Security Considerations in the Design of IEEE 802.15.4 Transceiver: A Review

K. Vivek Raj, P. Dinesha, and S. I. Arpitha Shankar

Abstract As internet of things (IoT) is extending internet connectivity beyond standard devices; the secure data transmission between IoT devices becomes more challenging. However, most of the traditional upper layer security schemes are computationally complex and increase the latency. Moreover, the security provided at upper layer is software implemented, and its strength depends on complexity of the encryption algorithm. This is a bottleneck situation for low-power IoT applications. As IoT uses many remote sensors which operate on battery power; IEEE 802.15.4 standard is gaining attention because of low-power consumption. An 802.15.4 protocol defines medium access control (MAC) and physical layer (PHY) specifications, and is designed to allow low-power, low-cost short range communication. Basic encryption and authentication in 802.15.4 are provided by link layer. Hence, considerable attention is required to study 802.15.4 specifications that can be used to provide alternative methods of security. So this paper is motivated to study the importance of 802.15.4 PHY. Firstly, we review the different physical layer security (PLS) schemes. Secondly, we present the concept of physical layer encryption (PLE) and further we analyze and compare the implementation of different PLE schemes in wireless standards. Later, we will try to give insights of 802.15.4 security standards and bring out the drawbacks of AES based link-layer security. Finally, we present the design and implementation aspects of 802.15.4 transceiver hardware architecture by considering performance and security.

K. Vivek Raj (✉)
Department of Electronics and Telecommunication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka 560078, India

P. Dinesha
Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bengaluru, Karnataka 560078, India

S. I. Arpitha Shankar
Department of Electronics and Telecommunication, GSSS Institute of Engineering and Technology for Women, Mysore, Karnataka 570016, India

K. Khanna et al. (eds.), *Cyber Security and Digital Forensics*,
Lecture Notes on Data Engineering and Communications Technologies 73,
https://doi.org/10.1007/978-981-16-3961-6_19

Keywords IEEE 802.15.4 · Computational security · Physical layer security · Internet of things · Physical layer encryption · Transceiver · Medium access control · Authentication

1 Introduction

In recent years, wireless communication is advancing with respect to its infrastructure and services with an aim of meeting rapidly growing demands. Wireless networks are being used for many applications. The International telecommunications Union [ITU] facts and figures in 2020 indicates that in 104 countries, half of the population is now using internet of which 70% are the youth [1]. Extending internet connectivity beyond conventional mobile phones and computers leads to evolution of new technology called internet of things. Currently, IoT is gaining more importance and it is playing important role in most of the fields such as health monitoring, automation, e-cities and so forth. However, secure data communication on IoT technology is more challenging scenario due to many constraints like power consumption, less storage memory and availability of processing power etc. [2]. Due to this, existing cryptographic techniques that are provided at the upper layer are not suitable because of their power consumption and the complexity in implementation. The IEEE 802.15.4 is designed to provide very low-cost communication between nearby devices in wireless personal area network (WPAN). Low-power wireless connectivity of 802.15.4 attracts wide variety of applications especially which operates on battery power. Since IoT employs different sensors which rely on battery, the use of 802.15.4 becomes most common in IoT applications. The structure of 802.15.4 protocol stack is shown in Fig. 1. It defines PHY and MAC layer specifications. PHY sits at the bottom of the protocol stack and transmit data packets. Direct sequence spread spectrum (DSSS) allows two physical layer configurations one works at 868/915 MHz and provides data rate of 20–40 kbps, second operates at 2.4 GHz with 250 kbps.

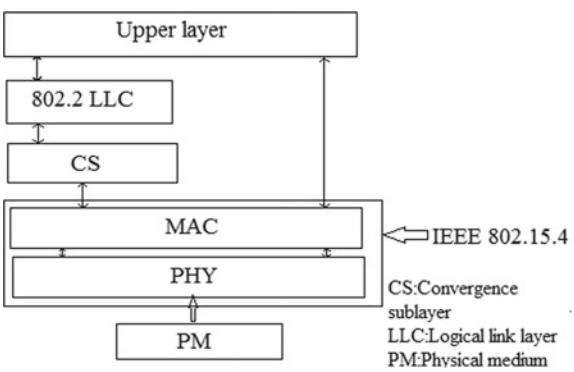

Fig. 1 IEEE 802.15.4 protocol stack

However, further revision in the standard allows the use of different modulation schemes. MAC layer performs different functions including channel access, frame delivery, synchronization, flow control, error control and it also provides interface between PHY and application layer. 802.15.4 is gaining importance as demand for IoT is increasing and security becomes a major concern. The PHY security technology combines the communication PHY and the security layer; hence, it is important to study the fundamental ability of the 802.15.4 PHY to offer secure wireless communication. In recent times, PLS and PLE are in much attention. Both of these approaches exploit the properties and characteristics of the PHY to provide the security. PLS provide information-theoretic security that is impossible to break by computing power. On the other hand, PLE is based on computational complexity and uses distribution of secret key. Unlike conventional cryptography, encryption in PLE is performed during the modulation process. That is in PLE, the security is provided at signal level. Further, PLE takes advantage of effect of the channel and noise. Hence, it increases the strength of underlying algorithm as it makes difficult in receiving the encrypted text itself. However, there is a clear difference between PLS and PLE.

Some of the characteristics which differentiates PLE from PLS are listed below.

1. Unlike PLS, PLE can guarantee secrecy, even if the channel capacity of eavesdropper is better than legitimate channel.
2. PLE has low-computational complexity, provides low latency with minimum power consumption and provides long lifetime hence it is best suited for IoT applications.
3. PLE provides security at signal level. It uses Boolean algebra therefore it gives much more functions to design and construct secure encryption algorithm.
4. In contrast to PLS which only focuses on eavesdropping attack, PLE uses randomness function which can be used to prevent linear and plaintext attacks.

Since our focus is on 802.15.4 protocol, further we concentrate more on the security aspects in the design of 802.15.4 transceiver. Table 1 provides the comparison between PLS, traditional cryptography and PLE and shows that PLE is different than PLS and conventional cryptography.

Table 1 Comparison of PLS, cryptography and PLE

Type	Distribution of key	Type of channel	Type of security	Operate domain
PLS	NO	Noise channel	Prefect secrecy, depends on channel	Complex vector
Traditional cryptography	YES	Perfect channel	Computationally secure	Bit level
PLE	YES	Noise channel	Computationally secure, uses characteristics of channel	Complex vector and signal level

Most of the available upper layer encryption schemes are computationally complex and increases the latency and its strength completely depends on complexity of the encryption algorithm. However, PLS schemes can provide security at the physical layer, but its implementation faces serious problems. PLS cannot guarantee secrecy if the legitimate node has weak channel capacity than eavesdropper or if no channel information of eavesdropper is available. Power consumption is large in PLS as it uses more number of relays or antenna systems. From Table 1, we have seen that PLE schemes have many advantages over other two. It is more practical to use PLE in the design and construction of secure 802.15.4 transceiver.

Rest of the paper is organized as follows. Section 2 presents overview of PLS. In Sect. 3, PLE and its implementation in different wireless systems are discussed. In Sect. 4, different security suits of 802.15.4 protocol is compared. Section 5 gives hardware implementation of 802.15.4 transceiver, and finally Sect. 6 provides conclusion.

2 Physical Layer Security

PLS provides unbreakable, quantifiable and provable secrecy from the information-theoretical point of view. PLS takes an advantage of wireless channel characteristics for improving the reliability and security. In this subsection, we discuss about different PLS schemes such as information-theoretic security, artificial noise generated secrecy, secure beam forming and diversity-assisted security.

2.1 Information-Theoretic Security

It is a cryptosystem whose secrecy is derived mainly from an information theory. Basic principle of security schemes was developed by focusing on the properties of mathematical structures. Claude Shannon proposed a security principle as a mathematical transformation of valid plaintext into another set of reliable cryptograms. Here, each transformation is done by encrypting the message, using secret keys. This cryptosystem is unbreakable even though attacker has unlimited computing power. One-time pad is an example of such a cryptosystem. This secrecy system was designed for protection against eavesdropping attacks. Since Shannon model uses distribution of key, key management becomes difficult for wireless networks with no fixed infrastructure [3]. Wyner improved Shannon's model without secret keys and analyzed the performance of a discrete memory less wiretap channel and achieved perfect secrecy, provided if the capacity of a channel of the link spanning from an sender to receiver must be greater than the wiretap link between the sender and the adversary [4] and he proved that secure communications without keys can be realized with channel quality between intended nodes which is

better than the adversary link [5]. However, the use of information theoretic security is not practical because of difficulty in key generation and distribution. Further, secrecy capacity of wireless networks is extremely attenuated because of time varying fading effect. Usually, fading degrades the signal received at the legitimate receiver, which decreases the capacity of the valid channel, and reduces the secrecy capacity.

2.2 Artificial Noise Aided Security

Artificial noise (AN) has been exploited to enhance the security performance by degrading the capacity of the adversary, termed as artificial noise aided security. Basic principle of the noise injection method is to simultaneously transmit the message and the generated noise in order to reduce the performance of the adversary [5]. In AN pre-coding, the source node splits the transmission power between data transmission to legitimate receiver and the noise transmission to the eavesdropper. The transmitter is designed in such a way that only adversary channel is selectively degraded. With this model, certain minimum rate of security can be achieved. However, secrecy cannot be guaranteed, if the eavesdropper channel is better than the recipient [6, 7]. AN pre-coding gives provable security at the PHY, but it comes with an extra cost of additional energy requirements. In this approach, a fraction of transmission power of message signal is taken to produce the AN. It depletes transmission power that can be utilized to improve the capacity of a channel and receiver signal-to-noise ratio (SNR). Hence, it is a compromise between the transmission power and secrecy rate [8].

2.3 Security Oriented Beam Forming

This technique is extensively used in the relay systems; it helps in improving the SNR at the receiver end. It has an ability to control the direction of transmission, it only focuses energy in specified direction and suppresses energy in other direction. This in turn increases the energy efficiency of a system. Consider a model which consists of A, B and C, where A is the transmitter, B is the receiver, and C is the eavesdropper. When A sends information to B in the presence of C, and if C is within the coverage area then C can easily intercept the message sent by A to B. Thus, this can be avoided by using beam forming. Beam forming creates a beam only in the direction of B to maximize the SNR ratio and suppresses the transmission or reception in the direction of the C. One of the main features of beam forming techniques is spatial filtering. The spatial filtering helps in distinguishing the secure and insecure locations for the transmission of information. Beam forming helps in utilizing the wireless medium in order to provide better service with respect to error performance and bit rate at the PHY [7].

However, beam forming faces issues such as fraction of the power being spread through minor side lobes, even though signal is directed toward legitimate node and the transmitted power is concentrated in the beam of main lobe. It creates a loophole for an eavesdropper who is in the coverage area to decode the transmitted information. It is also observed that beam forming only concentrates on improving the quality of the main channel and it neglects the possibility of having favorable channel by eavesdropper. Further, beam forming is computationally expensive and difficult to implement [8].

2.4 Security Diversity Techniques

The diversity technique is usually employed to enhance the transmission reliability which in turn improves the wireless security and also to reduce the duration of fading, experienced at the receiver. The PLS can be improved by various diversity methods which includes MIMO, multiuser and cooperative diversity [9].

MIMO Diversity: In this technique, multiple antennas are used for transmitting and receiving the signal. When the information bearing signal is sent through the channel, it will be transmitted through more than one antenna and, while receiving, it will be received through multiple antennas. Basically, MIMO is considered as an effective method of overcoming wireless fading and thus increases the channel capacity. However, there is possibility that eavesdropper could also utilize the structure of MIMO to improve the capacity of wiretap channel.

Multiuser Diversity: This is obtained by the user scheduling it either at the transmitter or at the receiver. Basically, it uses OFDMA and TDMA. So at any point of time, transmitter will select the best user among different receivers based on the quality of their channel and throughput. Disadvantage of this method is that if the user is far away from the base station and experiences deep fading and worst propagation loss, then the user will not get a chance to access channel. Hence, user fairness needs to be maintained and should provide guarantee that each user will get opportunity to use the channel [10].

Co-operative Diversity: Cooperative diversity is one of the important beam forming techniques against eavesdropping. It is a multiple antenna technique which is employed to improve the legitimate channel capacities for a given set of bandwidth [9]. Cooperative network includes source (s), X relays (r), destination (D) and an eavesdropper (E). X relays (r) is used to help the message transmission between source and destination. The source first transmits the message to X relays that then relay (r) sends the received signal to the destination.

2.5 Physical Layer Secret Key Generation

Secret key is extracted by exploring the physical layer characteristics such as channel randomness, independent channel variation over space, channel reciprocity. The randomness is extracted either from amplitude or phase of wireless fading. Key is generated by alternatively sending probe signal and estimating the channel state information (CSIs). Intended nodes can convert their CSI into the same bit strings. The bit discrepancies are corrected using privacy amplification techniques and key reconciliation [11]. Basically, two methods are used to generate key streams, one way is by using received signal strength (RSS) where power of received signal is used and in the other scheme phase of the received signal is used to extract the common randomness. Even though this can provide an alternative approach to the conventional key generation algorithms there are certain limitations which requires an attention. RSS provides a low-key bit generation rate and it faces scalability issues however signal phase based scheme gives good performance the implementation is difficult since it requires analog-to-digital converter which increases hardware complexity [11].

Even after researchers have proposed significant number of mathematical models, algorithms, and solutions, PLS faces challenges in its implementation. Most of the problems which are faced by PLS completely depend on the channel. PLS, cannot guarantee security if the channel capacity of eavesdropper is better than legitimate channel or unavailable eavesdropper's CSI. Increased power requirement in PLS due to the use of MIMO and relay systems [12] is another issue. In addition to this, all the existing work related to PLS is only concentrated on improving the security against eavesdropping attack by completely neglecting the various wireless PHY attacks. Hence, it is important to search alternative techniques to improve security at the PHY.

3 Physical Layer Encryption

PLE is yet another method of providing security at the PHY. Unlike PLS, PLE rely on computational complexity and uses distribution of secret key. PLE has no strict requirement on the channel conditions and the number of antennas. Compared to upper layer security schemes PLE resists the influence of noise and the effect of the channel in order to give reliability along with security. PLE provides security at the signal level and makes use of channel error to enhance the secrecy level. PLE schemes are more modulation intended; uses joint design of encryption and modulation, and it varies along with wireless technology. Based on processing of plain text PLE can be categorized into two types: Stream and Block PLE.

Stream PLE: It uses an encryption unit which encrypts binary message sequence using pseudo-random cipher key streams. Key streams are generated by using pseudo-random complex sequence generation function. The encrypted symbol is a

function of message binary sequence and complex sequence. And the complex sequence is calculated based on the initial key. In stream PLE, each plain text symbol is encrypted with the corresponding key symbol. Receiver jointly performs decryption and demodulation to get plaint text back. Security in stream PLE depends on encryption function and the complex sequence. This scheme provides low-propagation error and latency. Disadvantage is low diffusion and lacks symbol overlap. Hence, stream PLE is mostly used in simple and high-speed applications.

Block PLE: This scheme encrypts a fixed size plaintext symbols as one block. Block PLE uses mapping functions which maps fixed block of an input sequence to complex vector based on corresponding key. Different types of mapping functions can used to design PLE and they can be random. In block, PLE encrypted output depends on block of binary sequence, mapping function and a key. Designing a suitable mapping function plays key role. Advantages of block PLE are; it provides high diffusion and is immune to tampering, it suffers with error propagation and slow encryption process.

In recent years, many researchers had proposed PLE implementation techniques in various communication systems like OFDM, MIMO and 802.15.4 so on. In this subsection, we try to present PLE schemes used in different wireless standards. As 5G is in focus, MIMO technology is evolving significantly and there is a need for security. New PLE method is proposed to improve the security in MIMO with spatial modulation [13]. Adding spatial modulation to MIMO provides high energy and spectral efficiency. This paper presents a chaotic-antenna-index-3D modulation and rotated constellation points PLE which effectively makes use of spatial modulation as well as chaotic theory. Key generation algorithm is designed based on chaotic theory. Security can be achieved by protecting the spatial constellation diagram, for this the chaotic sequence generated antenna index is used. The simulation results clearly show that even with infinite MIMO system, eavesdropper cannot recover plaintext. In [14], PLE implemented at the PHY using OFDM is discussed. The encryption method reserves a part of OFDM subcarriers which transmits dummy data used to hide information at subcarrier level and provides randomness. This makes information about subcarriers unclear. Obfuscation of subcarrier makes the transmission secure. Along with obfuscation it also uses re-sequencing of training symbols. The reserved subcarriers used for re-sequencing provides protection to entire packet in physical layer without affecting synchronization and channel estimation between intended user meanwhile it prevents the eavesdropper from doing all these operations. This scheme is implemented on 802.11 OFDM and compared the results with key rate, complexity and search space. Calculated results show that entire data search space is (48!)38 and a search space for entire packet is 2.47×10^{173} with this eavesdropper will take 3.74×10^{121} years to break. Key streams are generated using stream ciphers. Key rate can be adjusted by varying 's' OFDM symbol and 'k' reserved subcarrier. With increase in s and k value increases the search space which in turn improves security.

Further Li et al. [15] presented both stream and block PLE for 802.11 OFDM in their work. Two PLE framework designs are developed which can provide security

against known plaintext and chosen-plaintext attacks (CPA). In design framework, reliability and security are considered together. Stream PLE unit have of two parts; pseudo-random complex number generator (PRCNG) which is used to generate pseudo-random complex binary sequences (PRCBS). Both the legitimate user generates same PRCBS using a key. Next part is the design of encryption function, which performs mapping of plaintext symbols into constellation points (complex signal). The mapping is done according to PRCBS. Constellation distance and confusion are taken into account, while designing the mapping function. 3D constellation scheme maps 2 bit message to 3D constellation point and these points are distributed over spherical surface. After mapping, 3D rotation is used to disturb the constellation. This disturbance creates confusion which helps in improving the security. In block, PLE key generation algorithm produces three sub keys K1, K2, K3 which are used at three different stages. Three stages of PLE are bit change stage, modulation stage and block change stage. Bit change disturbs and creates confusion among the binary sequence using first sub key K1. Modulation uses K2 to map confused sequence to complex vector. Block change stage is a function used to make symbols confuse and interlace so that it will be difficult for eavesdropper to get plaintext. At this stage, K3 maps 2 complex vector spaces. Table 2 shows the comparison between different PLE methods used for 802.11 OFDM. Search and key space, CPA security, throughput, BER performance and design complexity are considered for performance analysis. All three PLE schemes give similar results when it comes to bit penalty, key and search space. The subcarriers obfuscate scheme uses a part of transmission power to send dummy bits so its throughput decreases. And since it uses two stream ciphers CPA security relies on stream cipher which it uses. Block PLE and stream PLE provide better throughput performance however CPA security in stream PLE depends on PRCNG which is used to produce PRCBS using keys. All three are linearly complex and these PLE can be software or hardware implemented.

Huo et al. [16] presented a new generalized phase encryption scheme which can be applied to any of the wireless communication standard independent of modulation scheme. XOR encryption uses bitwise XOR between data bits and the corresponding key bit to give encrypted output. Unlike XOR encryption, phase encryption is performed on modulated sequences. Basically, phase encryption

Table 2 Comparison between different PLE methods

Type	Bit penalty	Throughput decrease	Search space	Key space	CPA security	Complexity
Subcarrier obfuscate [15]	NO	Depends on reserved subcarrier	High	High	Relies on stream cipher	Linear
Block PLE [16]	NO	NO	High	High	Good	Linear
Block PLE [16]	NO	NO	High	High	Relies on PRCNG	Linear

neither depends on system or on specific modulation scheme. Security functions provided at upper layers makes added data and the headers of succeeding layers unprotected and it is vulnerable to traffic analysis attacks. Authors proposed PHY structure using phase encryption. Here, two bits are used to encrypt one modulated symbol. First bit represents real part and another bit is used for imaginary part. Modulated symbol consists of $\log_2 M$ bit information where M is the size of constellation. It shows phase encryption is not one to one mapping of plaintext and secret key. N bit symbols are encrypted by a key stream of 2-bits. Further, 1 bit key stream is enough to encrypt modulated symbol in case if it consists of only real component. Once phase encryption is done the modulated discrete symbols and encrypted sequence are given to digital to analog converter. Obtained analog part is up converted into carrier frequency later it is transmitted over a channel. In phase encryption, the cipher text is a complex number and relation between plaintext and cipher text depends on channel coding, source coding and type of modulation is used. Since the encryption is done at physical layer just before the transmission can prevent the traffic analysis attack. Comparison results of both XOR and phase encryption are given in Table 3. From the result, it is shown that phase encryption gives higher encryption efficiency and can be used as a substitution for XOR encryption.

Generalized phase encryption is extended to design the PHY of 802.15.4. [17]. Since PLE is modulation specific considerable attention is required for each wireless standard. Even though different PLE methods are already available, most of them are for OFDM systems [14, 15]. And some schemes are implemented by rotating the constellation points [13]. Paper [16] presented the phase encryption to mitigate traffic analysis. All the above-mentioned methods are concentrated in providing security to 802.11 OFDM systems. But all these schemes are not suitable when it comes to the security of IEEE 802.15.4 because of different operating conditions of its devices. In general, security services like confidentiality, integrity of 802.15.4 is provided via MAC. These security primitives increase the computational energy which cannot be neglected [18]. Hence in [17] authors proposed an efficient phase encryption scheme for PHY of 802.15.4 and analyzed it against energy depletion and traffic analysis attack. During an encryption, phase of the modulated symbol changes with respect to key. The size of key is depends on the underlying modulation method. Each one of the modulated symbols consists of 2

Table 3 Comparison between XOR and phase encryption

Type	Encryption	Encryption efficiency	Cipher text	Mapping
XOR encrypted	Before modulation	Low	Bit level	Bit to bit
Phase encrypted	After modulation	High	Complex number	2 bits used to encrypt 1 modulated symbol

message bits and it is the form (I, Q). Values of I and Q are from the set of {1, −1}. Hence I and Q of key stream also take its values from the set of {1, −1} .cipher text is produced by multiplying the corresponding components of the modulated symbol and key streams.

4 IEEE 802.15.4 Security Suits

In recent years, 802.15.4 standard is becomes popular and an association with an IoT makes its applications even broader.802.15.4 protocol defines low-power, low-complexity and low-data rate communication in WPAN. An 802.15.4 application includes smart cities, home and industrial automation, health monitoring and military surveillance so on. All these applications need secure transmission of information. Particularly, when it comes to a health and military applications, security is the utmost concern. Hence, it is very important to study the security aspects of IEEE 802.15.4. This section presents the IEEE 802.15.4 security specification. Security requirements of 802.15.4 are frame integrity, confidentiality and access control. Integrity resists the modification of frames; Confidentiality guarantees that only intended nodes can transmit the secret message. Access control protects the frames against unauthorized users. Sastry et al. [19] extensively discussed about security provisions. In 802.15.4 link-layer security provides confidentially, integrity and access control. The 802.15.4 uses two types of packets; data packet which uses a flag to indicate type of packet, security enable and addressing modes. At last 2 bytes of CRC are used for error correction. Acknowledgment packet is used to send acknowledgment by the recipients. In 802.15.4, MAC layer controls the security. In case of security requirement, the application has to explicitly specify that using different control parameters. Application can choose different security schemes which control the security for transmission of message. Security suits of 802.15.4. Specification can be broadly categorized into two types: secure and unsecure mode. Table 4 gives information of security suits supported by 802.15.4. Each scheme offers different aspects of security. Null suit is unsecure where it defines no security. AES-CTR only performs encryption and gives confidentiality. AES-CBC-MAC provides data integrity which comes with 3 variations

Table 4 Comparisons between various IEEE 802.15.4 security suits

Security suit	Description
Null	Unsecure
AES-CTR	Only encryption
AES-CBC-MAC-128,64,32	Authentication only. Flexible with different MAC sizes: 128,64, 32 bits
AES-CCM-128,64,32	Authentication and encryption flexible with different MAC sizes: 128, 64, 32 bits

based on size of the MAC bit. Size can be 32, 64 or 128 bits. Each one is considered as separate security suit. Higher the size of MAC bits lower the risk of adversary, but it increases the size of packets. Whereas AES–CCM first provides integrity using CBC-MAC later it encrypts the data by using AES-CTR.

However, the above-mentioned security suits faces serious problems. Implementation of AES-CTR is unsafe because, encryption without authentication introduces significant risk of vulnerability at protocol level. Also it is shown that AES-CTR is more prone to denial of service attacks. Further, none of these security suits gives data integrity to acknowledgment packets. With jamming, this loophole can be used to stop the delivery of packets. This makes acknowledgments untrustworthy. A new method of security enhancement in 802.15.4 Zigbee is proposed [20]. This is done by altering the MAC. This paper also presents security enhancement in application and network layer, and it is implemented by using RFID detector and application gateway. In Zigbee, security is maintained by external service provider interface, which work on every layer. In order to enhance the security, MAC addressing, authentication, security unit is added at MAC layer. RFID detector is integrated at network layer, and APL security is included at application layer. Riverbed modeler is used to implement the zigbee protocol and simulation results shows with the proposed work MAC can block unauthorized devices and performs authentication, network layer blocks illegal packet and application layer block adversary data. Since performance and security compete for same CPU, memory, energy and bandwidth, it is very much necessary to analyze the resource consumption, while giving security. Hence, further we study the impact of security on memory, energy consumption and network performance [21]. To test security, authors used 2Tmotesky motes with 48 kbyte ROM and MSP430 microcontroller operates at 8 MHz with RAM of 10 kbytes. In order to analyze the network performance, full function device (FFD) and reduced function device (RFD) are consider. FFD acts as PAN coordinator which manages network and security. RFD acts as a sender and continuously transmits protected data to the PAN coordinator using a common secret key shared between RFD and FFD. After receiving data packets, PAN coordinator verify data frame and sends back ACK. Memory consumption is compared with and without security sub layer. Obtained results shows that without security FFD function takes 33.2 Kbytes that is (69% of total memory) and the same FFD with security consumes 39.31 Kbytes (81.9%) overall there is around 13% increase.

Similarly for RFD takes 34.43 Kbytes (71.7%) without and 39.85 Kbytes (81.1%) with security, 9.4% increase. By adding security layer the size and complexity of PAN coordinator increases. Table 5 shows how different security suits affect the transmission of frames. When compared to null security suit, 26.2% reduction in frames when only encryption (AES-CTR) is provided. With only authentication (CBC-MAC) 28 to 33.5% of frames are reduced (varies with size of MAC bits) and adding both encryption and authentication (AES-CCM) reduces 28.2 to 33.9% of frames. Size of each frame increase with different security suits as it adds overhead. Cost of energy consumption when implemented security suits is shown in Table 6. Overall energy consumption is split into energy for secure one

Table 5 Security impact on frame transmission

Security suit	Frames	Decrease in frame (%)	Frame size (bytes)
Null	7685.5	–	27
AES-CTR	5671.6	26.2	37
AES-CBC-MAC-4,8,16	5534.8, 5371.6, 5110.3	28, 30.1, 33.5	41, 45, 53
AES-CCM-4,8,16	5514.6, 5374.4, 5082.1	28.2, 30.1, 33.9	41, 45, 53

Table 6 Energy consumption

E (μJ)	V (v)	I	t (ms)	Device
$E1$ = 240.54	3.6	17.4 mA	3.84	CC2420
$E2$ = 150.34	3.6	17.4 mA	2.40	CC2420
$E3$ = 2.66	3	600 μA	1.48	MSP430

frame transmission (E1), energy for encryption and authentication (E2) and energy for security management (E3). As 802.15.4 protocol gaining importance for its low-power, low-complexity nature, and all these parameters discussed above plays an importance role hence one has to look in this direction in the design of efficient and secure 802.15.4 protocol.

After analyzing related work it is clear that there is less research work done toward the implementation of efficient and secure 802.15.4 protocol. As for as IoT applications are concerned the existing security suits using AES is unsuitable. Hence, it is important to search for alternative security methods which meet the low power and low-complexity requirements.

5 Hardware Implementation of IEEE 802.15.4

IEEE 802.15.4 defines PHY and MAC layer specifications. PHY is designed to transmit data packets. Physical layer operates at 868/915 MHz and 2.4 GHz. Further revisions in 802.15.4 allow the use different modulation schemes including BPSK, QPSK, O-QPSK, GFSK and UWB. In 802.15.4 data link consists of two parts; link control and MAC. Link control is standard used in all 802 protocols logic. MAC layer is designed to perform various operations like channel access, frame delivery, synchronization; flow control and error control etc. In this subsection, various hardware implementation techniques of IEEE 802.15.4 are discussed. A small subset of 802.15.4 MAC protocol is designed to provide a point to point communication [22]. Author implemented 2.4 GHz protocol design. Mapping of bit to symbol is done by mapping 4 bit of LSB to first symbol and 4 bit of MSB to next symbol. Later each and every symbol are mapped to 32-chip sequence.

Mapped chip sequences now modulated by using O-QPSK. Modulated signals are then added with 16-bit cosine and sine values. Summed signal is finally transmitted. At the receiver sine and cosine are subtracted. Demodulation is later performed to get original signal. Verilog code is used to design the proposed protocol. Virtex-4 pro FPGA is used for hardware implementation which has a clock speed of 100 MHz. Since the design has to work only at 250 kHz; this hardware is not suitable for optimal zigbee transceiver design. However, clock divider circuit can be used, but it will add additional hardware. 2.4 GHz zigbee receiver is implemented using sparton-3E XC3S500E FPGA kit, which supports clock frequency of 250 kHz and 2000 kHz [23]. The receiver consists of O-QPSK demodulator, chip-synchronization and de-spreading block which are designed using Verilog. Further to optimize, the design all the blocks are integrated into single Verilog module. The proposed system gives data rate up to 250 kbps. In [24], MQAM modulation scheme is used to design 802.15.4 transceiver which operates at 2400 MHz. Proposed system consists of FIR filter, serial in parallel out and parallel in serial out shift registers, up and down samplers and a chip generator block. Verilog is used as a designing language and it is implemented over sparton-3 XC3S200E FPGA. Model–sim is used to simulate the waveforms of transceiver. The clock speed used is 1000 kHz and 8 MHz, even though 802.15.4 standard is designed for very low-power applications, designing energy aware transceiver is very much needed. Elmiligi et al. [25] implemented energy scalable 802.15.4 transceiver using a BPSK modulation which uses 868 MHz frequency band. VHDL is used to design zigbee transceiver and AMIRIX AP1000 for implementation. Recently, a design of fully integrated 802.15.4 zigbee transceiver is implemented on ARTIX-7 using Verilog [26]. Table 7 gives the comparison results of the implementation techniques discussed above.

All the research work discussed above only concentrated on the efficient hardware implementation of 802.15.4 transceiver design and they failed to implement security services to 802.15.4 transceiver along with performance. Nain et al. [17]

Table 7 Comparison between different implementation techniques

References	[23]	[24]	[25]	[26]
Design approach	Verilog	Verilog	VHDL	Verilog
FPGA family	Sparton-3E XC3S500E	Sparton-3 XC3S200E	AMIRIX AP1000	Atrix-7
Modulation scheme	O-QPSK	MQAM	BPSK	O-QPSK
Operating frequency	2.4 GHz	2.4 GHz	868 MHz	2.4 GHz
Clock frequency	250 kHz and 2 MHz	1 MHz and 8 MHz	105.502 MHz	270.1 MHz
LUTs	3,228	2526	284	428
FFs	2993	60	227	179
Slice registers	–	320	229	224

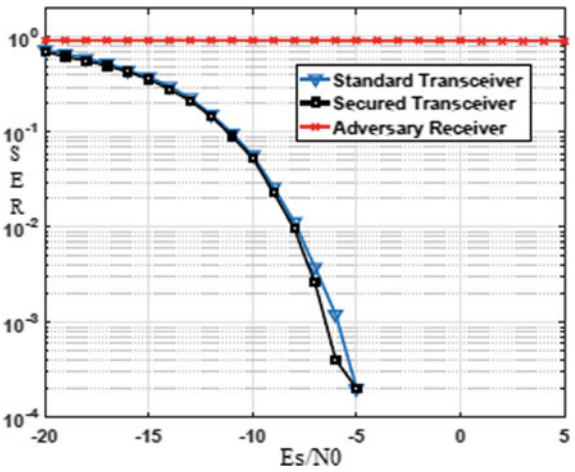

Fig. 2 Comparison of SER

designed and implemented a secure IEEE 802.15.4 transceiver which provides a protection against multiple attacks. Along with the confidentiality and message integrity, proposed scheme provide security to brute-force, cryptanalysis and traffic analysis attacks. Proposed secure transceiver uses a stream PLE scheme using phase encryption which provides a security at physical layer during the modulation. The PHY preamble here uses 8 symbols/256 chips which will be converted to 128 complex samples when it is modulated. Since QPSK is used, one of the 4 phases is used to rotate each sample according to key. This gives 4^{128} possible set of key for 1 preamble. This proposed system resists brute-force attack. Secure 802.15.4 transceiver is designed in Xilinx environment using Verilog. After simulation, results are analyzed in terms of security. Figure 2 gives the comparison of symbol error rate (SER) between standard and proposed 802.15.4 transceiver in noisy environment. The result shows that there is no degradation in SER performance at legitimate node and a very high SER degradation at adversary which increases the difficulty for an attacker to get the plain text.

Proposed system is implemented on Kintex-7 FPGA and ASIC UMC. Synthesis results show that proposed secure PLE based 802.15.4 transceiver uses 132,046 gates compared to the gate count of 104,477 in standard design. 26% increase in the gate count is observed and the implementation on FPGA uses 6507 slices and 15,954 LUTs. However, this resource overhead is because of RC4 cipher.

6 Conclusion

With the growing demand for the IoT applications, IEEE 802.15.4 protocol is gaining much attention in recent times. In this paper, we presented the importance of 802.15.4 PHY and discussed how security can be achieved by exploiting the

characteristics of physical layer. PLS and PLE schemes are studied extensively and distinguished between them. Different PLS schemes are reviewed with their limitations. Next, the concept of PLE is introduced and discussed about stream and block PLEs. Further various PLE implementation techniques are analyzed and compared. However, most of the research works on PLE have been done on 802.11 OFDM. Later, we looked into existing security suits of IEEE 802.15.4 standard and discussed the loopholes in AES based encryption schemes as they failed to provide data integrity to acknowledgment packets. Since performance and security compete for same resources, impact of security on memory, energy and network are analyzed. It is observed that the existing designs consume more memory space and energy. Finally, we reviewed various FPGA implementation of 802.15.4 transceiver design and most of them are only concentrated on performance and the security aspect is completely neglected. After detailed survey, it is observed that a very less research work is done toward the design of hardware based secure and efficient IEEE 802.15.4 transceiver. PLE has low-computational complexity, provides low latency with small power consumption and provides longer lifetime. Future scope of this paper proposes the integration of PLE scheme along with the efficient lightweight key generation algorithm for the design of 802.15.4 transceiver system which can greatly enhance the security and efficiency thereby providing the security to IoT applications.

References

1. ITU, ICT Facts and Figures, 2020. Available on-line at https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx
2. Stankovic, J.A.: Research directions for the internet of thing. IEEE Internet Things J. **1**, 3–9 (2014)
3. Zou, Y., Zhu, J., Wang, X., Hanzo, L.: A survey on wireless security: technical challenges, recent advances, and future trends. Proc. IEEE **104**, 1727–1765 (2016)
4. Wyner, A.D.: The wire-tap channel. Bell Syst. Tech. J. **54**, 1355–1387 (1975)
5. Sun, L., Du, Q.: A review of physical layer security techniques for internet of things: challenges and solutions. In: Entropy (2018)
6. Hyadi, A., Rezki, Z., Alouini, M.: An overview of physical layer security in wireless communication systems with CSIT uncertainty. IEEE Access **4**, 6121–6132 (2016)
7. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. IEEE Trans. Wirel. Commun. **7**, 2180–2189 (2008)
8. Sanenga, A., Mapunda, G.A., Jacob, T.M.L.: An overview of key technologies in physical layer security. In: Entropy, Multidisciplinary Digital Publishing Institute (2020)
9. Johansson, M.: Benefits of multiuser diversity with limited feedback. In: 4th IEEE Workshop on Signal Processing Advances in Wireless Communications—SPAWC, Rome, Italy, pp. 155–159 (2003)
10. Zou, Y., Zhu, J., Wang, X., Leung, V.C.M.: Improving physical-layer security in wireless communications using diversity techniques. IEEE Netw. **29**, 42–48 (2015)
11. Ren, K., Su, H., Wang, Q.: Secret key generation exploiting channel characteristics in wireless communications. IEEE Wirel. Commun. **18**, 6–12 (2011)
12. Trappe, W.: The challenges facing physical layer security. IEEE Commun. Mag. **53**, 16–20 (2015)

13. Wang, S., Li, W., Lei, J.: Physical-layer encryption in massive MIMO systems with spatial modulation. China Commun. 159–171 (2018)
14. Zhang, J., Marshall, A., Woods, R., Duong, T.Q.: Design of an OFDM physical layer encryption scheme. IEEE Trans. Veh. Technol. **66**, 2114–2127 (2017)
15. Li, W., Mclernon, D., Lei, J., Ghogho, M., Zaidi, S.A.R., Hui, H.: Cryptographic primitives and design frameworks of physical layer encryption for wireless communications. IEEE Access **7**, 63660–63673 (2019)
16. Huo, F., Gong, G.: Physical layer phase encryption for combating the traffic analysis attack. In: IEEE International Symposium on Electromagnetic Compatibility (EMC), Raleigh, NC (2014)
17. Nain, A.K., Bandaru, J., Zubair, M.A., Pachamuthu, R.: A Secure phase-encrypted IEEE 802.15.4 transceiver design. IEEE Trans. Comput. **66**, 1421–1427 (2017)
18. Razvi Doomun, M., Sunjiv Soyjaudah, K.M., Bundhoo, D.: Energy consumption and computational analysis of rijndael-ES. In: 3rd IEEE/IFIP International Conference in Central Asia on Internet, Tashkent, pp. 1–6 (2007)
19. Sastry, N., Wagner, D.: Security considerations for IEEE 802.15.4 networks. In: Proceedings of the 3rd ACM Workshop on Wireless Security, Association for Computing Machinery, New York (2004)
20. Biddut, M.J.H., Islam, N., Sultana, R.S., Sarker, A., Rahman, M.M.: A new approach of ZigBee MAC layer design based on security enhancement. In: IEEE International Conference on Telecommunications and Photonics (ICTP), Dhaka, pp. 1–5 (2015)
21. Daidone, R., Dini, G., Tiloca, M.: On experimentally evaluating the impact of security on IEEE 802.15.4 networks. In: International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, pp. 1–6 (2011)
22. Bhat, N.S.: Design and implementation of IEEE 802.15.4 mac protocol on FPGA. In: Innovative Conference on Embedded Systems, Mobile Communication and Computing (ICEMC2) (2011)
23. Ahmad, R., Sidek, O., Shukri, M.: Implementation of a Verilog-based digital receiver for 2.4 GHZ Zigbee applications on FPGA. J. Eng. Sci. Technol. **9**, 135–152 (2014)
24. Supare, V.P., Sayankar, B.B., Agrawal, P.: Design & implementation of MQAM based IEEE 802.15.4/ZigBee tranceiver using HDL. In: International Conference on Smart Technologies and Management for Computing, Energy and Materials (ICSTM), Chennai, pp. 455–458 (2015)
25. Elmiligi, H., El-Kharashi, M.W., Gebal, F.: Design and implementation of BPSK MODEM for IEEE 802.15.4/ZigBee devices. In: IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Vancouver, BC, pp. 1–5 (2016)
26. Guruprasad, S.P., Chandrasekar, B.: Design and implementation of 802.15.4 transceiver for wireless personal area networks (WPANs) on FPGA. Int. J. Innovative Technol. Exploring Eng. (2020)