Energy Saving Mechanisms in the Security of the Internet of Things

Morteza Zolfpour Arrekhlou[1], Afsoun Sarvqad[2], Pouya Rouzbeh Javan[3]

1. **Assistant Professor of Computer and Information Technology, Sepidan Branch, Islamic Azad University, Iran, Sepidan**
2. **Student MSc in Electronic Engineering, Sepidan Unit, Islamic Azad University, Iran, Sepidan, Sarvqad.asarvghad@rose.shirazu.ac.ir**
3. **Student MSc in Electronic Engineering, Sepidan Unit, Islamic Azad University, Iran, Sepidan**

Abstract

Energy consumption is one of the priorities of security on the Internet of Things. It is not easy to find the best solutions that will reduce energy consumption, while ensuring that the security requirements are met. Many of the issues that have been presented so far have covered the basics of security, such as the basic principles of encryption, extension environments, target applications, and so on.

This paper examines one of the most effective energy-efficiency mechanisms for providing Internet-based security services. By studying techniques that enable the development of advanced energy-efficient security solutions, we take a closer look at the ideas that have already been introduced in this area. In this study, not only the security issues, but also the energy impacts on solutions have been considered. Initially, the amount of energy related to security services is introduced. Then a classification is proposed for energy efficient mechanisms on the Internet of Things. Finally, the main drivers of the impact of energy saving techniques are analyzed for security solutions.

Keywords: Internet of things, Security, Energy Saving

Received 01/06/2018
Approved 01/07/2018

1. INTRODUCTION

The Internet of Things (IoT) is a relatively new idea that attracted the attention of all the scientific and industrial communities. It involves network expansion in the true sense of the word, including the connection of physical things. With respect to communication technologies, the things (such as sensors, stimulators, RFID tags) can communicate with each other as well as with users to achieve common goals. Although the potential of the Internet-produced things helps many different applications in different areas (such as intelligent cities, smart grids, health care, etc.), the deployment of this technology on a large scale also depends on power and security [1, 2].

Many Internet applications are the things that are very sensitive. For example, the parameters measured by sensors in a health care program measure the physiological signs of a human being, such as heart rate or body temperature. This sensitive information should not be made available to unauthorized persons. On the other hand, the Internet of Things for many types of attacks is vulnerable. The ability to listen (eavesdropper), modify or interfere with information in networks that typically use wireless communications without proper infrastructure is easier than wire-based networks. The things can also be compromised, and malicious nodes may enter the network, which may lead to unauthorized actions on data and network resources. In addition, the Internet of Things can be a major breach of privacy for users. Therefore, it is important to consider the security services needed to ensure the protection of the Internet of Things from attacks.

Security services are usually based on heavy-duty programs (e.g., encryption / decryption and signature / authentication). They generally need to consume a lot of resources to maintain a high level of security. However, the Internet of Things includes devices that are limited in terms of resources (e.g., energy, storage, and communications). The use of heavy security initiatives in some nodes, as RFID sensors or tags, requires a lot of energy resources, which can distract nodes from performing their core tasks. Since nodes are powered by batteries and are expected to continue to operate on the same battery for a long time, the optimal energy consumption of this type of network is essential and vital. When the things need to operate independently without human intervention, battery replacement may even be impossible in many cases. Therefore, security solutions should work with regard to the energy constraints of the nodes or with a long-term view of them.

Received 01/06/2018
Approved 01/07/2018

With the advent of Low-power and Lossy Networks (LLNs), several studies have been conducted on energy-saving solutions for security services. These studies are diverse and include a variety of aspects, such as security initiatives, development environments, targeted applications, and so on. Therefore, finding an efficient method is important and requires careful study that reduces energy consumption while providing a degree of security assurance. The goal is to evaluate the efficient energy mechanisms that can be used in Internet security things. This research is designed to help design security protocols and to choose the right mechanism for energy saving. With this aim in mind, this paper proposes the categorization of energy-efficient mechanisms in the Internet of Things, examining each of the major mechanisms and analyzing its application. The benefits of this review are helping to use energy efficient mechanisms for Internet security solutions. While other studies on the security of the Internet of Things have focused more on energy efficiency protocols, we go beyond this and we propose an energy-efficient solution based on energy efficiency.

The contents of this review can be summarized in three principles:

- Discussion of the security services on the Internet of Things from the point of view of energy consumption
- An energy efficient energy efficiency classification is suggested in the Internet Security of the Things. Each of them, along with some of the suggested solutions that use these mechanisms, is being studied.
- Discussion on the environment and application of energy saving mechanism in the Internet security services of the things.

The remainder of this article is as follows: In Section 2, studies on the security of the Internet of Things are presented and the motivation for doing so. Part Three deals with services that can be taken into consideration to ensure the security of the Internet. It will also point to the amount of energy related to security services. Energy saving mechanisms in security will be studied in the fourth section. This section provides a classification of existing mechanisms and examines the solutions that use these techniques. In the fifth section, we will look at the appropriate environment and the use of energy saving mechanisms for Internet security solutions. Finally, Section Six concludes with this article.

2. RELATED WORKS

Received 01/06/2018
Approved 01/07/2018

Several studies on the security of the Internet of Things have led to the emergence of security issues on the Internet of Things. Most of these studies examine existing security protocols and their solutions. For example, Autoseri and colleagues [1] conduct a general study of the Internet of Things, and they study some privacy restrictions and privacy solutions, as well as issues that may be addressed. Mirundi and his colleagues examined the same observations [2].

Other surveys deal with a specific security service on the Internet. Roman et al. [3] have evaluated key management systems for Wireless Sensor Networks (WSNs) in the Internet of Things. These reviews include public key cryptography, pre-shared key and key management systems associated with the link layer. Yan and his colleagues [4] offer a survey on trust management for the Internet of Things.

The authors identify the goals of trust management systems and evaluate existing Internet solutions for the things. Nguyen and colleagues focus on bootstrapping on the Internet of Things. They provide a classification of the existing security protocols for a secure Bootstrap process on WSNs and the Internet of Things. They also discuss their use and limitations.

Other studies on the security of the Internet of Things have led to the proposal and deployment of a new architecture. The authors focus on the security and privacy of Internet distributed objects. They carry out the features of the distributed method and analyze the attacker's models and examine the existing security solutions. Greenal et al., [7] pointed out in another study how to create a secure way when connecting things to the Internet. This paper will highlight the low-level integration of WSN strategies with the Internet and the security it needs, looking at the integration approach.

Research reference	Research objectives
[1 and 2]	Open Public Issues in Internet Security Things
[3]	KMS for WSNs on the Internet of Things
[4]	Trust Management Solutions and Challenges
[5]	A solution for a secure bootstrap process

Received 01/06/2018
Approved 01/07/2018

[6]	Security issues and privacy on the Internet are distributed objects
[7]	WSN security solutions integrated with the Internet
[8]	Security standards for Internet communications objects
[9]	Security, privacy, trust needs and solutions
[10]	Security rules and privacy challenges

Table 1: Research on Internet Security of Things

The expansion and deployment of the Internet of Things is dependent on the development of new communications protocols and standards. Granoll et al. [8] refer to the security standards for Internet communications of Things. They consider a stack of standard communication protocols designed for the Internet of Things. Then, they consider security issues and discuss the stack for each communication protocol.

The security offers provided relate to middleware-based projects and solutions. Sikari [9] has conducted a survey on the Internet of Things. They analyze existing solutions in terms of security, trust and privacy, as well as the exclusion of projects and middleware that deal with these issues.

Issues of security and privacy on the Internet of Things can also be legally discussed. Weber [10] refers to the Internet security of things. He offers security and privacy requirements and discusses strengths to create a proper legal framework by an international legislator.

This review of the studies mentioned above is different in comparison with the Internet security of things. In fact, many of the solutions provided to provide network security point to energy as a key factor in the security of the Internet of objects, since it is expected that things with limited resources are independent for a period of time Work a long time. On the other hand, there have been numerous works on energy security issues in the field of security. The aforementioned research further explores the solutions that are appropriate for the Internet of Things (summarized in Table 1); mainly refers to energy efficiency goals. The purpose of this

Received 01/06/2018
Approved 01/07/2018

study is to explore techniques that enable the development of energy-based security solutions. This provides an instructional approach and helps design a security protocol to optimize efficient solutions. Such a view has not been used in previous studies.

To achieve the goals set out in the research, we begin by providing some of the security services on the Internet of things, as we will point to the efficient and efficient use of energy.

3. SECURITY SERVICES ON THE INTERNET

Security can be guaranteed by using certain services to protect against attacks. In fact, security services are based on the steps needed to deal with threats. In Section 1, we will examine some of the security services that can be used on the Internet of Things. This section also relates to security related resources.

3-1 Confidentiality

Information privacy is a security service that ensures that the contents of a specific message are not accessible to an unauthorized person. This is done by encrypting messages using symmetric or asymmetric encryption, so it can only be decoded by the authorized person.

With low power consumption (limited nodes), symmetric cryptographic schemes are widely used in limited networks such as WSNs. Many evaluations, for example [11, 12], show that symmetric ciphers (such as AES, RC5 [13, 14] or Skipjack [15]) are suitable for finite things. However, key management in symmetric encryption creates problems when a large-scale network is found.

In the Internet of Things, the problem of scalability is more intense. In fact, since 2006, writers such as Lopez [16] further reveal the limitation of the use of symmetric encryption for WSN. On the other hand, asymmetric cryptography provides efficient key management, but it increases the consumption of more energy than symmetric cryptography. Protocols such as RSA [14] or IBE [17], which are widely used on the Internet, are very sensitive to computations. In terms of processing and consuming resources, the use of these protocols for the Internet of objects will be very heavy.

3-2 Authentication and access control

Received 01/06/2018
Approved 01/07/2018

Authentication is a security service that is used to ensure that people who claim to be (corporate authentication) or received messages are the same as the original message (message confirmation). As used to control access or to allow or prohibit access to resources by a person, according to the organization's policy. Access control is generally performed after the verification of institutions / data.

Because of the low cost of computing, some access control and verification solutions are used in networks that are limited by symmetric encryption (including [18-20]). It is often used with mechanisms for distributing keys. However, it may also do these solutions only for applications designed for them and may not be supported on large-scale networks. Moreover, when using symmetric cryptography, it is difficult to ensure that the message is verified with the advantage of not denying it. Even though some solutions, such as SNEP and μTESLA [21], need to synchronize time and manage keystrokes by storing them by mimicking asymmetric encryption (through disclosure of latency keys and one-way key chain keys). This will cause traffic problems for large and large-scale networks.

On the other hand, authentication and access control solutions based on asymmetric cryptography eliminate the need for more complex protocols and increased security. However, public key cryptography in a limited node is very difficult to process and consume, as previously mentioned. For example, feature-based encryption (ABE) and its related protocols are widely used to control access with scalable management. Considering these protocols for limited networks, for example, the Internet of Things, is related to the cost of consumption.

3-3 Signature / confirmation

Digital signing is a security service that adds an entity or identity to a piece of information. This ensures authentication, integrity and non-denial. One of the most important uses of digital signatures is public key certification.

For digital signatures, public key cryptography is used more often. X.509 and ISO / IEC9796 are based on public key cryptography. Examples of asymmetric encryption have been used in the RSA encryption [14] or the prototype [24]. However, these asymmetric protocols are very heavy in terms of calculation, and their direct use of objects for the Internet will be inappropriate.

Although single-signature designs (many of which come from symmetric key encryption) require less computations, they need to be changed after each use. So that signatures cannot be

Received 01/06/2018
Approved 01/07/2018

falsified [25]. It affects the storage and capacity of communications and traffic in networks and reduces the percentage of use of these schemes for some applications.

Cause	Explanation
Heavy operations	The basic operations used in asymmetric cryptography is usually heavy
Data size	The size of the data is proportional to the overhead on energy consumption
Number of calls	The frequent use of a security service can have a huge impact on consumption

Table 2: Analysis of energy consumption in security services

3-4 Key deployment

A key deployment or bootstrapping key is a process that allows the setting between two or more parties to be used to share encrypted keys. Essentially, a secure communication link between the nodes (before the network can work or when a re-entry is required) is necessary to be able to perform other security services.

Pre-distribution designs are commonly known as symmetric key designs, which include quantitative calculations. They work on pre-installed credits (pre-deployment). Several pre-distribute solutions are presented in this area, which are mainly used for WSN (such as [26-30]). However, these programs can also be designed and executed for local networks, but the creation of keys with a remote entity cannot be solved. Many Internet objects of the things require the establishment of secure connections between nodes without the need for any prior knowledge of each other or shared sharing keys.

In contrast, asymmetric key designs for the Internet are more focused and do not require basic knowledge. However, the two categories of asymmetric key designs, key transfers, and key agreements, include high-level computing and processing. Key transport protocols (such as loss) TLS [31] are based on public key cryptography, which is usually sensitive to resources. Key protocol protocols (such as Internet Key Keys (IKE), the Host Identity Protocol (HIP) [33]) also use many resources, because they essentially use asymmetric encryption.

Received 01/06/2018
Approved 01/07/2018

Additionally, an authentication mechanism for asymmetric key designs may be needed to connect the partner key to establish a connection. Asymmetric key patterns for very limited resources such as the Internet of things cause very heavy pressure.

3-5 Negotiation

Several security services for the Internet are needed, many of which include heavy bumps. The issue of energy savings in LLNs should be solved somehow. For example, it offers several key solutions to create WSNs based on pre-distribution (less energy consumption, but not economical for large networks). However, the Internet faces new features, such as scalability. This makes some energy security solutions not suitable for Internet applications at the moment. The problem of energy use in security services is more intense in the Internet of Things.

To understand the overhead reasons, an analysis is made on the use of security services in the context of the Internet of Things. The results of this analysis can be summarized in three levels: heavy operations, data size and number of calls. Table 2 provides a summary of the above analysis.

Heavy operations

The most important reason for high security costs is heavy processing operations. This processing is mainly done in asymmetric cryptography. In fact, asymmetric cryptography is based on the use of hard issues for security purposes, so it is impossible or very difficult to reconstruct private parameters from the public [25]. The mathematical operations used for these types of issues are issues such as exponential (power) and residual issues that are generally operational with heavy processing.

The power (g^e) and its residual (g^e mod p) are the basis of many cryptographic protocols such as Delphi-Hellman (DH) [34] (which are the basis of many key negotiation protocols) or RSA. These operations are very computationally heavy, since the parameters used in it are numerically numerical for a number of reasons. Shrinking the parameters can reduce the overhead of the operations, but it is not always possible, as the risk of guessing the parameters increases. Watro et al., proposed adaptation of the RSA protocol with limited resources. Their idea is based on the use of smaller parameters such as less power. However, this is at the expense of the security level [36]. The evaluation by Watro et al. [35] on Mica1 shows that RSA deviation can reduce the runtime by more than 10 seconds using small indexes.

Received 01/06/2018
Approved 01/07/2018

Other operations that are used in many cryptographic protocols are a two-way linear pairing. These are other applications to provide security concepts such as IBE [17] and its variants (the idea of which was given by Shamir in 1984) (or ABE [23] and its variants). However, these are extremely heavy-duty operations for limited nodes (the basic mathematical operations are heavily based on basic processing). Olivera et al. [38] and colleagues show that running pairing operations on the MicaZ node using the TinyPBC suggestions requires more than 5.5 seconds. Given the fact that cryptographic operations generally require pairing at least twice, it means that the security service can take up to 11 seconds.

Data size

A security service is used to ensure data is secure. The time taken to run the security service is proportional to the size of the data. When the data size is large, it will take longer to run. Energy consumption follows directly from this fact.

The data size is not only about the data to be processed, but also the metadata of the security protocol data. In fact, security protocols that outline communication aspects, such as Internet Protocol Security (IPsec), Transport Layer Security (TLS) [40], or Datagram TLS (DTLS) [41]), a packet header have been considered. As it is sent and received by limited nodes, the size of this series also affects the amount of energy consumed.

Number of calls

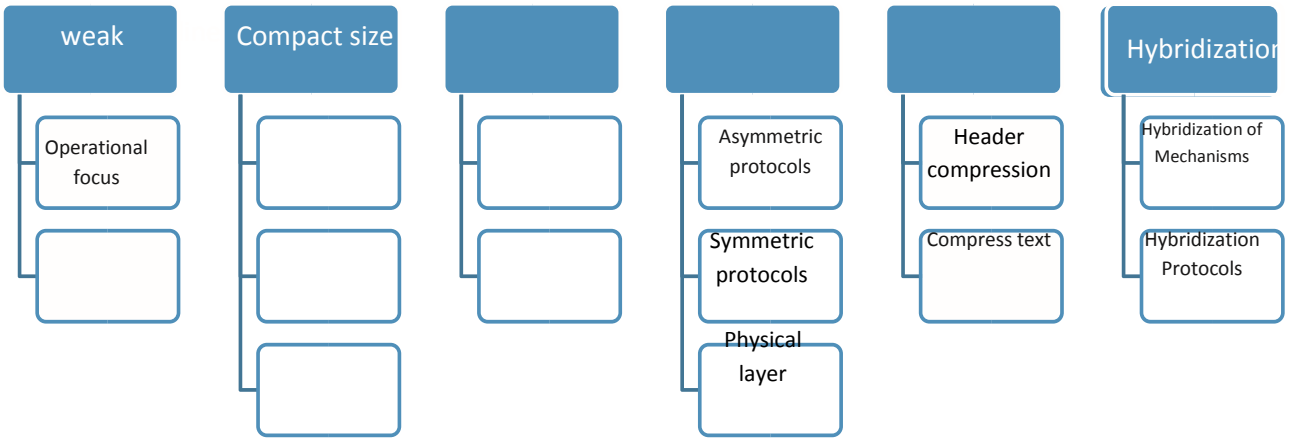
Another issue that affects the amount of energy used by security services is the number of calls. This parameter depends on how the security service is used, as well as the number of times that you need to use this service. For example, consider a key deployment protocol that is relatively heavy (in seconds or seconds, respectively). A limited node can execute this protocol at one time at the same time. However, if this step is repeated several times (for example, because of a re-request), the energy implications can be critical. The frequent use of a security service has a great impact on consumption, compared with a small use of it.

It seems that many of the security protocols needed on the Internet are heavy computing and computing. This raises the need for mechanisms that reduce energy consumption in security solutions. The next section examines energy-efficient energy security techniques.

4. Energy saving techniques in security

Received 01/06/2018
Approved 01/07/2018

In this section, we examine the main mechanisms available to save energy in security services. Solutions that use these techniques are also provided. The proposed classification of energy saving mechanisms is summarized in Figure 1.



Online security / offline security (offline)

The concept of online security / offline (offline) involves breaking down the encryption scheme in two steps. First, it is done offline (before the security service) (before knowing the destination, encryption message or signature, etc.) before the security service begins. This phase reduces part of cryptographic overlays by computing and storing the results of some of the operations that are required. The second step is done online. Using the stored results from the first phase, and its use in the second phase, the operations will be very quick [42, 43]. Therefore, online / offline security (offline) can reduce energy consumption by off-line transmission, before deployment (or when an available external power source is available), and only in the second stage Instead of the entire encryption scheme, it will do just that.

An online / offline approach (offline) to change the security scheme in the encryption algorithm helps to create two steps. Heavier operations are transmitted to the offline stage (offline), so the energy consumption for the plan is reduced. Obviously, what is transmitted offline must be computed before the security service begins. It is difficult to use an online / offline approach because some heavy operations generally relate to data that may not be known in advance (e.g., encryption message, destination key, etc.). Based on the two-phase method for encryption, we propose to classify online / offline (offline) approaches into two categories: axis-driven and service-centric.

Received 01/06/2018
Approved 01/07/2018

4.1.1 Operations-oriented

The correct method for enforcing online / offline security is performed by transferring all advanced operations that need to be pre-calculated to offline. This will reduce the consumption associated with it, in the online phase. Operational-focused solutions are placed on the surface of the encryption operations and offer a way to calculate these operations.

Some security plans can naturally be divided into online and offline stages. Pleasure and his colleagues in [44] propose schemes that optimize the power consumption of cryptographic operations in wireless sensor networks (EH-WSN).

	Balanced assistant	Focused on threats
Service focused	Half-balanced assistant	Data-centered
	An unreliable assistant	

The sequence of passwords is usually executed using the XOR operator between simple text bytes and key sequence bytes. These are produced randomly from the series. The proposal is based on preprocessing of bytes and the key sequence buffer during periods of high energy, and they can be used in subsequent procedures. The results of the evaluation using the code sequence Trivium ATmega128L and MSP430 indicate that energy consumption can be reduced by 14%.

In [43, 45], Schnorr is offering nonlinear sign-on / off-line signing plans for smart cards. Its purpose is to reduce the cost of the calculator for the signer and to obtain consistent equivalence-based (fixed-base) matching algorithms, which are examples of Brickell-McCurley [46] or El-Gamal [24]. This is done by preprocessing and saving a set of x i = a r i mod p and r i are randomly selected. For each signature, the conjugate is calculated as the multiplication of x i. However, Flight in [47, 48] shows that the plan is vulnerable to attacks that run on secret key recovery (private key). In fact, the combination of power does not guarantee randomness, and dependency may be created, leading to a successful attack chance. Since then, other solutions have been proposed to predict synchronic calculations. For example, the suggestion in [49] introduces a method for dividing the power to a product of a given number of cases with more crashes. A suggestion inspired in [50] by its idea. This is a surplus

Received 01/06/2018
Approved 01/07/2018

chain technique for calculating product yields. This method is a bit slower than the method described in [49], but requires much less memory.

Geo et al. [51, 157] (and other works such as [52-55]) in designing an on line / off-line project (for offline) for a variety of IBE-based encryption such as Boneh-Boyen IBE [56, 158] or goutricus IBE [57] are using this method. In such protocols, neither the message nor the identity of the recipient at the offline stage is known. This idea is based on the addition of a correction factor. In fact, in the Boneh-Boyen IBE encryption text, the section containing the destination attribute takes the form below.

$_0 = (h_1 . g_1^{ID})$

And a message m for encryption takes the form below.

$e (g_1 , g_2)^s . m$

(e represents a two-way or two-way map, while g_1, h, and g_2 are elements of a cyclic group of first order blows, see [56] for details). For the second part, e $(g_1, g_2)^s$ can be performed off-line and only one line multiplication (online) is required. However, in the first part, the identifier is in powers, which are the operations that have high energy consumption. The solution is modified according to the following model. In the offline, C_1 and C_2 form are calculated $_1 = (h_1 . g_1^{\alpha})^s, C_2 = g_1^{\beta s}$.

Note that α and β are random numbers). The node in the online C3 (offline) is calculated as C 3 = β-1 (ID –α) and adds it to the encryption text. This method requires a multiplication and a subtraction. Decoding can be obtained by calculating C0 as $C_0 = C_1 . C_2^{C_3}$. This may be due to the presence of an algebraic relationship between different identities. Note that these methods generally use key encapsulation mechanisms (KEM^2) to speed up the on-line online process.

In [58], Hopper and Waters suggest on-line and off-line schemes (on-line / offline) for feature-specific encoding (ABE). Offline as defined in IBE, neither messages nor attributes in encryption are used. The authors talk about a large structure [59], which provides an algebraic relationship between traits (a correction solution similar to that already provided for IBE). Additionally, authors propose the key generation phase, online / offline optimization. The bulk of the key-production work can be done by offline servers and then transmitted to online servers, while incoming requests can be processed quickly. (A similar correction solution is used to generate keys). The evaluation of the performance suggests that more than 99% of computational work can be transmitted to off-line (offline) in many scenes.

Received 01/06/2018
Approved 01/07/2018

4.1.2 Service-oriented

The second-class line-of-security / offline is called service-oriented. Unlike the first, service-centric approaches provide methods for constructing two phases without going to the level of cryptographic operations. Online / offline line-based services-based services do not require advanced knowledge of the encryption operations protocol to build processes. Some of the related solutions are listed below.

In [42], Eyon et al., offer a way to build online / offline sign-offs. The solution is one-time signatures that are computationally very fast. The offline phase involves generating the pair of confirmation / confirmation keys at once and signing them using the signature signing scheme (energy efficiency optimization). Online, the node retrieves unused pairs of one-time keys and then signs the message using a signed signature once (fast-acting) signature. Confirmation is performed by checking the first key once according to the original signature designs (to confirm that it has been signed by the sender), and then this key can be used to confirm the message. However, as described in other works, this method increases the size of each of the signatures by a quadratic factor, which is the main problem (note that the confirmation of the key once and its signature both Signed messages are attached to enable verification.)

In [60], Shamir and Theon consider another online / offline signature scheme (online / offline) based on secret hysterics functions [61]. An interlocking Hash function, h, is a potential function connected to two keys (a public key HK and a private TK). More precisely, given a message such as m and an auxiliary like r, it is difficult to find m, r so that h (m, r) = h (m ', r') is only known by HK. Let's deal with knowing the two keys. However, when TK is also known, it's easy to find them. In the off-line (offline), the node randomly generates m ', r', and the hash (Hash) uses HK to calculate them. The result is then signed using the essential signature plan. When the message for the signature, m, in the online phase is known, uses the node of its TK to find r such that h (m, r) = h (m ', r'). To confirm the need to calculate h (m, r) before validating it using the signature scheme is essential. Compared to Yewon's and his colleagues' suggestions, only r should be added to the signature to be verified.

In [62], Bainchi et al., have proposed an on-line / off-line project, which supports the CP-ABE protocol [63] in the EH-WSN. The problem with using such a design for ABE relies on the fact that if the message is not known in the offline phase, its features will not be determined (access policy). Their proposed solution uses KEM (using offline CP-ABE encryption and encryption

Received 01/06/2018
Approved 01/07/2018

codes online using session keys) and based on knowledge of access control policies that can be implemented over the length of time Program modes to be considered. When there is an energy surplus, the session keys are generated and encrypted using access control policies, which is most likely to capture the situation and this method is useful. The Markov model is based on choosing the best strategy to store and minimize potential cache. However, this technique can only be used for this matter, because information about destination and access is not always available. The difference between online / offline approaches (online / offline) (operations-oriented and service-oriented) has created a two-step solution. Online and offline solutions identify heavy protocol processing operations and suggest that they provide a mechanism to predict their computation. In contrast, service-focused solutions provide a way to build two phases without reducing heavy activity. This will make the client solutions more general than the centralized activity. Even the proposal in [62], which raises the CP-ABE protocol, can be considered for other protocols.

A summary of security solutions

On line / off-line (online / offline) is presented in Table 3.

Service / protocol	Network / device	Pre-Calculation Method	Reference	operations
Authentication	EH-WSN	Direct	[44]	Operations-focused
Signature	Smart cards	Expandable Factor	[43, 45, 49 and 50]	
Confidentiality	Smart cards	Correction technique	[51]	
Access control	Smart cards	Correction technique	[58]	

Received 01/06/2018
Approved 01/07/2018

Signature	--	Signing up once at KEM	[42]	Service-focused
Signature	----	Intersecting function	[60]	
Access control	EH-WSN		[62]	

Table 3: Online / offline security-based approaches

4.2 Security outsourcing

The outsourcing approach is based on the use of cryptographic support for high cost computing operations. This includes dividing the encryption algorithm into two parts. The first case runs locally, which has less computational compression. The second item is computed by cryptographic helpers and can perform computational calculations. Outsourcing solutions can reduce energy consumption by providing some operating costs to more powerful devices.

Outsourced security is stronger for assistants based on heavy operations. However, the interference of other entities in a job such as security may be crucial and strategic. For example, consider the CP-ABE protocol [63]. Part of the encryption operations is performed by multiplying the plain text M with exponent e $(g, g)^{\alpha s}$. A simple way to apply outsourcing is to calculate e $(g, g)^{\alpha s}$ in the node. However, knowing this flexibility will help the node retrieve plain text, even if it does not (split with power) into the node. Additionally, if the nodes return the wrong result, this can lead to a misleading security operations.

Depending on the type of donation nodes and what should be given, we suggest that we consider categorizing outsourcing approaches into three types: remote security using Trust Assistants, use of Half Trust Assistants and the use of Unreliable Assistants.

4.2.1 Trust Assistants

Browser security can rely on trust helpers (trust assistants). Both sides fully trust me and there will be no security risks. Therefore, heavy operations can be transferred to that assistant without compromising security. Some outsourced security approaches are based on the trust assistants in the following cases.

Received 01/06/2018
Approved 01/07/2018

In [36, 64], Ho and his colleagues provide a security service based on the RSA and XTEA protocol [65] for WSNs, using the help of a Trust Platform (TPM). TPM is a processor assistant that is intended to be added. It is a dedicated security chip designed to support cryptographic operations such as key generation, message signing and message encryption using a secure hash algorithm and random generators [66].

Katmaier et al. [67, 68] suggest a method for creating and activating a key in DTLS using TPM assistance. TPM-equipped nodes can achieve full-fledged access to secure communications. Other nodes that are not equipped with TPM share DTLS types with shared keys.

Other solutions for providing similar help as TPMs are provided by using other types of hardware. In [69], Barbareschi and colleagues have provided an implementation to support RSA / AES based security services on WSNs using the FPGA (Xilixn Zynq 70 0 FPGA / SoC family). Josef et al., [70] provided an outsourcing approach to implement IBE in a WSN. Their solution relies on the use of the ARM processor (ARM1176JZF-S) instead of the TPM chip.

Trust outsourcing solutions are mainly based on hardware devices that can be added to the resource-limited node. This can help us to become more confident about security. However, this can be very expensive because the need to equip each resource-limited node with a dedicated assistant.

4.2.2 Half Trust Assistants

When a dedicated hardware such as TPM is not available as a trust assistant, a node may access unrestricted devices to perform external encryption operations externally. However, when it does, it is very important to ensure that the information that the donor does not deliver is not securely disclosed to others. This requires confidentiality to be respected when outsourcing is secure. The term "half-trust" refers to an entity that correctly performs what is requested, but can also provide more certainty about the reliability of the information. Here are some of the solutions that help assistants or half-trust assistants when outsourcing security:

Thaati et al., [71.72] provide an outsourcing approach that enables a limited resource node to encode data using ABE (CP-ABE [63] and KP-ABE [73]), and it Save on a remote server. As explained in their papers, the power (exponential) for linear calculation increases with the number of traits. Their approach to computing the exponential a g includes the selection of n helpful tools and the division of a into n, part a, with the sum of all of them equal to a.

$(a - \sum_{i=1}^{n} a_i)$

Received 01/06/2018
Approved 01/07/2018

Then, each calibrator shows the ga i calculations, and the limited resource node can obtain the initial data with some multiple multiplications.

$(g^a = \prod_{i=1}^{n} g^{a_i})$

Green and his colleagues proposed [74] a method for deciphering ABE in cloud storage applications. Its goal is to reduce the cost of decoding allowed users to request data stored in the cloud. In their proposed solution, they stated that the cloud user could be converted with a switch that allows the cloud to nearly decode the encrypted text to the same encrypted text without being able to read anything about the message. After that, the user can perform decryption using his secret key with cheaper operations.

4.2.3 Unreliable Assistants

Another aspect that can be created when developing outsourced security solutions is to be careful. In fact, even if the helper cannot learn something about the security of information, returning wrong results will result in false security operations. The term "unreliable donor" means that the donor may potentially have an error and result in inaccurate results. Therefore, in these cases, external security solutions require mechanisms to check the outcomes and identify failures. Below are some of the metrics that are presented to assistants (unofficial donors).

In [75], the authors provide a protocol for modifying the adaptation license g a mod p using two unreliable assistants. In their solution, it is assumed that one of the contributors may deviate from the correct function, regardless of which one of them has this error. This is based on the breakdown of a and g into fragments that are randomly sent to each donor (to ensure confidentiality), and then they want to compute a set of (base profiles). The limited resource node can test donors by comparing some of the outputs that should provide the same result.

In [76], authors propose the method of obtaining the calculation of elliptic curve pairs e (A, B) using a donor. The restricted node requests a series of hidden pairs of A and B, then examines the outputs by comparing the ones that should show the same result. However, this solution needs to perform multiple computing nodes.

Ben Saideh et al., in their work [77], deal with asymmetric key designs (the key to transportation and the key to the agreement) for the Internet of Things. They use several donors and offer thresholds. In this method, the receiver can construct the main message (n is the number of contributors) to construct the original message if at least K receives a piece of n

Received 01/06/2018
Approved 01/07/2018

message piece. In fact, in addition to protecting the threshold distribution against packet loss, it can also be used to check accuracy. By constructing and comparing different combinations of k packages from a set of n packets, one can identify a node that detects incorrect information. A suggestion for key transfer from Sayed and colleagues [77] considers protocols such as TLS and understands them. In the protocols, heavy sections of processing operations are asymmetric processing (encryption with the public key of the recipient and the signature of the message). The authors' solution is based on dividing the secret message into pieces and sending each one to a donor who performs asymmetric cryptography. The threshold distribution is based on a default error correction method [78] that adds redundancy to the packets so that if at least K packets are received, it can be retrieved.

The second proposal [77] is the Diffie-Hellman-based Collaborative Key Protocol, such as the IKE and HIP. The more costly parts of the calculations are two modular (DH) and signature. To calculate the modular (modular) g^a mod p, the authors suggest that a be divided into n parts a i, such as:

$\sum_{i-1}^{n} a_i = a \bmod p$

Each aid receives an a $_{i \text{ and}}$ calculates g ^{a} i mod p. The restricted node only applies n multiplications to obtain a modular one.

$(g^a \bmod p = \prod_{i}^{n}{}_{1} g^{a_i} \bmod p)$.

The signature is also loaded into donor nodes. The threshold distribution is based on the Lagrange polynomial algorithm used in [79].

The principle of outsourcing some cryptographic operations to stronger assistants effectively helps reduce energy consumption. However, it may also raise security issues. The difference between the three approaches in the node type is helpful. Once trusted, each section can be sent to the donor without any security concerns to do that. The use of half-trust assistants entails the risk of confidentiality of the data; the transferred part should not lead to data disclosure. Similarly, when using donor nodes that may potentially be mistaken and return the wrong results, the outsourcing solution should examine the mechanism to validate the results. Table 4 examines a summary of security approaches.

Service / protocol	Network / device	Confidentiality	Reference	operations

Received 01/06/2018
Approved 01/07/2018

RSA/XTEA based services	WSN	-	[36 and 64]	Trust assistant
Key deployment	IoT	-	[67 and 68]	
Key establishment	WSN	-	[69]	
IBE	WSN	-	[70]	
Access control (KP-ABE)	Cloud IoT	Secret key sharing	[72]	Half-trust assistant
Access control (CP-ABE)	IoT	Secret key sharing	[71]	
Access control (ABE)	Cloud based	Part of the message opening	[74]	
Exponentiation based protocols	-	Secret key sharing	[75]	Unreliable assistant
Pairing based protocols	Smart cards	Secret key sharing	[76]	
Key transport	IoT	Secret key sharing	[77]	
Key agreement	IoT	Secret key sharing	[77]	

Received 01/06/2018
Approved 01/07/2018

Table 4: Outward Security Approach

4.3 Compliance or security compatibility

An adaptive approach involves setting or maintaining security measures in a variety of circumstances. This can be considered when internal or environmental parameters affecting the system (which are considered to be unclear after design time) and changes in runtime occur [80]. Since the Internet of Things is a very dynamic environment, adaptive security can be used to reduce energy consumption by implementing security measures. In fact, as it is unchanged, static security is always considered to be the worst thing that wastes network resources.

As stated in [81], compatibility can be done in a parametric or structural way. Initially, adaptation is associated with changes that may occur in security measures and settings (such as the size of the key or the number of operational periods). In contrast, the structural method means changing the security method. For example, depending on the current state of the system, the security protocol can replace the other protocol.

To enforce security, it is necessary to make a sufficient decision about the change in security measures. Otherwise, it can disrupt system security. For example, an adaptive approach, when energy is low, will reduce the level of security (to extend the life of the node). A malicious node can actually exploit this situation, and if the energy is low, it will have the advantage of attacking it. The statistics show that attackers can hack a small part of the system and even access more important parts [82]. We propose that adaptive security solutions be categorized according to considerations into decision making, to be divided into two categories: threat-driven and data-driven. In fact, these two types of elements are in the security: the data that must be secured to them and protect them against those who want to act against them.

4.3.1 Threat-focused

One way to ensure security is to assess threats. If there is no risk, no security measures are required and this will take unnecessary resources. The adaptive-security security approach focuses on assessing threats for the dynamic implementation of security, not systematically and in the worst case scenario. Some of the security-compatible security solutions are calculated below.

Received 01/06/2018
Approved 01/07/2018

In [83], Lee and colleagues propose a trust-based model for implementing routing security in ad-hoc (MANET) mobile networks. Instead of requesting and verifying the certification at each routing stage, it avoids the suggestion that when a trusted node interacts with it.

Chigan and colleagues in [84] propose a framework that is consistent with security in MANET security services. A unique module has been suggested to select a layer-to-layer interactive protocol with the desired security level. At runtime, the self-line modem module calculates the security of packet validity. In [85], Younis and colleagues propose proposing a trust-based compliance approach for security routing data in the WSN. Data between nodes can be encrypted at different levels, proportional to the trust path. The topic is determined by the less trusted node in the path. However, the assessment of trust in these solutions based on classical criteria such as fall rates and collision or collision with media access may not provide good reasons for changing the level of security (for example, increasing packet loss does not mean that The level of encryption will increase. In practice, trusted management systems are designed to be designed with selfish behaviors and internal attacks, not to help with cryptographic actions. In another solution, Helvey and his co-worker [86] put forward this issue and provide an adaptive security model based on trust for the Internet of Things. Instead, it systematically uses data authentication in every step or hop, but its solution allows the node to be validated only when it is necessary, depending on the trust level of the sender of the message. Here, the node's behavior is its capacity to send verified messages. However, as the authors have said, their solution requires recommendations on insecurity.

Hamidi and Abi proposed a game-based Markov-based model for adaptive security in the Internet of Things, with emphasis on e-health programs. To model the mathematical framework, the dynamic context in which the objects work, includes threat and resource models. A set of strategies has been proposed for implementing security to deal with threats and resources. However, the authors do not define how a node determines if another has been compromised. They simulate an epidemic of spreading the virus in the WSNs, which makes them more analytical. The same theory can be proposed for work by Wang and his colleagues.

4.3.2 Data-centered

Another approach to compliance is to evaluate the sensitivity of the data. Data-focused approaches are emphasized on data rather than on the environment to assess threats. Exercising security measures on non-sensitive information consumes energy unnecessarily. The goal has

Received 01/06/2018
Approved 01/07/2018

always been to adapt the security to the sensitivity of the data, not always consistent with its highest level. Some of the data-compatible adaptive approaches to data are presented below.

In [89], authors propose a consistent security model for WSNs. Each application has its own security requirements. When the current energy limitations cannot meet the program's requirements, the degree of security gradually decreases. However, as stated by the authors, the decline in communications security will increase potential attacks for data transmitted over these periods of reduced security.

Todo and his colleagues [90] propose a consistent security approach for the EH-WSN. Each packet is placed at a priority level, indicating the importance of the package and the security requirements that indicate the appropriate security package for that package. There are strategies to maximize the number of priority packets to ensure that the security needs of each package are guaranteed. Reducing security is only done when the energy limits of the system are not guaranteed. However, the authors note the fact that security reduces the potential for attacks.

Contrary to the suggestion in [90], Moro and his colleagues in [91] suggest an alternative adaptation for EH-WSN. Their approach is based on the fact that the receiver starts with the idea that [92] at which the sender's node waits for the receiver's signature before sending the data. A receiver will match its own security of its energy and sends it to senders using a signal. This method allows the sender to select the appropriate receiver based on the packet sensitivity level. However, although this method allows a sender to choose based on the sensitivity of the appropriate packet receiver, it may be exploited by a malicious node. For example, if an unidentified node knows that the node has stopped its security measures, it can use this situation to inject unwanted packages (nodes) over the network through that node.

The proposed approach in [93] introduces a customizable security module for wireless devices. The idea is that the level of security services can be based on the number of years that need to be protected. A plan that offers many years of suitable security parameters is suggested. However, it is assumed that the number of years in which information should be protected is known.

The main difference between threatening and data-centric approaches is a security compliance approach. Emphasis on threat-based approaches to adaptation based on the assessment of environmental threats, and data-centric approaches emphasize data security. This is the main

Received 01/06/2018
Approved 01/07/2018

factor in choosing between two methods. In cases where the program can provide data sensitivity specifications, we may consider a data-centered approach to compliance. Otherwise, we need to be able to assess threats to make enough changes in security. Table 5 provides a summary of adaptive security approaches.

Service / protocol	Network / device	The desired method	Reference	operations
Signature	MANET	Trust Management	[83]	Threat driven
Confidentiality	WSN	Trust Management	[85]	
Authentication	IoT	Trust Management	[86]	
Authentication	IoT	game theory	[87]	
Confidentiality + Authentication	IoT	Markov processing	[88]	
Identity	WSN	Sensitivity data	[89]	Data driven
Confidentiality + Authentication	EH-WSN	Sensitivity data	[90]	
Confidentiality +	EH-WSN	Sensitivity data	[91]	

Received 01/06/2018
Approved 01/07/2018

Authentication				
Confidentiality + Authentication	Wireless devices	Lifetime of data	[93]	

Table 5: Appropriate security approach

Both approaches involve different levels of service. However, note that a threat-centric approach to end-to-end security is more than a data-driven approach. In fact, a threat-centric solution for end-to-end points should also take into account the threat assessment in the communication path. In contrast, in almost non-threatened environments, data-centric approaches can easily result in low-security security.

4.4 Implementation using low power security protocols

Many of the old security protocols and algorithms are designed without regard to resource consumption. The emergence of computational computing increases the need for light security protocols to be processed. This is an efficient field for mathematicians. The goal is to provide efficient security protocols that require less energy. In fact, by implementing (or re-implementing) security solutions based on low-power security protocols, power consumption can be reduced effectively. This section provides an overview of some of the well-known security protocols that are naturally low-end. This includes asymmetric encryption, symmetric encryption, as well as physical layer security protocols that are not based on encryption.

4.4.1 Asymmetric protocols

In public key cryptography, the key pair must be selected so that the private key can be created from the public key, equivalent to solving a difficult but solvable computational problem. For example, the RSA encryption security is based on the integer factoring difficulty (IFP). The security of the El-Gamal cryptography system and its types, such as DSS, is based on the severity of the discrete logarithm problem (DLP). Domain sizes, key parameters, and math operations are fundamental issues affecting the operations of the cryptographic system and security services [25].

Received 01/06/2018
Approved 01/07/2018

Other mathematical problems, whose failure can be the basis for public key cryptography, are proposed. In the following, some asymmetric encryption is provided that can be considered for resource limited devices (summarized in Table 8).

Properties	Computational issues	Year	Scheme
Encryption is faster than decryption Decryption at speed is comparable to RSA	IFP	1979	Rabin
Faster than RSA Small keys and certificates	ECDLP	1985	ECC
Faster encryption and decryption Large size generic parameters	ACT	1978	McEliece
Faster encryption and decryption Great Message Spreadsheet	SVP	1998	NTRU

Table 6: Low-power encryption solutions

4.4.1.1 Robin's scheme

Received 01/06/2018
Approved 01/07/2018

The Rabin scheme [94] is an old algorithm based on integer factorization (IFP). So its security is similar to RSA. The main feature of this algorithm is the computational asymmetry between encryption and decryption. The first stage of operations is much faster than its second stage, which is similar to the RSA using similar parameters. This will make Rabin's design attractive for resource-limited networks that need to be encrypted or verified. Proposals, as [95,96], refer to the Rabin scheme for implementing security solutions for Internet objects of objects using [95] a WSN program using nodes consisting of an Atmel 8mm microcontroller and a spartan - IIE FPGA vs. inactive RFID tags [96].

4.4.1.2 ECC design

Elliptic Curve Cryptography (ECC) is a public key encryption method that can be used for cryptography and digital signatures [97]. This is based on the difficulty of calculating discrete logarithms in the elliptic points of an elliptic curve (this is ECDLP: an elliptic curve-discrete algorithm). The main operations of ECC are the scalar multiplication, which is very heavy in terms of processing. However, the same level of security provided by RSA can be measured by ECC using smaller sizes. This, in turn, affects the performance of basic math operations (faster computing). This also has a positive impact on the amount of data transferred and stored. Table 6 provides a comparison between the key parameters required by RSA and ECC for a similar security level.

Key size in ECC-bit	Key size in RSA-bit	Level of security
160	1024	80
224	2048	112
256	3072	128
384	8192	192
512	15360	256

Table 7: The size of keys

Many works, such as [99,100], indicate that ECC is more suitable for smaller devices than RSA. The evaluation of Lead [99] includes two 8-bit processors (Chipcon CC1010 and Atmel ATmega128), while [100] also utilizes Atmel ATmega128. ECC ensures smaller key guarantees, faster calculations, as well as energy and bandwidth. In addition, several protocols

Received 01/06/2018
Approved 01/07/2018

have been extracted from ECC, such as ECDSA, Diffie-Hellman (ECDH), ECDH, Encryption Integrated Curve Design (ECIES), etc. [98].

4.4.1.2 McEliece design

McEliece is a public key cryptography based on the ACT theory of encryption [101]. Its security is based on correcting error codes and arbitrary linear decoding problems. Encryption involves multiplying plain text with a matrix and then adding a random vector to it. The matrix represents a parameter that is generated by a linear code. The decoder can retrieve the message by considering the ciphertext as the code that receives an error. These operations take McEliece very fast. Research activities such as [102-104] show that McEliece is much faster than the classic encoders as RSA or El-Gamal.

The main form of McEliece is the public key size (matrix). Compared to some cryptans like RSA, McEliece public keys are very expensive to store. In summary, they are presented in Table 7 of [105]. That's why McEliece has little attention to limited networks [25]. However, some solutions, [103,104], propose McEliece implementations for embedded devices, such as FPGAs (Xilinx families). Even if FPGAs are less restricted than other devices, they are part of the Internet of Things.

4.4.1.3 NTRU scheme

NTRU (TR polynomial ring) is a public key encryption used for encryption and digital signatures [106]. This method is based on the shortest vector (SVP) problem. NTRU operations are built on a polynomial ring, which makes it a very fast decoder compared to the RSA, El-Gamal and ECC systems. Many of the assessments like [22, 107-109] show that the NTRU has lower power consumption on different devices, including FPGAs and microcontrollers.

NTRU also requires less memory and less computing than other public key encryption. In fact, NTRU is faster than RSA and ECC. However, NTRU is reasonably priced compared to McEliece, but is also at worst expanding the message for encryption and signature [108]. This can affect the storage and communication capacity.

Various low-power encryption systems provide lightweight security services for processing, based on them (confidentiality, digital signing, authentication, etc.). By using low power cryptography, saving heavy processing costs, energy saving can be done effectively. As shown in Table 8, each cipher has its own advantages (advantages and disadvantages). Selection of a

Received 01/06/2018
Approved 01/07/2018

design can be done depending on the type of program. For example, the Rabin scheme can be effective for applications that require encryption and signature authentication. Objects with fairly modest memory can use McEliece's security services. From the guided work, ECC can be pointed out that ECC has the most use compared to other low-power encryption systems. Many solutions for resource-limited networks are based on ECC-based services (such as ECDSA, ECDH, etc.). This is most likely due to the cost-effective ECC in terms of computing and storage. Limited resource nodes are generally limited in energy and storage capacity.

4.4.2 Symmetric protocols

Although classical symmetric cryptography is lighter in terms of computing as compared to asymmetric cryptography (for example, AES using a 8-bit controller is 100 to 1,000 times faster than ECC), some of the recently developed symmetric protocols , Are more efficient. The emergence of very limited devices has led to the development of symmetrical cryptography. This includes two classes of symmetric protocols: block ciphers and stream ciphers.

Most common protocols use block encryption. Stream cryptography can be easily created by block encryption, while some protocols cannot be designed with stream cryptography [25]. Due to their widespread use, many lightweight encryption blocks are suggested. Examples of these protocols are KATAN [111], KLEIN [112], mCrypton [113], Piccolo [114], PRESENT [115], TWINE [116] and EPCBC [117]. However, block encryption is generally designed to work on a platform (software or hardware). In 2013, the National Security Agency released its code blocks families SIMON and SPECK [118]. The purpose of these protocols is to provide security, lightweight and flexible. They earn a good performance in hardware and software environments. The evaluations presented in the explanatory document [118] use ASIC and 8-bit microcontrollers. They show good results from the two protocols compared to many of the cited passwords in terms of ability, traceability, and so on.

Lightweight ciphers have just received a lot of attention recently. Such protocols are more appropriate for applications in which the length of a plain text is unknown or continues, such as the flow of data in resource-limited networks. The eSTREAM project [119] was a major effort by the Network of Excellence Cryptology to carry out the compilation and compilation of the enclosed text. As a result of this project, a series of new data stream encryption protocols are presented. This protocol includes HC-128 [120], Rabbit [121], Salsa120 [122],

Received 01/06/2018
Approved 01/07/2018

SOSEMANUK [123] - which are effective in running applications - Grain v1 [124], MICKEY2.0 [125] and Trivium [126] which are hardware protocols. Other protocols are discussed in [127].

4.4.3Physical layer security protocols

Physical layer security is another branch of secure communication that acts on the physical layer, without encrypting data at higher levels. Based on the physical nature of the channel, such nodes as the physical channel crash (such as noise and fluctuations caused by the fading of the message during a collision) are used. In this approach, the sender encrypts the messages so that the receiver can capture the information, while it is possible to prevent the commentary being interpreted or manipulated by unauthorized persons [128]. Security approaches in the physical layer are less energy-consuming because they do not require heavy operations and processing as much as the classical encryption performed on higher layers. This makes physical security approaches suitable for resource-limited networks such as the Internet of Things [82 and 129].

Two methods of research on the security of the physical layer have been made: encryption (encoding) in the transmission and secret key key agreement (series). The encoding in the transfer can be done without the need for a secret or confidential key. The first work on sending a message was done by Wiener [130], where loopholes in a channel using a wire display a copy of a message sent to the destination node. It has also been extended to non-decomposable channels [131]. Recently, many efforts have been made to eradicate wireless waves, the existence of several antennas and channels with several users. For example, the effect of fading on confidentiality has been studied in [132,133], the degree of confidentiality in multiple antennas has been investigated in [134,135], while channels with multiple access in [136, 137] has been investigated. Other studies on coding in transmission have been investigated [138].

Physical layer security approaches can also be used to provide an agreement key in existing cryptographic systems. The idea of this method is to use a shared key that connects the nodes to the use of a secret key, as there is a potential for eavesdropping. It is possible that two nodes agree on a secret key on public channels, in [139] this mechanism is shown. The author suggests that even noisy communications can be used to create coupled sequences in two nodes, enabling them to agree on a secret key. A related work close to this method is presented in [140]. Recently, many clandestine secret methods operate on the basis of cross-channel

Received 01/06/2018
Approved 01/07/2018

wireless metrics as a source of random conditions. Such approaches include key generation based on the use of multi-band channel parameters [141], channels where wireless fading occurs [142], the content of Gaussian multi-dimensional wireless channel information [143], etc.

4.5 Compression of Size

As a security service in relation to data, the runtime is proportional to the size of the data. Most data are large and take longer to run. Energy consumption is directly related to this parameter. Size compressions techniques help reduce consumption by reducing the size of data. This can be related to the protocol header or data to be processed in the encryption algorithm.

4.5.1 Header compression

Security protocols are also important for solving communication issues, as well as secure, packet headers. The header size directly affects energy consumption, as it is transmitted by a limited resource node.

Reza [144] and his colleagues refer to the use of IPsec to protect data in 6LoWPAN sensor networks. When IPsec is considered, IPv6 sub-headers must be included in any data processing. Authors' suggestions provide 6LoWPAN specification that allows encryption and compression of IPsec headers. Compression in the 6LoWPAN layer is generally based on the deletion of fields that are implicitly known to all nodes or can be obtained from other layers. This solution allows the packet size to be appropriate for an 802.15.4 frame and thus reduces energy consumption when sending packets due to a small closed package. The header compression can also reduce the number of steps for authentication (when the original message is authenticated, the physical address or MAC is also added to the packet). For example, at least the IPsec header uses 24-byte HMAC-SHA1-96, which can be 16 bytes after optimizing compression.

In another work, Raza et al. [145, 146] suggest a compression solution for waste reduction. Authors refer to the DTLS protocol to protect CoAP in networks that support 802.15.4. Their solution provides specifications for compressing the DTLS header in the 6LoWPAN layer. The evaluation shows that DTLS header compression reduces energy consumption, especially if the use of DTLS involves the partitioning of uncompressed headers.

Received 01/06/2018
Approved 01/07/2018

In [147], Lifoth and colleagues show that decreasing header size can reduce energy consumption. Their proposed security protocol at the link layer for WSNs does this compression by removing the cache field from the header and replacing it with a feedback feed that is simultaneously on each side.

4.5.2 Compression of encrypted text

In addition, some of the effects focus on reducing processing, and consequently reducing the size of encrypted text, mainly for ABE protocols. In [148], Cheng and colleagues provide a method for reducing consumption in the CP-ABE protocol by compressing its features. In fact, the overhead of this protocol happens by adding some attributes that are expressed by users. This proposal will reduce the size by combining a number of expressed attributes with the gateways AND (att1 AND att2 AND att3) into a unit called the "community of attributes". This is done using the correct first number. Any integer greater than 1 can be expressed as a product of the first divisor in a unique way. Thus, the mapping of each of the attributes is mapped to a number of first numbers, and the mapping of the traits is represented as the product of the first numbers.

In [149], Chen and his colleagues faced the same problem and proposed a solution to the CP-ABE. Their solution was to build the AND gateways and to combine attributes. This means that the user-defined properties with the AND gate are aggregated into an attribute.

Other solutions that provide ABE protocols for compressing encrypted text, regardless of its size policies, are presented in [150-152].

4.6 Hybridization

Ultimately, hybridization can be used to combine and utilize various solutions. This issue is about energy saving mechanisms or security protocols. Some of these are listed below.

4.6.1 A combination of mechanisms

Based on the mechanisms mentioned above, they can be combined to reduce consumption. Each of them refers to a particular way to reduce energy consumption. A combination of mechanisms can be considered for solutions in different fields. For example, in [58], authors have explained the possibility of combining their solution (on-line / off-line security in ABE) with what is described in [74] (Outdoor Security in ABE). In fact, the authors' suggestions make it easier to perform encryption with pre-computation. But they do not take a method for decoding operations. On the other hand, the solution in [74] assumes that the encrypted ABE

Received 01/06/2018
Approved 01/07/2018

text may be stored in the cloud and offers an outsourcing method for users to request decryption. A combination of these solutions reduces consumption for encryption and decryption in ABE.

In [153], the authors examine compression of headers and outsourced security to reduce energy consumption in the HIP. This indicates that the hedge in the resource-limited nodes, in addition to the fact that heavier computing is performed for each initiator and respondent. The proposed solution takes into account the two mechanisms of optimization and energy saving.

4.6.2 A combination of protocols

Energy consumption can be reduced by combining protocols. Some protocols save energy, but they cannot match things with the Internet. Other protocols are not compatible with the objects of the Internet, except in terms of energy. Hybrid solutions will be beneficial for protocols to gain more benefits.

In [154], Wicks and colleagues propose a hybrid deployment framework for WSNs. In this solution, the constrained nodes use symmetric cryptography for power, and only gates that use more energy use public key cryptography. This is done by allowing the gateways to verify the finite nodes. This method uses relatively cheap encryption, and when it accesses a gateway, it uses public key cryptography that is heavier in terms of processing, and sometimes even digital signing is possible.

In the framework of AGREE, proposed by Bainchi et al. [62], we mention a solution that allows to reduce CP-ABE costs by combining it with a symmetric protocol such as AES. This method is based on data encryption with symmetric protocol and symmetric key encryption used with CP-ABE. This method is very useful because the symmetric key size is generally smaller than the data size. Additionally, for encryption with the same policy, CP-ABE is performed only once (to encrypt the symmetric key used).

5. MORE DISCUSSION

The proposed classification in this paper shows that there are several ways to reduce energy consumption in security protocols. Many security services are involved in various situations. This section provides an analysis of the considerations and parameters that will affect the use of the energy-saving mechanism.

The application of the energy saving mechanism depends on specific factors. More precisely, two parameters that can affect the application of mechanisms are identified: the deployment

Received 01/06/2018
Approved 01/07/2018

environment in which the energy-saving mechanism is used and the target protocol. Below, efficient energy mechanisms are discussed with respect to these parameters. Discussions focus on the causes of consumption (heavy operations, data size, and number of calls) identified in Section 3.5. Table 11 summarizes this discussion.

Application	Cause of intake			Parameter		
	Number of calls	Data size	Heavy operations	Protocol	Peripheral	
The availability of a measurable piece			X	X		Online security / off-line
There are advantages in mobile and limited resources						
The signature is more than simple encryption						
Service focused						
Need help			x	x	x	Outsourcing of security
Transferable to offline / out-of-line						
Data availability	x		x		x	Adaptive security
Independent of the protocol						
Security in limited resources and availability			x	x		Limited resource security protocols
Reduction of the size of the data		x		x		Compression of Size

Table 8: Application of Saving Mechanisms

Received 01/06/2018
Approved 01/07/2018

Online / offline security reduce energy consumption by spending part of the overall security plan. As based on the use of the pre-calculation technique, the use of this technique does not really depend on the deployment environment. However, some programs can offer more benefits, since the storage space for the Internet nodes of objects is limited. An online incentive program for online / offline is mobile technology. A mobile object can perform offline calculations and store results when connected to an electrical power supply. When the device is separate, calculations are applied on-line using stored results. The same observations can be observed for energy technology. Restricted resources can use energy in periods where external energy is available for pre-calculation, and then use the results. Several developed solutions, for example, [44, 58, and 62] refer to these types of programs (see Table 3). You can always apply this mechanism to other networks using offline phase before deployment.

Online / Outside Security requires several pre-computational operations. The solutions presented in this article provide specifications for the construction of two stages. As outlined in Section 4.1, service-centric approaches are public and are not connected to a data protocol. In contrast, operations-focused solutions focus more on how precompiled heavy operations are, and are only suitable for protocols that can be exploited based on specific operations. For example, [44] aims to target encoder-based protocols [43], which defines algorithms based on the base modular syntax [58] for the ABE protocol. This will depend on online security / off-line (offline) security targeting.

Online / offline security are a heavy energy consumer (with some heavy operations pre-processing and maintenance). This makes the technique not dependent on the particular security service, but it can be used in any protocol that computes computable parts. However, using this mechanism for cryptographic schemes is generally more difficult than signing. In fact, depending on the type of entity being considered, a message is encrypted. Therefore, the receiver is not known, in addition to the fact that the encryption message is not known until the on-line online phase is known. This does not apply to signatures because the node signs all messages using its private key (see table 9).

	Dependent on key	
The node signs with its private key	-	Signature

Received 01/06/2018
Approved 01/07/2018

Encrypts the public key using the public key	+	Cryptography
According to the signatory, the review is done	+	Check
Decrypt with your private key	-	Decrypt

Table 9: The dependence of asymmetric schemes in the key

The online / offline concept was introduced in the 1990s, but its first application for key public cryptography in 2008 (as claimed by authors in [5]).

Online security / offline security for encryption schemes is still possible. Many of the solutions, such as [51-55], are based on a factor correction scheme that uses algebraic relationships to make cryptographic methods consistent with their own view. However, it generally has decoding heavy duty (factor correction by decoding). In addition, the problem of key dependency on encryption schemes can be less restrictive than the time it is known, as suggested in the proposed solution in [62].

Outsourced security is based on heavy-duty operations to more powerful devices. Its use mainly depends on the deployment environment, because it requires the availability of helpful tools that should be used for resource-limited nodes. Some solutions, like [77,155], use heterogeneous objects on the Internet to transfer heavy operations to other powerful devices. Other works like [72.74] use the cloud for outsourcing. While other solutions like [36, 64] are based on access to TPM modules. Note that due to the fact that this mechanism uses nodes or other devices, particular attention should be given to what should be granted and to the type of helping devices (trust, semi-trust or unreliable). This does not help to focus on the security of the nodes, but it takes into account the security of the resource-limited nodes.

As with online / offline applications, outsourced security uses heavier operations as energy consumers (by giving it to the donor) and is not related to a specific service. For example, [36] RSA and XTEA are using trusted assistant [71] CP-ABE with semi-trust assistants [75] interested in power or display protocols using Irregular devices. This makes an outsourcing

Received 01/06/2018
Approved 01/07/2018

solution dependent on the target protocol (the target protocol should be based on the operations determined by the outsourcing solution).

Of the work done, the security of the outsourced and online security / offline security-related communications can be outlined. In fact, both are based on dividing the encryption scheme into two parts and implementing only one part of it by itself. The other part is passed as an assistant to the device for external security or before it is calculated for online / offline security. In this way, an external process can be converted to an online / offline section, and already computes the portion to be allocated to it. However, this part should be pre-calculated so that it can be calculated in the offline phase of the line. One of the applications that can be used to transfer from external sources to online / offline security is mobile or mobile environments. A limited node can lose your device assistant (due to mobility). Therefore, before losing contact with auxiliary devices, a limited node can run offline phase to reduce future consumption.

An online / offline scheme can also be transferred to one of the external sources, and this section has passed the pre-calculation to it. However, as outsourcing techniques with the help of other donor organs, particular attention is paid to the type of donor (trusted, semi-trusted or unreliable) and what needs to be done in order to fail in security. Take up It can also be considered in mobile environments where a node that has online security / off-line (offline) access can access the device assistant. For this purpose, it can be transformed into outsourcing and transferring the pre-calculation part to these devices. Table 10 summarizes the linkages and criteria between these two mechanisms.

Environment	Subject	Formation	Assignment
Assistant departure time	The requirement to more calculation	Pre-Calculation section	Outsourcing online / offline
Time to access the assistant	Assistant does not require security	Compensation to advance calculation	online / offline to outsource

Table 10: Relationship between online / offline security and its outsourcing

Received 01/06/2018
Approved 01/07/2018

Security compatibility (security compliance) is based on security settings based on the field of work. This method is related to applications that may occur in environments where data sensitivity is high on security issues or in an environment where the level of security threats that the security service needs to create against them. In fact, the use of adaptive security is directly related to the deployment environment. This requires the availability of information at run-time, against threats or data sensitivity, so that it sets the security level without compromising security. For example, solutions [83-86] are based on the possibility of assessing nodes' confidence around security enforcement and [89-91] for information intelligence information programs.

On the other hand, adaptive security solutions do not need to know the purpose of the security protocol and its operations to comply. As mentioned in Section 4.3, this information can be done either parametric or structural. Using security-compatibility solutions is not dependent on a particular class of security protocols.

Adaptive security allows you to systematically save the worst case by adopting security measures. This can be done by making changes (parametric or structural) in security protocols or by simply calling the protocol only when necessary. For example, in [90], compatibility can be done by changing the encryption key while in compliance with [87] it is done by applying or not authenticating the service. Therefore, adaptive security can be reduced by targeting heavy processing operations or the number of calls.

Low-power security protocols are an alternative solution for heavy classical cryptography in terms of processing. It provides a base for building energy efficient security services. Therefore, with a specific security solution, energy can be reduced by replacing the heavy protocol with a low power and low power protocol. This requires access to a low-power equivalent protocol. For example, in a solution that needs a negotiated key; ECDH can be used instead of DH. However, a security protocol may not have the same implementation in some low-security security classes. For example, McEliece's encryption system [101] does not allow message signatures (although solutions are later proposed as [156]). Paying attention to low-security security depends on the target protocol.

Low security protocols provide efficient services based on operations that are less heavily processed. This will increase the use of low-power security protocols. For example, the main function of ECC [97] is numerical multiplication using smaller parameters (compared to RSA).

Received 01/06/2018
Approved 01/07/2018

NTRU operations [106] are built on a polynomial ring, which is much faster compared to cryptographic systems such as RSA and El-Gamal, which are based on modular modularity. Physical security protocols do not rely on heavy operations that are present in classical apps.
Execution time and energy consumption are also as important as data, compression techniques and data size reduction is still important while retaining the features of the protocol. The header compression techniques in the security protocols, which consider aspects of communication, determine its importance. These protocols are IPsec, TLS, or DTLS, for example. In addition, other data compression solutions have been reported to reduce processing. These two categories of size compression method are directly related to the destination protocol. The header compression solution, in certain fields, is designed, as in [144-146], for specific protocols, some of which header fields can be compressed (for example, they can be uncovered from other headers). The same observations can be made for solutions that reduce data processing.
Obviously, this technique achieves better energy efficiency by considering the size of the data as a reason for consumption. Solutions, for example, in [144-146] reduce consumption simply by reducing header size, because they are transmitted by resource-limited nodes. In addition, solutions such as [148,149] heavy operations continue to be maintained. However, processing for some large data is reduced by the size expressed by users.
It turns out that many of the efficient mechanisms of energy are independent of the target platform. For example, outsourced security anticipates costly operations due to heavy processing operations to other donors, to help nodes reduce consumption, online security, and off-line (offline). Adaptive security is based on dynamic changes at the security level, while compression of size, aims to reduce the size of the data. These mechanisms are not related to a particular platform, and they can work with various Internet-based objects. In addition, low-security security protocols are designed for resource-limited nodes. Performance evaluations related to these protocols are mainly done by looking at resource constraints.

6. CONCLUSION

The Internet of Things (IoT) has expanded widely in many areas (healthcare, smart grids, transportation, production systems, etc.). Sensitivity related to the subject, attention to the security services on the Internet requires objects. Devices connected to the Internet are objects

Received 01/06/2018
Approved 01/07/2018

that are limited to resources and designed to work for a long time. However, many security measures usually have high energy consumption.

This paper examines mechanisms for energy efficiency in the field of Internet security of objects. Earlier studies are more concerned with studying Internet security solutions that are economically efficient. This article is a step further and addresses the mechanisms that will enable the development of energy security solutions. The classification of energy storage techniques is suggested in the Internet security of objects. Each method has been studied, as well as the related work that it uses. This research shows that any energy saving approach involves changes to the main security protocol, and some new issues may occur.

That is why discussions are under way on the use of energy saving techniques. Discussions have focused on the application of mechanisms and parameters affecting their use, which is still widely used. From this study, it can be concluded that various solutions can be considered to reduce energy consumption in security services. This research also increases the need for comparable assessments in terms of stored energy between different methods and mechanisms. In fact, an effective evaluation should consider comparable environments, such as target operating systems (such as microprocessors, FPGAs, ASICs), similar target protocols, and so on. This can be presented as a new perspective. We believe that such a view may be accepted in the scientific and industrial communities and can help designers of the security protocol to select the appropriate mechanism and how it can be applied.

References

[1] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805, doi: 10.1016/j.comnet.2010.05.010 .

[2] D. Miorandi, S. Sicari, F.D. Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516, doi: 10.1016/j.adhoc.2012.02.016 .

[3] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sen- sor networks in the context of the internet of things, Comput. Electr. Eng. 37 (2) (2011) 147–159 . Modern Trends in Applied Security: Architectures, Imple- mentations and Applications, doi: 10.1016/j.compeleceng.2011.01.009 .

Received 01/06/2018
Approved 01/07/2018

[4] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134, doi: 10.1016/j.jnca.2014.01. 014 .
[5] K.T. Nguyen, M. Laurent, N. Oualha, Survey on secure communication pro- tocols for the internet of things, Ad Hoc Netw. 32 (2015) 17–31 . Inter- net of Things security and privacy: design methods and optimization, doi: 10.1016/j.adhoc.2015.01.006 .
[6] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279 . Towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet, doi: 10.1016/j.comnet.2012.12.018 .
[7] J. Granjal, E. Monteiro, J.S. Silva, Security in the integration of low-power wireless sensor networks with the internet: a survey, Ad Hoc Netw. 24, Part A (2015) 264–287, doi: 10.1016/j.adhoc.2014.08.001 .
[8] J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tut. 17 (3) (2015) 1294–1312, doi: 10.1109/COMST.2015.2388550 .
[9] S. Sicari, A. Rizzardi, L. Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: the road ahead, Comput. Netw. 76 (2015) 146–164, doi: 10. 1016/j.comnet.2014.11.008 . [10] R.H. Weber, Internet of things - new security and privacy challenges, Comput. Law Secur. Rev. 26 (1) (2010) 23–30, doi: 10.1016/j.clsr.20 09.11.0 08 .
[11] C. Karlof, N. Sastry, D. Wagner, Tinysec: a link layer security architecture for wireless sensor networks, in: Proceedings of the 2Nd International Confer- ence on Embedded Networked Sensor Systems, in: SenSys '04, ACM, New York, NY, USA, 2004, pp. 162–175, doi: 10.1145/1031495.1031515 .
[12] Y.W. Law, J. Doumen, P. Hartel, Survey and benchmark of block ciphers for wireless sensor networks, ACM Trans. Sen. Netw. 2 (1) (2006) 65–93, doi: 10. 1145/1138127.1138130 . [13] J. Daemen, V. Rijmen, Aes proposal: Rijndael, 1999.
[14] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126, doi: 10. 1145/359340.359342 .
[15] NIST, Skipjack and kea algorithm specifications version 2.0. nist, 1998.
[16] J. Lopez , Unleashing public-key cryptography in wireless sensor networks, J. Comput. Secur. 14 (5) (2006) 469–482 .

Received 01/06/2018
Approved 01/07/2018

[17] D. Boneh, M. Franklin, Identity-Based Encryption from the Weil Pairing, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 213–229. doi: 10.1007/ 3- 540- 44647- 8 _ 13 .
[18] F. Bergadano, D. Cavagnino, B. Crispo, Individual single source authentication on the mbone, in: 20 0 0 IEEE International Conference on Multimedia and Expo. ICME20 0 0. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No.00TH8532), 1, 2000, pp. 541–544 vol.1, doi: 10.1109/ICME. 20 0 0.869659 .
[19] Z. Benenson , N. Gedicke , O. Raivio , Realizing robust user authentication in sensor networks, Real-World Wireless Sensor Netw. (REALWSN) 14 (2005) 52 .
[20] S. Banerjee, D. Mukhopadhyay, Symmetric key based authenticated querying in wireless sensor networks, in: Proceedings of the First International Confer- ence on Integrated Internet Ad Hoc and Sensor Networks, in: InterSense ’06, ACM, New York, NY, USA, 2006, doi: 10.1145/1142680.1142709 .
[21] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, Spins: security proto- cols for sensor networks, Wirel. Netw. 8 (5) (2002) 521–534, doi: 10.1023/A: 1016598314198 .
[22] G. Gaubatz, J.-P. Kaps, B. Sunar, Public Key Cryptography in Sensor Networks—Revisited, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 2–18. doi: 10. 1007/978- 3- 540- 30496- 8 _ 2 .
[23] A. Sahai, B. Waters, Fuzzy Identity-Based Encryption, Springer Berlin Heidel- berg, Berlin, Heidelberg, pp. 457–473. doi: 10.1007/11426639 _ 27 .
[24] T. ElGamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. doi: 10 –18.10.1007/3- 540- 39568- 7 _ 2 .
[25] A .J. Menezes , S.A . Vanstone , P.C.V. Oorschot , Handbook of Applied Cryptogra- phy, 1st, CRC Press, Inc., Boca Raton, FL, USA, 1996 .
[26] L. Eschenauer, V.D. Gligor, A key-management scheme for distributed sensor networks, in: Proceedings of the 9th ACM Conference on Computer and Com- munications Security, in: CCS ’02, ACM, New York, NY, USA, 2002, pp. 41–47, doi: 10.1145/586110.586117 .
[27] D. Liu, P. Ning, Location-based pairwise key establishments for static sensor networks, in: Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, in: SASN ’03, ACM, New York, NY, USA, 2003, pp. 72–82, doi: 10.1145/986858.986869 .

Received 01/06/2018
Approved 01/07/2018

[28] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: Security and Privacy, 20 03. Proceedings. 20 03 Symposium on, 2003, pp. 197–213, doi: 10.1109/SECPRI.2003.1199337 .

[29] H. Chan, A. Perrig, Pike: peer intermediaries for key establishment in sen- sor networks, in: Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., 1, 2005, pp. 524–535 vol. 1, doi: 10.1109/INFCOM.2005.1497920 .

[30] A. Fanian, M. Berenjkoub, H. Saidi, T.A. Gulliver, A scalable and efficient key establishment protocol for wireless sensor networks, in: 2010 IEEE Globecom Workshops, 2010, pp. 1533–1538, doi: 10.1109/GLOCOMW.2010.5700195 .

[31] F.L.M.N.K.N.J. Arkko, E. Carrara, MIKEY: Multimedia Internet KEYing, IETF RFC 3830, Technical Report, 2004 August.

[32] C. Kaufman, Internet Key Exchange (IKEv2) Protocol, IETF RFC 4306, Technical Report, 2005 December.

[33] P.J.R. Moskowitz , P. Nikander , T. Henderson ,Host Identity Protocol, IETF RFC 5201, Technical Report, 2008 .

[34] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory 22 (6) (1976) 644–654, doi: 10.1109/TIT.1976.1055638 .

[35] R. Watro, D. Kong, S.-f. Cuti, C. Gardiner, C. Lynn, P. Kruus, Tinypk: Securing sensor networks with public key technology, in: Proceedings of the 2Nd ACM Workshop on Security of Ad Hoc and Sensor Networks, in: SASN '04, ACM, New York, NY, USA, 2004, pp. 59–64, doi: 10.1145/1029102.1029113 .

[36] W. Hu, P. Corke, W.C. Shih, L. Overs, secFleck: A Public Key Technology Plat- form for Wireless Sensor Networks, Springer Berlin Heidelberg, Berlin, Hei- delberg, pp. 296–311. doi: 10.1007/978- 3- 642- 00224- 3 _ 19 .

[37] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 47–53. doi: 10.1007/3- 540- 39568- 7 _ 5 .

[38] L.B. Oliveira, M. Scott, J. Lopez, R. Dahab, Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks, in: Net- worked Sensing Systems, 2008. INSS 2008. 5th International Conference on, 2008, pp. 173–180, doi: 10.1109/INSS.2008.4610921 .

Received 01/06/2018
Approved 01/07/2018

[39] V. Manral , Cryptographic Algorithm Implementation Requirements for Encap- sulating Security Payload (ESP) and Authentication Header (AH), IETF RFC 4835, Technical Report, 2007 .

[40] E.R.T. Dierks , The Transport Layer Security (TLS) Protocol Version 1.2, IETF RFC 5246, Technical Report, 2008 .

[41] E. Rescorla, N. Modadugu, Datagram transport layer security version 1.2(2012).

[42] S. Even , O. Goldreich , S. Micali , On-line/off-line digital signatures, J. Cryptol. 9 (1) (1996) 35–67 .

[43] C.P. Schnorr, Efficient Identification and Signatures for Smart Cards, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 6 88–6 89. doi: 10.1007/ 3- 540- 46885- 4 _ 68 .

[44] S. Pelissier, T. Prabhakar, H. Jamadagni, R. VenkateshaPrasad, I. Niemegeers, Providing security in energy harvesting sensor networks, in: Consumer Com- munications and Networking Conference (CCNC), 2011 IEEE, 2011, pp. 452–456, doi: 10.1109/CCNC.2011.5766511 .

[45] C.P. Schnorr, Efficient signature generation by smart cards, J. Cryptol. 4 (3) (1991) 161–174, doi: 10.10 07/BF0 0196725 .

[46] E.F. Brickell, K.S. McCurley, An interactive identification scheme based on dis- crete logarithms and factoring, J. Cryptol. 5 (1) (1992) 29–39, doi: 10.1007/ BF00191319 .

[47] P. de Rooij, On the Security of the Schnorr Scheme using preprocess- ing, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 71–80. doi: 10.1007/ 3- 540- 46416- 6 _ 6 .

[48] P. de Rooij, On schnorr's preprocessing for digital signature schemes, J. Cryp- tol. 10 (1) (1997) 1–16, doi: 10.10 07/s0 0145990 0 016 .

[49] E.F. Brickell, D.M. Gordon, K.S. McCurley, D.B. Wilson, Fast Exponentiation with Precomputation, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 200–207. doi: 10.1007/3- 540- 47555- 9 _ 18 .

[50] P. de Rooij, Efficient Exponentiation Using Precomputation and Vector Ad- dition Chains, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 389–399. doi: 10.10 07/BFb0 053453 .

[51] F. Guo, Y. Mu, Z. Chen, Identity-Based Online/Offline Encryp- tion, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 247–261. doi: 10.1007/978- 3- 540- 85230- 8 _ 22 .

Received 01/06/2018
Approved 01/07/2018

[52] Z. Liu, L. Xu, Z. Chen, Y. Mu, F. Guo, Hierarchical identity-based online/offline encryption, in: Young Computer Scientists, 2008. ICYCS 2008. The 9th Inter- national Conference for, 2008, pp. 2115–2119, doi: 10.1109/ICYCS.2008.290 .
[53] J.K. Liu, J. Zhou, An Efficient Identity-Based Online/Offline Encryption Scheme, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 156–167. doi: 10.1007/ 978- 3- 642- 01957- 9 _ 10 . [54] S.S.M. Chow, J.K. Liu, J. Zhou, Identity-based online/offline key encapsulation and encryption, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, in: ASIACCS '11, ACM, New York, NY, USA, 2011, pp. 52–60, doi: 10.1145/1966913.1966922 .
[55] S.S.D. Selvi, S.S. Vivek, C.P. Rangan, Identity Based Online/Offline Encryption and Signcryption Schemes Revisited, Springer Berlin Heidelberg, Berlin, Hei- delberg, pp. 111–127. doi: 10.1007/978- 3- 642- 24586- 2 _ 11 .
[56] D. Boneh, X. Boyen, Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 223–238. doi: 10.1007/978- 3- 540- 24676- 3 _ 14 .
[57] C. Gentry, Practical Identity-Based Encryption Without Random Oracles, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 445–464. doi: 10.1007/ 11761679 _ 27 .
[58] S. Hohenberger, B. Waters, Online/Offline Attribute-Based Encryption, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 293–310. doi: 10.1007/ 978- 3- 642- 54631- 0 _ 17 .
[59] Y. Rouselakis, B. Waters, Practical constructions and new proof methods for large universe attribute-based encryption, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, in: CCS '13, ACM, New York, NY, USA, 2013, pp. 463–474, doi: 10.1145/2508859.2516672 .
[60] A. Shamir , Y. Tauman , Improved online/offline signature schemes, in: Pro- ceedings of the 21st Annual International Cryptology Conference on Ad- vances in Cryptology, in: CRYPTO '01, Springer-Verlag, London, UK, UK, 2001, pp. 355–367 .
[61] H. Krawczyk , T. Rabin , Chameleon signatures., in: Symposium on Network and Distributed Systems Security (NDSS '00), 2000, pp. 143–154 .
[62] G. Bianchi, A.T. Capossele, C. Petrioli, D. Spenza, Agree: exploiting energy har- vesting to support data-centric access control in {WSNs}, Ad Hoc Netw. 11 (8) (2013) 2625–2636, doi: 10.1016/j.adhoc.2013.03.013 .

Received 01/06/2018
Approved 01/07/2018

[63] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based en- cryption, in: Security and Privacy, 2007. SP ’07. IEEE Symposium on, 2007, pp. 321–334, doi: 10.1109/SP.2007.11 .

[64] W. Hu, H. Tan, P. Corke, W.C. Shih, S. Jha, Toward trusted wireless sensor networks, ACM Trans. Sen. Netw. 7 (1) (2010) 5:1–5:25, doi: 10.1145/1806895. 1806900 .

[65] R.M. Needham , D.J. Wheeler , Tea extensions, Report, Cambridge University, Cambridge, UK, 1997 .

[66] T.C. Group , Trusted Platform Module Specification, Technical Report, 2014 .

[67] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, A dtls based end-to-end security architecture for the internet of things with two-way authentication, in: Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on, 2012, pp. 956–963, doi: 10.1109/LCNW.2012.6424088 .

[68] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, G. Carle, {DTLS} based security and two-way authentication for the internet of things, Ad Hoc Netw. 11 (8) (2013) 2710–2723, doi: 10.1016/j.adhoc.2013.05.003 .

[69] M. Barbareschi, E. Battista, A. Mazzeo, S. Venkatesan, Advancing wsn physical security adopting tpm-based architectures, in: Information Reuse and Inte- gration (IRI), 2014 IEEE 15th International Conference on, 2014, pp. 394–399, doi: 10.1109/IRI.2014.7051916 .

[70] Y.M. Yussoff, H. Hashim, M.D. Baba, Identity-based trusted authentication in wireless sensor network, arXiv preprint arXiv:1207.6185 (2012).

[71] L. Touati, Y. Challal, A. Bouabdallah, C-cp-abe: Cooperative ciphertext policy attribute-based encryption for the internet of things, in: Advanced Network- ing Distributed Systems and Applications (INDS), 2014 International Confer- ence on, 2014, pp. 64–69, doi: 10.1109/INDS.2014.19 .

[72] L. Touati , Y. Challal , Collaborative kp-abe for cloud-based internet of things applications, in: Communications (ICC), 2016 IEEE International Conference on, 2016 .

[73] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine- grained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, in: CCS ’06, ACM, New York, NY, USA, 2006, pp. 89–98, doi: 10.1145/1180405.1180418 .

Received 01/06/2018
Approved 01/07/2018

[74] M. Green , S. Hohenberger , B. Waters , Outsourcing the decryption of abe ci- phertexts, in: Proceedings of the 20th USENIX Conference on Security, in: SEC'11, USENIX Association, Berkeley, CA, USA, 2011 . 34–34

[75] S. Hohenberger, A. Lysyanskaya, How to securely outsource cryptographic computations, in: Proceedings of the Second International Conference on The- ory of Cryptography, in: TCC'05, Springer-Verlag, Berlin, Heidelberg, 2005, pp. 264–282, doi: 10.1007/978- 3- 540- 30576- 7 _ 15 .

[76] B. Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, M. Scott, Secure Delegation of Elliptic-Curve Pairing, Springer Berlin Heidelberg, Berlin, Hei- delberg, pp. 24–35. doi: 10.1007/978- 3- 642- 12510- 2 _ 3 .

[77] Y.B. Saied, A. Olivereau, D. Zeghlache, M. Laurent, Lightweight collaborative key establishment scheme for the internet of things, Comput. Netw. 64 (2014) 273–295, doi: 10.1016/j.comnet.2014.02.001 .

[78] M. Watson , Basic Forward Error Correction (FEC) Schemes, RFC 5445, Techni- cal Report, 2009 .

[79] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613, doi: 10.1145/359168.359176 .

[80] E. Yuan, N. Esfahani, S. Malek, A systematic survey of self-protecting software systems, ACM Trans. Auton. Adapt. Syst. 8 (4) (2014) 17:1–17:41, doi: 10.1145/ 2555611 .

[81] C.T. Hager , Context Aware and Adaptive Security for Wireless Networks, Vir- ginia Polytechnic Institute and State University, 2004 Ph.D. thesis .

[82] W. Trappe, R. Howard, R.S. Moore, Low-energy security: limits and oppor- tunities in the internet of things, IEEE Secur. Privacy 13 (1) (2015) 14–21, doi: 10.1109/MSP.2015.7 .

[83] X. Li, M.R. Lyu, J. Liu, A trust model based routing protocol for secure ad hoc networks, in: Aerospace Conference, 2004. Proceedings. 2004 IEEE, Vol. 2, 2004, pp. 1286–1295, doi: 10.1109/AERO.2004.1367726 .

[84] C. Chigan , L. Li , Y. Ye , Resource-aware self-adaptive security provisioning in mobile ad hoc networks, in: Wireless Communications and Networking Con- ference, 2005 IEEE, 4, IEEE, 2005, pp. 2118–2124 .

Received 01/06/2018
Approved 01/07/2018

[85] M. Younis, N. Krajewski, O. Farrag, Adaptive security provision for increased energy efficiency in wireless sensor networks, in: 2009 IEEE 34th Confer- ence on Local Computer Networks, 2009, pp. 999–1005, doi: 10.1109/LCN. 2009.5355022 .
[86] H. Hellaoui, A. Bouabdallah, M. Koudil, Tas-iot: trust-based adaptive security in the iot, in: 2016 IEEE 41st Conference on Local Computer Networks (LCN), 2016, pp. 599–602, doi: 10.1109/LCN.2016.101 .
[87] M. Hamdi, H. Abie, Game-based adaptive security in the internet of things for ehealth, in: Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 920–925, doi: 10.1109/ICC.2014.6883437 .
[88] E.K. Wang, T.-Y. Wu, C.-M. Chen, Y. Ye, Z. Zhang, F. Zou, MDPAS: Markov Decision Process Based Adaptive Security for Sensors in Internet of Things, Springer International Publishing, Cham, pp. 389–397. doi: 10.1007/ 978- 3- 319- 12286- 1 _ 40 .
[89] A.V. Taddeo, L. Micconi, A. Ferrante, Gradual adaptation of security for sen- sor networks, in: World of Wireless Mobile and Multimedia Networks (WoW- MoM), 2010 IEEE International Symposium on a, 2010, pp. 1–9, doi: 10.1109/ WOWMOM.2010.5534903 .
[90] A . Taddeo , M. Mura , A . Ferrante , Qos and security in energy-harvesting wire- less sensor networks, in: Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on, 2010, pp. 1–10 .
[91] A.D. Mauro, X. Fafoutis, N. Dragoni, Adaptive security in odmac for multihop energy harvesting wireless sensor networks, Int. J. Distrib. Sen. Netw. 2015 (2015) 6 8:6 8–6 8:6 8, doi: 10.1155/2015/760302 .
[92] E.Y.A. Lin, J.M. Rabaey, A. Wolisz, Power-efficient rendez-vous schemes for dense wireless sensor networks, in: Communications, 2004 IEEE International Conference on, Vol. 7, 2004, pp. 3769–3776, doi: 10.1109/ICC.2004.1313259 .
[93] P. Keeratiwintakorn, P. Krishnamurthy, Energy efficient security services for limited wireless devices, in: 2006 1st International Symposium on Wireless Pervasive Computing, 2006, pp. 1–6, doi: 10.1109/ISWPC.2006.1613636 .
[94] M.O. Rabin , Digitalized Signatures and Public-Key Functions as Intractable as Factorization, Technical Report, 1979 .

Received 01/06/2018
Approved 01/07/2018

[95] G. Murphy , A. Keeshan , R. Agarwal , E. Popovici , Hardware - software imple- mentation of public-key cryptography for wireless sensor networks, in: 2006 IET Irish Signals and Systems Conference, 2006, pp. 463–468 .
[96] Y. Oren, M. Feldhofer, A low-resource public-key identification scheme for rfid tags and sensor nodes, in: Proceedings of the Second ACM Conference on Wireless Network Security, in: WiSec ’09, ACM, New York, NY, USA, 2009, pp. 59–68, doi: 10.1145/1514274.1514283 .
[97] N. Koblitz , Elliptic curve cryptosystems, Math. Comput. 48 (177) (1987) 203–209 .
[98] D. Hankerson , A.J. Menezes , S. Vanstone , Guide to Elliptic Curve Cryptography, Springer Science & Business Media, 2004 .
[99] N. Gura, A. Patel, A. Wander, H. Eberle, S.C. Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, Springer Berlin Heidelberg, Berlin, Hei- delberg, pp. 119–132. doi: 10.1007/978- 3- 540- 28632- 5 _ 9 .
[100] A.S. Wander, N. Gura, H. Eberle, V. Gupta, S.C. Shantz, Energy analysis of public-key cryptography for wireless sensor networks, in: Third IEEE In- ternational Conference on Pervasive Computing and Communications, 2005, pp. 324–328, doi: 10.1109/PERCOM.2005.18 . [101] R. McEliece, A public-key cryptosystem based on algebraic(1978).
[102] P. Loidreau, Strengthening McEliece Cryptosystem, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 585–598. doi: 10.1007/3- 540- 4 4 4 48-3 _ 45 .
[103] T. Eisenbarth, T. Güneysu, S. Heyse, C. Paar, MicroEliece: McEliece for Em- bedded Devices, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 49–64. doi: 10.1007/978- 3- 642- 04138- 9 _ 4 .
[104] S. Heyse, I. von Maurich, T. Güneysu, Smaller Keys for Code-Based Cryptography: QC-MDPC McEliece Implementations on Embedded Devices, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 273–292. doi: 10.1007/ 978- 3- 642- 40349- 1 _ 16 .
[105] D.J. Bernstein, T. Lange, C. Peters, Attacking and Defending the McEliece Cryp- tosystem, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 31–46. doi: 10. 1007/978- 3- 540- 88403- 3 _ 3 .
[106] J. Hoffstein, J. Pipher, J.H. Silverman, NTRU: A Ring-Based Public Key Cryp- tosystem, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 267–288. doi: 10. 10 07/BFb0 054 86 8 .

Received 01/06/2018
Approved 01/07/2018

[107] D.V. Bailey, D. Coffin, A. Elbirt, J.H. Silverman, A.D. Woodbury, NTRU in Con- strained Devices, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 262–272. doi: 10.1007/3- 540- 44709- 1 _ 22 .

[108] G. Gaubatz, J.P. Kaps, E. Ozturk, B. Sunar, State of the art in ultra-low power public key cryptography for wireless sensor networks, in: Third IEEE Interna- tional Conference on Pervasive Computing and Communications Workshops, 2005, pp. 146–150, doi: 10.1109/PERCOMW.2005.76 .

[109] B. Biswas, N. Sendrier, McEliece Cryptosystem Implementation: Theory and Practice, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 47–62. doi: 10. 1007/978- 3- 540- 88403- 3 _ 4 .

[110] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, L. Uhsadel, A survey of lightweight- cryptography implementations, IEEE Design Test Comput. 24 (6) (2007) 522–533, doi: 10.1109/MDT.2007.178 .

[111] C. De Cannière, O. Dunkelman, M. Kneževi ´c, KATAN and KTANTAN —A Family of Small and Efficient Hardware-Oriented Block Ciphers, Springer Berlin Hei- delberg, Berlin, Heidelberg, pp. 272–288. doi: 10.1007/978- 3- 642- 04138- 9 _ 20 .

[112] Z. Gong, S. Nikova, Y.W. Law, KLEIN: A New Family of Lightweight Block Ci- phers, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 1–18. doi: 10.1007/ 978- 3- 642- 25286- 0 _ 1

[113] C.H. Lim, T. Korkishko, mCrypton –A Lightweight Block Cipher for Security of Low-Cost RFID Tags and Sensors, Springer Berlin Heidelberg, Berlin, Heidel- berg, pp. 243–258. doi: 10.1007/11604938 _ 19 .

[114] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, T. Shirai, Piccolo: An Ultra-Lightweight Blockcipher, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 342–357. doi: 10.1007/978- 3- 642- 23951- 9 _ 23 .

[115] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Rob- shaw, Y. Seurin, C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 450–466. doi: 10.1007/ 978- 3- 540- 74735- 2 _ 31 .

[116] T. Suzaki, K. Minematsu, S. Morioka, E. Kobayashi, TWINE: A Lightweight Block Cipher for Multiple Platforms, Springer Berlin Heidelberg, Berlin, Hei- delberg, pp. 339–354. doi: 10.1007/978- 3- 642- 35999- 6 _ 22 .

Received 01/06/2018
Approved 01/07/2018

[117] H. Yap, K. Khoo, A. Poschmann, M. Henricksen, EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 76–97. doi: 10.1007/978- 3- 642- 25513- 7 _ 7 .

[118] R. Beaulieu , D. Shors , J. Smith , S. Treatman-Clark , B. Weeks , L. Wingers , The simon and speck families of lightweight block ciphers. cryptology eprint archive, 2013 .

[119] M. Tahmassebpour, Performance Evaluation and Scalability of IP-based and Heuristic-based Job Scheduling Algorithm Backup Systems. Indian Journal of Science and Technology, Vol. 9 (26), 2016, doi: 10.17485/ijst/2016/v9i26/97260.

[120] H. Wu, The Stream Cipher HC-128, Springer Berlin Heidelberg, Berlin, Heidel- berg, pp. 39–47. doi: 10.1007/978- 3- 540- 68351- 3 _ 4 .

[121] M. Boesgaard, M. Vesterager, E. Zenner, The Rabbit Stream Cipher, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 69–83. doi: 10.1007/ 978- 3- 540- 68351- 3 _ 7 .

[122] D.J. Bernstein, The Salsa20 Family of Stream Ciphers, Springer Berlin Heidel- berg, Berlin, Heidelberg, pp. 84–97. doi: 10.1007/978- 3- 540- 68351- 3 _ 8 .

[123] C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, H. Sibert, Sosemanuk, a Fast Software-Oriented Stream Cipher, Springer Berlin Heidelberg, Berlin, Heidel- berg, pp. 98–118. doi: 10.1007/978- 3- 540- 68351- 3 _ 9 .

[124] M. Hell , T. Johansson , W. Meier , Grain: a stream cipher for constrained envi- ronments, Int. J. Wireless Mobile Comput. 2 (1) (2007) 86–93 .

[125] S. Babbage, M. Dodd, The MICKEY Stream Ciphers, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 191–209. doi: 10.1007/978- 3- 540- 68351- 3 _ 15 .

[126] C. De Canniere , B. Preneel , Trivium specifications, eSTREAM, ECRYPT stream Cipher Project, Citeseer, 2005 .

[127] C. Manifavas , G. Hatzivasilis , K. Fysarakis , Y. Papaefstathiou , A survey of lightweight stream ciphers for embedded systems, Secur. Commun. Netw. 9 (10) (2016) 1226–1246 .

[128] M. Tahmassebpour, A.M. Otaghvari, Increase Efficiency Big Data in Intelligent Transportation System with Using IoT Integration Cloud. Journal of Fundamental and Applied Sciences, Vol. 8 (3S), 2016, pp. 2443-2461.

Received 01/06/2018
Approved 01/07/2018

[129] A. Mukherjee, Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints, Proc. IEEE 103 (10) (2015) 1747–1761, doi: 10.1109/JPROC.2015.2466548 .
[130] A.D. Wyner, The wire-tap channel, Bell Syst. Tech. J. 54 (8) (1975) 1355–1387, doi: 10.1002/j.1538-7305.1975.tb02040.x .
[131] I. Csiszar, J. Korner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory 24 (3) (1978) 339–348, doi: 10.1109/TIT.1978.1055892 .
[132] Y. Liang, H.V. Poor, S. Shamai, Secure communication over fading channels, IEEE Trans. Inf. Theory 54 (6) (2008) 2470–2492, doi: 10.1109/TIT.2008.921678 .
[133] P.K. Gopala, L. Lai, H.E. Gamal, On the secrecy capacity of fading chan- nels, IEEE Trans. Inf. Theory 54 (10) (2008) 4687–4698, doi: 10.1109/TIT.2008. 928990 .
[134] A. Khisti, G.W. Wornell, Secure transmission with multiple antennas i: the misome wiretap channel, IEEE Trans. Inf. Theory 56 (7) (2010) 3088–3104, doi: 10.1109/TIT.2010.2048445 .
[135] F. Oggier, B. Hassibi, The secrecy capacity of the mimo wiretap channel, IEEE Trans. Inf. Theory 57 (8) (2011) 4 961–4 972, doi: 10.1109/TIT.2011.2158487 .
[136] Y. Liang, H.V. Poor, Multiple-access channels with confidential messages, IEEE Trans. Inf. Theory 54 (3) (2008) 976–1002, doi: 10.1109/TIT.2007.915978 .
[137] E. Tekin, A. Yener, The gaussian multiple access wire-tap channel, IEEE Trans. Inf. Theory 54 (12) (2008) 5747–5755, doi: 10.1109/TIT.2008.2006422 .
[138] Y. Liang, H.V. Poor, S. Shamai (Shitz), Information theoretic security, Found. Trends Commun. Inf. Theory 5 (4–5) (2009) 355–580, doi: 10.1561/ 010 0 0 0 0 036 .
[139] U.M. Maurer, Secret key agreement by public discussion from common infor- mation, IEEE Trans. Inf. Theory 39 (3) (1993) 733–742, doi: 10.1109/18.256484 .
[140] R. Ahlswede, I. Csiszar, Common randomness in information theory and cryp- tography. i. secret sharing, IEEE Trans. Inf. Theory 39 (4) (1993) 1121–1132, doi: 10.1109/18.243431 .
[141] Y. Shen, M.Z. Win, Intrinsic information of wideband channels, IEEE J. Sel. Areas Commun. 31 (9) (2013) 1875–1888, doi: 10.1109/JSAC.2013.130919 .
[142] L. Lai, Y. Liang, H.V. Poor, A unified framework for key agreement over wire- less fading channels, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 4 80–4 90, doi: 10.1109/TIFS.2011.2180527 .

Received 01/06/2018
Approved 01/07/2018

[143] G. Pasolini, D. Dardari, Secret information of wireless multi-dimensional gaussian channels, IEEE Trans. Wireless Commun. 14 (6) (2015) 3429–3442, doi: 10.1109/TWC.2015.2406320
[144] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing com- munication in 6lowpan with compressed ipsec, in: 2011 International Confer- ence on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1–8, doi: 10.1109/DCOSS.2011.5982177 .
[145] S. Raza, D. Trabalza, T. Voigt, 6lowpan compressed dtls for coap, in: 2012 IEEE 8th International Conference on Distributed Computing in Sensor Sys- tems, 2012, pp. 287–289, doi: 10.1109/DCOSS.2012.55 .
[146] S. Raza, H. Shafagh, K. Hewage, R. Hummen, T. Voigt, Lithe: lightweight secure coap for the internet of things, IEEE Sens. J. 13 (10) (2013) 3711–3720, doi: 10. 1109/JSEN.2013.2277656 . [147] L.E. Lighfoot, J. Ren, T. Li, An energy efficient link-layer security protocol for wireless sensor networks, in: 2007 IEEE International Conference on Elec- tro/Information Technology, 2007, pp. 233–238, doi: 10.1109/EIT.2007.4374458 .
[148] Y. Cheng, J. Ren, Z. Wang, S. Mei, J. Zhou, Attributes union in cp-abe algorithm for large universe cryptographic access control, in: 2012 Second International Conference on Cloud and Green Computing, 2012, pp. 180–186, doi: 10.1109/ CGC.2012.13 .
[149] C. Chen, Z. Zhang, D. Feng, Efficient Ciphertext Policy Attribute-Based Encryption with Constant-Size Ciphertext and Constant Computation-Cost, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 84–101. doi: 10.1007/ 978- 3- 642- 24316- 5 _ 8 .
[150] J. Herranz, F. Laguillaumie, C. Ràfols, Constant Size Ciphertexts in Threshold Attribute-Based Encryption, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 19–34. doi: 10.1007/978- 3- 642- 13013-7 _ 2 .
[151] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, C. Ráfols, Attribute-based encryption schemes with constant-size ciphertexts, Theor. Comput. Sci. 422 (2012) 15–38, doi: 10.1016/j.tcs.2011.12.004 .
[152] C. Wang , J. Luo ,An efficient key-policy attribute-based encryption scheme with constant ciphertext length, Math. Probl. Eng. 2013 (2013) .
[153] S. Sahraoui, A. Bilami, Efficient hip-based approach to ensure lightweight end- to-end security in the internet of things, Comput. Netw. 91 (2015) 26–45, doi: 10.1016/j.comnet.2015.08.002 .[154] J. Mache, C.Y. Wan, M. Yarvis, Exploiting heterogeneity for sensor network security,

Received 01/06/2018
Approved 01/07/2018

in: 2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2008, pp. 591–593, doi: 10.1109/SAHCN.2008.80 .
[155] Y. Saied, A. Olivereau, D-hip: a distributed key exchange scheme for hip-based internet of things, in: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a, 2012, pp. 1–7, doi: 10. 1109/WoWMoM.2012.6263785 .
[156] N.T. Courtois, M. Finiasz, N. Sendrier, How to Achieve a McEliece-Based Digital Signature Scheme, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 157–174. doi: 10.1007/3- 540-45682- 1 _ 10 .
[157] Sandoval. E. M. L. (2017). Capital intelectual en la competitividad de las MIPYMES en Tacna-Peru. Opcion, vol. 33, No. 84 (2017): 504-535
[158] Paniagua. W. G. C. & Gago. D. O. (2017). Estudio de estrategias cognitivas, metacognitivas y socioemocionales: Su efecto en estudiantes. Opcion, vol. 33, No. 84 (2017): 557-576

Received 01/06/2018
Approved 01/07/2018