 802.15.4 standard is based upon Symmetric Key Cryptography (SKC) with the adoption of AES-128 (Advanced Encryption Standard) algorithm with 128 bit key length encryption. The incorrect application suites of a good algorithm can morever destroy security. This can be avoided by so-called encryption modes, i.e. how a cryptographic algorithm is applied. The encryption is a defence technique against passive attacks (eavesdroppers,...). But, it is important to protect yourself from active attackers who send maliciously modified messages. The cryptography can detect unauthorized sent or modified messages by appending cryptographic checksums, so-called MACs (Message Authentication Code), in this context named MICs (Message Integrity Check). Indeed, the MIC guarantees that the message is generated by the sender and not by the attacker. The MIC proves that the secret key is not leaked. The CCM encryption mode allows to enable the integrity protection. Furthermore, the integrity protection has some important consequences:

- The message payload can not be modified by the attacker.
- The sender ID in the MIC excludes the spoofing attack.
- The frame counter in the MIC computation excludes replay attacks.
- The time stamps in the MIC computation excludes delay attacks.

2.4 VULNERABILITIES AD-HOC UWB-IR NETWORK BASED SKC

Symmetric key cryptography is used because it is much faster, and easier to implement. Indeed, due to the use of CCM mode in UWB-IR, only AES encryption is used. This allows simpler (and smaller) software and reduced encryption hardware. Furthermore, the same key is used for authentication and encryption, without compromising security. Thus key initialization is rare, firmware becomes smaller and faster. However, the use of SKC in Ad-Hoc UWB-IR Networks procures several disadvantages:

- ***The Key transfer is risky***: If the master key, which has to be distributed during initialization by out of band ways is compromised, security might be lost.
- ***The CCM mode allows encryption without authentication***: This mode is insecure.
- ***The message is encrypted twice***: First for the MIC computation, and second for the encryption itself.
- ***The MIC encryption is not necessary***: Due to the nonce structure, there are no identical payloads.
- ***The design of CCM mode is bad***: The criticisms are classified into five categories: efficiency, parameterization, complexity, variable-tag-length subtleties, and some wrong security claims. Other modes like EAX are more elegant [5], [6].

3 PUBLIC KEY CRYPTOGRAPHY SCHEME FOR AD-HOC UWB-IR NETWORK

Asymmetric Key Cryptography or Public Key Cryptography (PKC) scheme came to solve the problem of key management in Symmetric Key Cryptography (SKC) used in WSNs. Indeed, PKC provides two keys to each user (Secret (private) Key=sk, Public Key=pk). The pk is used to encrypt the messages and the sk is used to decrypt them. Moreover, the public key cryptography can ensure confidentiality, integrity and authentication. Many schemes of PKC are proposed:

- Public Key Infrastructures.
- Identity-Based Cryptosystems.
- Self-Certified Keys
- Certificateless Public Key Cryptography.

3.1 PUBLIC KEY INFRASTRUCTURE (PKI)

The PKI scheme needs Trusted Certification Authority (CA) to issue certificates and verifies the link between the key-pair to a defined entity in network. The CA is the stone corner of Public Key Infrastructure (PKI). Often, the CA achieves these specification rolls: The management of generation, distribution, renewal and publication of these keys.

During setting up a PKI, the most challenge is handling trust management. Indeed, the conventional solution is using certificates. Moreover, Certificates are issued by trusted central authorities and are cryptographically hard to forge but they are not easy to set-up and pose operational difficulties [7]. Furthermore, no universel solution is recommended to deploy a PKI. Many considerations must be taken to make it work properly [8].

The CA which composes the public key infrastructure (PKI) is recognized as the efficient and powerful tool to ensure key management in conventional networks. However, PKI is omitted to use in WSNs, because of its great consumption of energy and bandwidth. Indeed, various reasons limited the success of PKIs in WSNs:

- Certificate Revocation.
- Handling authorization and audit.
- Managing certificate chains.
- Storage and distribution of certificates.

Besides, the computational cost of certificate verification (time, power, memory,...) is an important point of contention, specially for mobile devices [9] like UWB-IR.

3.2 IDENTITY-BASED CRYPTOSYSTEMS (IBC)

Due to the factors discussed in the previous paragraph, inadequate deployment and management of PKIs can compromise the security of the wireless networks. Hence, the need to find another solution to simplify certificates management rises. The first solution developed by Shamir in 1984 the notion "Identity-Based Cryptosystems and Signature Scheme was proposed"[10]. The idea is to use a unique identity (ID) for the user (MAC address, IP address ...) to derive its pk. This identity ID is used to send him encrypted messages. Indeed, This allowed parties to:

- Communicate securely without the need to exchange pk or sk.
- Retain the key directories.
- Use the services of a third party.

The advantage of the IBC scheme is to simplify certificate management when compared to PKIs. Indeed, to send encrypted messages the user needs only to know the identity of the receiver. However, the use of a trusted Private Key Generator (PKG) is required to join the identity of the user (ID) and the key pair (sK, pk). The PKG possesses the master Key used to generate all private keys of the users in the network. The rogue of PKG destroy all privacy in the wireless network. Indeed, IBC is vulnerable to the key escrow attack. This problem limits the use of IBCs to closed organizations [11]. Other solutions focus on utilizing more key pairs, using threshold, and considering expired date for the master key. However, they have some drawbacks that make them unsuitable for Ad-Hoc networks such as too much overhead to the network, more computation /communication for nodes which are resource constrained devices [12].

3.3 SELF-CERTIFIED KEYS (SCK)

The first idea of Self-Certified Keys was introduced by D.Girault in Eurocrypt 1991[13] and later enhanced by Petersen, Horster In Proc. Communications and Multimedia Security 1997[14]. A self-certified system is based on the existence of a Trusted Third Party(TTP). The users generate their own key pair (sk, pk) and communicate their pk to the TTP which creates a witness w by combining the user's identity ID with his/her pk [13,14]. Several methods are proposed to generate this witness:

- The TTP's signature on some combination of pk and ID.
- The part of a signature.
- The result of inverting a trapdoor one-way function derived from pk and ID.

This scheme allows any user from the network to extract pk from (w,ID). Although, the SCK scheme uses lightweight certificates and not the traditional certificates. Where the witness w binds the ID to the correct pk of the user. However, the sk is generated before the pk. For this reason, the SCK doesn't enforce cryptographic work flows[15].The rogue of TTP can reveal the private keys of all the users.

3.4 CERTIFICATELESS PUBLIC KEY CRYPTOGRAPHY

The idea of Certificateless Cryptography is proposed to avoid:

- The need of CA for PKI.
- The need of Trusted management PKG of IBC or TTP of SKC.
- The problem of key escrow of IBC.
- The secret (private) key sk of a user is entirely generated by the PKG.
- The problem of the rogue (privacy of the system totally dependent upon the PKG).

However, the idea of certificateless is based on the fact that the secret is generated by the PKG and the user separately. This would eliminate the possibility of the PKG's rogue, additionally the scheme is kept certificateless to protect the user from a dishonest party. A Certificateless Public Key Cryptography (CL-PKC) scheme is similar to the IBC scheme in the aspect that it relies on the existence of a TTP which possesses a master key and the scheme also uses the identity of the user. Indeed, these ideas were formally developed by Al-Riyami and Paterson (2003)[16].There are three parties involved in a CL-PKC scheme:

- The trusted third party : Key Generation Center (KGC).
- The Sender : the party sending the message.
- The Receiver : the party receiving the sent message.

The KGC uses master private key (msk) and the receiver's ID to generate a partial secret key psk. The receiver combines psk with a secret value a to derive his/her full secret key sk. The sk is known only by the receiver and key escrow is avoided. Furthermore, the receiver authenticates his identity (ID) to the KGC who must then securely transmit the psk. The receiver computes his/her sk by combining the same secret a value with the public parameters published by the KGC and distributes it. The generation of pk and sk is independent of each other and just requires the use of the same secret value a. The sender can obtain the pk related to an identity and uses it to send encrypted messages to the receiver[17]. Certificateless is the most adapted solution for the Ad-Hoc UWB-IR network. The question is how to choose the public key cryptosystems for this solution?

4 PUBLIC KEY CRYPTOSYSTEMS FOR CERTIFICATELESS

We demonstrate that CL-PKC is the best solution for securing data and communications in the Ad-Hoc Wireless based UWB radio. Indeed, CL-PKC is a public key based algorithm and it is mainly used for confidentiality, key distribution, authentication, integrity and non repudiation. The implementation of public key algorithms in very constrained devices such UWB-IR requires faster cryptosystems like all wireless devices (mobile phones smart cards, PDA etc).

The choice of Public Key CryptoSystems (PKCSs) for CL-PKC is the stone corner of our work. The public key pk is known to all and used to encrypt information. Only the person who has the corresponding private key sk can decrypt the information. The concept of asymmetric key cryptography was introduced by Whitfield Diffie and Martin Hellman[18].

The performance of a public key cryptographic system is measured in processing time, computational overheads, key size, and bandwidth. In the field where computing power, storage, and bandwidth are limited; carrying out complex operations on large data becomes an impractical approach to provide strong security. This is most obvious in constrained devices such as UWB-IR, which have very limited resources.

4.1 COMMONLY USED PUBLIC KEY CRYPTOSYSTEMS

In this paper we study three public key cryptosystems:

- RSA is the first public key cryptosystems. The name RSA algorithm is the initials of the surname of developers Ron **R**ivest, Adi **S**hamir, and Leonard **A**dleman. They are three MIT researchers.
- ECC is **E**lliptic **C**urve **C**ryptography.It provides the same level of security, with smaller key sizes than RSA.
- NTRU Cryptosystems were developed by Joseph H. Silverman, Jeffrey Hoffstein, Jill Pipher and Daniel Lieman. The NTRU is known as NTRUEncrypt. In 2009, NTRU Cryptosystem has been approved for standardization by the Institute of Electrical and Electronics Engineers (IEEE).

4.1.1 RSA CRYPTOSYSTEM : The RSA public and private key pair can be generated by the following procedure:

- Algorithm
  1. Choose two large prime numbers p and q.
  2. Compute $n = p * q$.
  3. Compute $\varphi(n)$ so that $\varphi(n) = (p-1) * (q-1)$.
  4. Choose the public key e so that $gcd\ (\varphi(n), e) = 1$; $1 < e < \varphi(n)$.
  5. Select the private key d so that $d * emod\varphi(n) = 1$.
  6. Public key $(pk) = (n, e)$ and Private key $(sk) = (n, d)$.
- Encryption $C = M^e modn$.
- Decryption $M = C^d modn = (M)^{ed} modn$.

4.1.2 ELLIPTIC CURVE CRYPTOSYSTEM ECC stands for Elliptic Curve Cryptography. Let E an elliptic curve over a finite field F_p $(p \neq 2, 3)$. Then E is a curve which consists of points satisfying the equation $y^2 = x^3 + ax + b$ ($a, b \in F_p, 4a^3 + 27b^2 \neq 0$). At first we have to choose the base elliptic curve point G with order divisible by a large prime. This point can be agreed before hand and can be made publicly available. Assume user A wishes to send message M to B Elliptic Curve Encryption/Decryption algorithm can be explained by following procedure:

- Algorithm
  1. A chooses a random positive integer k, a private key sk_A.
  2. Generates the public key $pk_A = sk_A.G$ and has a public key pk_B of B.
- Encryption: Calculates the cipher text C_M. consisting of a pair of points $C_M = k.G, M + k.pk_B$ where G is the base point selected on the Elliptic Curve, $pk_B = sk_B.G$ is the public key of B with private key sk_B.
- Decryption: To decrypt the cipher text, B multiplies the 1^{st} point in the pair by B's secret and subtracts the result from the 2^{nd} point: $M + k.pk_B - sk_B(k.G) = M + k(sk_B.G)sk_B(k.G) = M$.

4.1.3 NTRU CRYPTOSYSTEM : The NTRU Encrypt [19] is based on arithmetic in a polynomial ring $R = Z(x)/((x^N - 1), q)$ set up by the parameter set (N, p, q) with the following properties:

- All elements of the ring are polynomials of degree at most $N - 1$, where N is a prime.
- Polynomial coefficients are reduced either $modp$ or $modq$, where p and q are relatively prime integers or polynomials.
- p is considerably smaller than q, which lies between $N/2$ and N.

– All polynomials are univariate over the variable x.

Multiplication in the ring R is sometimes referred to as "Star Multiplication" based on the use of an asterisk $\star$ as an operator symbol. It can be best described as the discrete convolution product of two vectors, where the coefficients of the polynomials form vectors are in the following way: $a(x) = a_0 + a_1x + a_2x^2 + ... + a_N{-}1x^{N-1} = (a_0, a_1, a_2, ..., a_{N-1})$. Then the coefficients c_k of $c(x) = a(x) \star b(x) mod q$, p are each computed as the summation of partial products $a_i b_j$ with $i + j \equiv k mod N$. The modulus for reduction of each coefficient c_k of the resulting polynomial is either q for Key Generation and Encryption, or p for Decryption, as briefly described below. A thorough description of these procedures along with an initial security analysis can be found in [20].

– Algorithm: Key Generation The following steps generate the private key $f(x)$:

1. Choose a random polynomial F(x) from the ring R. $F(x)$ should have small coefficients, i.e. either binary from the set $\{0, 1\}$ (if $p = 2$) or ternary from $\{-1, 1, 0\}$ (if $p = 3$ or $p = x + 2$ [20]).
2. Let $f(x) = 1 + pF(x)$ to decrease the decryption failure rate.
3. The public Key h(x) is derived from $f(x)$ in the following way:
   (a) As before, choose a random polynomial $g(x)$ from R.
   (b) Compute the inverse $f^{-1}(x)(mod q)$.
   (c) Compute the public key as $h(x) = g(x) \star f^{-1}(x)(mod q)$.

– Encryption

1. Encode the plaintext message into a polynomial $m(x)$ with coefficients from either {0, 1} or {-1, 0, 1}.
2. Choose a random polynomial $\emptyset(x)$ from R as above.
3. Compute the ciphertext polynomial $c(x) = p\emptyset(x) \star h(x) + m(x)(mod q)$.

– Decryption

1. Use the private key $f(x)$ to compute the message polynomial $m'(x) = c(x) \star f(x)(mod p)$.
2. Map the coefficients of the message polynomial to plaintext bits.

5 PERFORMANCES AND SECURITY ANALYSIS OF PKCS

The aim of the study is to analyze the performance and the security of various public key cryptosystems (RSA, ECC and NTRU). The object is to demonstrate the best chosen PKCS to be implemented within a certificaless scheme for Ad-Hoc UWB-IR networks. The implementations are done using Java as a programming language. We have optimized the implementations for ARM9-32-bit microcontrollers and have tried to keep the code portable to other platforms. In order to keep the memory requirements low, it would be possible to import the code to limited environments, and do not use large look-up tables.

This choice is not arbitrary, because, the microcontrollers are specially suitable for the wireless sensor network environment, due to their cost effectiveness (enough computational capabilities, memory for executing simple tasks, consuming less energy...). Table 2 show the most microcontrollers used in WSN market[21] and their capabilities (such as frequency, word size, RAM memory, Instruction memory, and so on).

Table 2. Microcontrollers used in the sensor network market.

Model	Frequency	Word size	RAM memory	Inst. memory	Power(awake)	Power(slept)
PIC18F6720	20Mhz	8bit	4kB	128kB	2.2mA	1μA
MSP430F14x	4Mhz	16bit	2kB	60kB	1.5mA	1.6μA
MSP430F16x	8Mhz	16bit	10kB	48kB	2mA	1.1μA
ATmega128L	8Mhz	8bit	4kB	128kB	8mA	15μA
PXA271	13(416)Mhz	32bit	256kB	32MB	31-44mA	390μA
ARM920T	180Mhz	32bit	512kB	4MB	40-100mA	40μA

The performance of public key cryptosystems is evaluated and compared on the:

- Mathematical complexity of problem.
- Security level.
- Key size.
- Speed of encryption and decryption operations.

5.1 PKCSs AND THEIR MATHEMATICAL PROBLEMS

Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. In PKC, sk and pk keys are mathematically related complex function f. It is very hard to get private key from the public key. In order to recover the sk to decrypt information a mathematical problem P related to complex function f must be solved. The security of PKCS depends on the difficulty to solve P. Table 3 shows the different mathematical complexity problem for RSA, ECC and NTRU.

Table 3. Public Key Cryptosystems and their Mathematical Problems.

Cryptosystem	Mathematical Problem	Running times
RSA	Integer factorization	Sub exponential
ECC	Elliptic curve discrete logarithm	exponential
NTRU	Short Vector problem (geometrical problems)	exponential

The PKCSs RSA and ECC are based on the complexity of number theoretic problems and their security is highly reliable to the distribution of prime numbers or based on the discrete logarithm problem on finite fields. NTRU cryptosystem is based on geometrical problems.

5.2 PKCSs AND KEY SIZE

In Symmetric key cryptography, the minimum length of a key that is considered securely strong is 80 bits. However, the key length of 128 bits is recommended for more security. The private (sk) and public (pk) keys in RSA and ECC can be chosen from almost equal lengths. The Table 4 in [22] shows the public key sizes of RSA, ECC and NTRU algorithms along with Symmetric key sizes.

Table 4. Key sizes of PKCS vs SKC in bits.

Security Level (bits)	n	RSA key sizes (bits)	ECC Key sizes (bits)	NTRU Key sizes (bits)
80	251	1024	163	2008
112	347	2048	224	3033
128	397	3072	256	3501
192	587	7680	384	5193
256	787	15360	512	7690

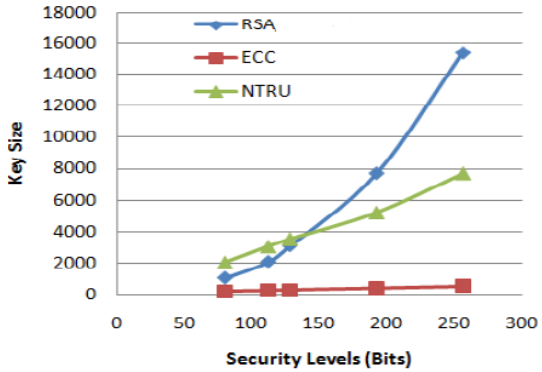

Fig. 3. Security levels vs Key size of various PKCS.

From the Table 4, and Fig 3 we conclude that:

- If the symmetric key size increases, the key sizes for RSA increases faster than the ECC.
- ECC systems can offer more security per bit increase in key sizes compared to RSA and NTRU.
- ECC has the smallest key size which makes it the best in use of bandwidth and the NTRU's bandwidth usage becomes more efficient with respect to RSA as the security level increases.

5.3 PERFORMANCE COMPARISON OF PKCs

5.3.1 COMPARING ENCRYPTION AND DECRYPTION IN RSA AND NTRU The performance comparison of RSA and NTRU public key cryptosystems is shown in Table 5, Fig 4 for encryption and Fig 5 for decryption. We can conclude that:

- The RSA public and private keys have the same size.
- The private keys sk of NTRU are shorter than their pk.
- NTRU encrypts and decrypts more messages than RSA with the same key sizes.

Table 5. Comparing Encryption and Decryption in RSA and NTRU.

PKC	Key size (bits)	Encrypt Block/ms	Decrypt (Block/ms)
RSA 1024	1024	1232	29
RSA 2048	2048	413	4
RSA 4096	4096	-	-
NTRU 167	1169	7038	4201
NTRU 263	1481	4789	2134
NTRU 503	4024	1945	812

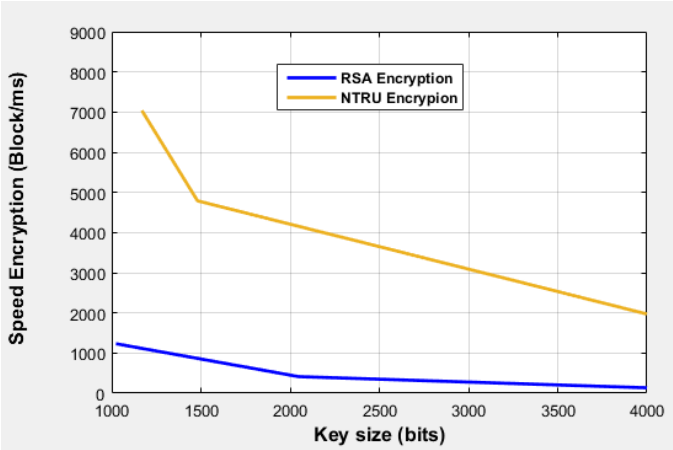

Fig. 4. Comparing Encryption in RSA and NTRU.

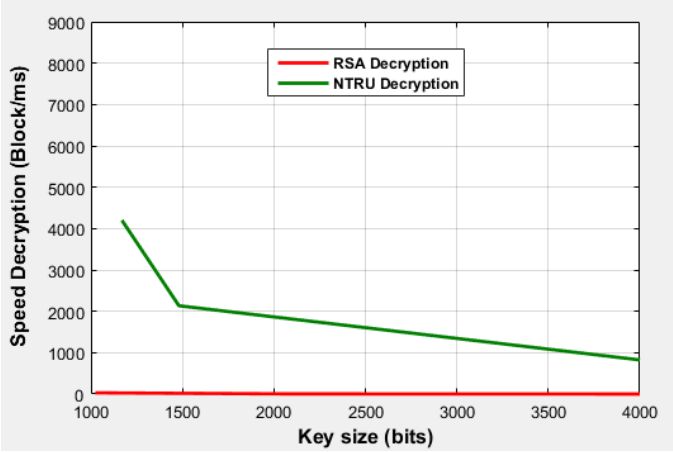

Fig. 5. Comparing Decryption in RSA and NTRU.

5.3.2 COMPARING ENCRYPTION AND DECRYPTION IN ECC AND NTRU The performance comparison of ECC and NTRU public key cryptosystems is shown in Table 6, Fig 6 for encryption and Fig 7 for Decryption, we can conclude that:

- The NTRU is faster than ECC with all levels of security.
- The performance of NTRU is superior than ECC in both encryption and decryption.

Table 6. Comparing Encryption and Decryption in ECC and NTRU.

PKC	Security (bits)	Encrypt ms	Decrypt (ms)
ECC 192	80	25.16	14.37
ECC 256	128	43.86	24.21
ECC 384	192	125.32	60.12
ECC 512	256	297.21	140.37
NTRU 251	80	1.05	5.75
NTRU 397	128	2.64	13.62
NTRU 587	192	5.99	29.69
NTRU 787	256	9.93	32.01

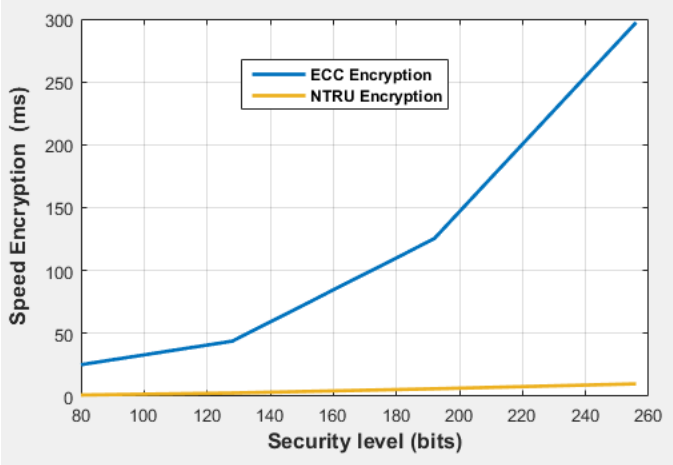

Fig. 6. Comparing Encryption in ECC and NTRU.

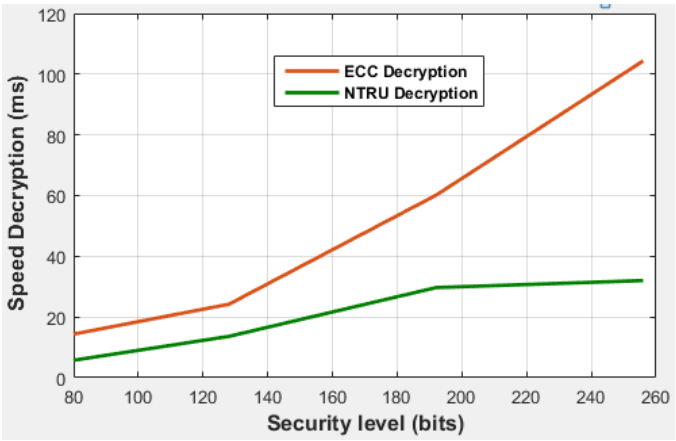

Fig. 7. Comparing Decryption in ECC and NTRU.

The following is a global table of comparison among RSA, ECC and NTRU. Let $|E|$ denote public key size. The ratio of $M : |E|$ suggests better economical value per public key bit being used. At the same time the ratio between the message and the ciphertext is $\approx 1 : 1$ which implies that the message expansion due to encryption is negligible [23].

6 CONCLUSION

In this paper, we proved that the security suites of IEEE 802.15.4 are not adapted to Ad-Hoc UWB-IR network. Indeed, they have multiple problems and vulnerabilities, due to the use of Symmetric Key Cryptosystem (AES) and specially the CCM mode. Unfortunately, the 802.15.4 standard, and all the chips that implement it, is not exempt of security flaws [24].

One of the security suites, AES-CTR, is deeply flawed, since it does not properly support replay detection and it is possible to launch denial of service (DoS) attacks sending a single forged packet. Also, the acknowledgement packets are not protected by a MAC, thus it is possible to forge them. Other minor problems include deleting the ACL when entering a low power mode.

Furthermore, we demonstrated that the best solution to secure data and communications in Ad-Hoc UWB-IR networks is certificateless based Public Key Cryptosystems. In fact, many PKCSs have been developed. Yet, in this work, we implemented, evaluated and compared the performance of three PKCSs: RSA, ECC and NTRU. From the obtained results, it was concluded that ECC has the best key size overall. NTRU was better than RSA if the security level starts from 192 bits to 256 bits. It is clear that the NTRU is very fast and achieves the highest security level compared to other PKCSs such ECC and RSA.

NTRU cryptosystem is slowly gaining more popularity thanks to many advantages like small key size, easy key generation, high speed encryption and decryption, and very low computation power. In addition, Operation speed is very fast, more efficient, consuming less space and it is more suitable for mobile devices. Furthermore, unlike RSA and ECC, NTRU is resistant to cryptographic attacks based upon quantum computing technics. As a result, NTRU was standardized as IEEE 1363.1-2008 and X9.98-2010. Consequently, it is the smallest public key cryptosystem available on market, and represents the first candidate to be adopted in UWB-IR infrastructures.

As a future work, we will focus on the analyse of NTRU cryptosystem efficiency in comparison with other alternative algorithms based on a different mathematical problem called the closest

lattice vector problem. Indeed, NTRU will be compared to other cryptosystems resistant to quantum computing attacks like McEliece,etc.

References

1. S. Wood and R. Aiello, "Essentials of UWB", Cambridge University Press, June 2008.
2. IEEE. 802.15.4a : Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Personal Area Networks (LR-WPANs)-Amendment 1 : "Add Alternate PHYs", August 2007.
3. IEEE Standard for Local and Metropolitan Area Networks-Part 15.6 : "Wireless Body Area Networks", February 2012.
4. M. Dinesh and E. Redddy, "Ultimate Video Spreading With Qos over Wireless Network Using Selective Repeat Algorithm", International Journal of Computer Science Engineering, vol. 2, no. 4, July 2013 .
5. Mihir Bellare, Phillip Rogaway and David Wagner "The EAX Mode of Operation". Computer Science, vol 3017. Springer, Berlin, Heidelberg FSE , January 2004, pp 389-407
6. P. Rogaway and D. Wagner, "A Critique of CCM", Eprint cryptology archive, February 2003.
7. C. Adams, S. Lloyd, "Understanding PKI: concepts, standards, and deployment considerations", Addison-Wesley Longman Publishing Co., Inc, November (2002)
8. P. Gutmann. PKI: its not dead, just resting. Computer 35(8), August 2002, pp.4149.
9. J. Dankers, T. Garefalakis, R. Schafflhofer, T. Wright, "Public key infrastructure in mobile systems". Electronics and Communication engineering journal 14(5), Octobre 2002, pp.180-190
10. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes". In CRYPTO, volume 196 of Lecture Notes in Computer Science, Sprinnger-Verlag Berlln Heldelberg August 1985, pp.47-53.
11. M.Bechler , H-J.Hof , D.Kraft , F.Pahlke, L.Wolf, "A cluster-based security architecture for ad hoc networks". Proceedings of IEEE INFOCOM (2004).
12. S.Zhao, Aggarwal, R.Frost, A.Aggarwal, X.Bai, "A Survey of Applications of Identity-Based Cryptography in Mobile Ad-Hoc Networks".Communications Surveys Tutorials, IEEE, January 2012, pp.1 - 21
13. M. Girault. "Self-Certified Public Keys". In EUROCRYPT 91, volume 547 of Lecture Notes in Computer Science, 490-497. Springer. Avril 1991, pp.490-497.
14. H. Petersen, P. Horster and D. P. Horster. "Selfcertified keys - Concepts and Applications". In In Proc Communications and Multimedia Security97, August 1997, pp.102-116.
15. Saeednia, Shahrokh, "A Note on Girault's Self-certified Model". Information Processing Letters 86(6), June 2003, pp.323-327.
16. Al-Riyami S.S, Paterson K.G, "Certificateless Public Key Cryptography". In ASIACRYPT, Lecture Notes in Computer Science, vol 2894, April 2003, pp.452-473.
17. K. Sharad, "Certificateless Encryption Scheme Using Biometric Identity". Master's Thesis, March 2012, pp. 24-26
18. W. Diffie and M. E. Hellman, "New directions in cryptography". IEEE Transactions on Information Theory, vol. IT-22, no.6, 1976 , pp.644-654.
19. J. Hoffstein, J. Pipher, J. H. Silverman, "NTRU: A Ring-Based Public Key Cryptosystem". ANTS III-Algorithmic Number Theory, 1998 pp 267-288.
20. G.Gaubatz, J.Kaps, B.Sunar, "Public Key Cryptography in Sensor Networks," In 1st European Workshop on Security in Ad-Hoc and Sensor Networks ESAS 2004,pp.2-18.
21. R.Roman, C.Alcaraz, J.Lopez "A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes", Mobile Network Application, October 2007, pp.231244.
22. P. Karu and J. Loikkanen "Practical Comparison of Fast Public-key Cryptosystems", Proceedings of the Helsinki University of Technology Seminar on Network Security fall 2000. Available at http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers.html.
23. J. Hoffstein, D.Lieman, J. Pipher and J. H. Silverman, "NTRU : A Public Key Cryptosystem", NTRU Cryptosystems Inc. (2008, April27)[Online].Available:http://http://grouper.ieee.org/groups/1363/lattPK/submissions/
24. N.Sastry , D.Wagner, "Security considerations for IEEE 802.15.4 networks", Proceedings of the 2004 ACM Workshop on Wireless Security, October 2004, pp.32-42.

AUTHORS

Jamel Miri was born in Sidi Bouzid, Tunisia. He Received the Dipl.- Engi. degree in Telecommunication engineering in 2001 from Sup'Com . Currently he is a Ph.D. student at the School of Engineering of Tunis (ENIT). The research works are realized Research Laboratory Innov'COM / Sup'Com. His principal research interests lie in the fields of Wireless Ad Hoc and Sensor Networks, Embedded and RFID Systems, focusing on identification, modeling and mitigation of network security vulnerabilities, and analysis of network performance such as UWB, WSNs and Ad'Hoc technology.

Bechir Nsiri was born in Boussalem, Tunisia. From September 2011 until now, he teaches in Higher Institute of Applied Science and Technology Mateur, Tunisia. He received his master degree and Ph.D. in telecommunication specialty from the National School of Engineering in Tunis (ENIT) in Tunisia in 2011. The research works are realized in Department Sys'COM laboratory in ENIT. His principal research interests lie in the fields of Wireless and Radio Mobile Telecommunications engineering such as MIMO OFDM technology and scheduling in radio network planning in LTE system.

Pr. Ridha Bouallegue was born in Tunis, Tunisia. He received the M.S degree in Telecommunications in 1990, the Ph.D. degree in Telecommunications in 1994, and the Habilitation a Diriger des Recherches (HDR) degree in Telecommunications in 2003, all from the National Engineer School of Tunis (ENIT), Tunisia. He is currently Professor in the National Engineer School of Tunis (ENIT) and Director of Research Laboratory Innov'COM / Sup'Com. His current research interests include mobile and satellite communications, Access technique, intelligent signal processing, CDMA, MIMO, OFDM and UWB system.