Hellaoui, Hamed; Koudil, Mouloud; Bouabdallah, Abdelmadjid

Energy Efficiency in Security of 5G-Based IoT: An End-to-End Adaptive Approach

Published in:
IEEE Internet of Things Journal

DOI:
10.1109/JIOT.2020.2974618

Published: 01/07/2020

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Hellaoui, H., Koudil, M., & Bouabdallah, A. (2020). Energy Efficiency in Security of 5G-Based IoT: An End-to-End Adaptive Approach. *IEEE Internet of Things Journal*, *7*(7), 6589-6602. Article 9001075. https://doi.org/10.1109/JIOT.2020.2974618

Energy-efficiency in security of 5G-based IoT: An end-to-end adaptive approach

Hamed Hellaoui, Mouloud Koudil and Abdelmadjid Bouabdallah

***Abstract*—The challenging problem of energy-efficiency in security of the Internet of Things (IoT) is tackled in this paper. The authors consider the upcoming generation of mobile networks, 5G, as a communication architecture for the IoT. The concept of adaptive security is adopted which is based on adjusting the security level as per the changing context. It has the potential of reducing energy consumption by adapting security rather than always considering the worst case, which is energy-consuming. The consideration of 5G introduces new dynamics that can be exploited to perform more adaptation. The proposed solution introduces an intelligence in the application of security, from the establishment phase to the use phase (end-to-end). The security level related to the used cryptographic algorithm/key is adapted for each node during the establishment phase, so to match with the duration of the provided services. A new strategy is formulated that considers both IoT and 5G characteristics. In addition, a solution based on the framework of coalitional game is proposed in order to associate the deployed objects with the optimized security levels. Moreover, the application of security is also adapted during the use phase according to the threat level. Trust management is used to evaluate the threat level among the network nodes. While existing works focus on performing the adaptation during the use phase, the proposed approach achieves more adaptation through the consideration of both IoT and 5G dynamics. Analysis and performance evaluations are conducted to show the effectiveness of the proposed end-to-end approach.**

***Index Terms*—Internet of Things (IoT), 5G, Adaptive security, Energy-efficiency, Game theory, Trust management.**

I. Introduction

Considered as one of the most technology affecting our life, the Internet of Things (IoT) is gaining much attention [2]. Analysts at 'Business Insider' estimate that 34 billion devices will be connected by 2020 [3]. Meeting the demands of IoT applications will require relying on an efficient architecture for communication. In this context, the 5^{th} generation of mobile networks, 5G, will be the communication standard to support diverse and densely connectable devices [4]. As the IoT growth will continue over the next years, the consideration of 5G as communication architecture for the IoT is the current trend. This combination, which is increasingly being approached as the Internet of Everything (IoE) [5], is giving rise to new type of services that meet user expectations. Despite all those potentials, a large-scale acceptance of such technology depends on its robustness and security.

Security services are typically provided by applying schemes such as encryption/decryption and signature/verification. These schemes are generally designed to maintain a high level of security against attacks, and are known to be resource-intensive. In the other hand, when considering the IoT, many connected devices are resource-constrained. Objects, such as sensors and RFID tags, can be limited in terms of energy, memory, computation, and storage. In addition, as such devices can be battery-powered and expected to operate for a long time, energy consumption is very critical for the IoT. Heavy security could lower the lifetime of IoT services and deviate the objects from their main tasks. Therefore, security services must be adapted to meet the energy-constrained nature of the IoT, while considering the 5G architecture.

Energy-efficiency has always been a challenging problem in security [6]. In this context, adaptive security is considered as a key method allowing to reduce energy overhead of security in resource-constrained networks. It consists in adapting security levels depending the context. Indeed, static security must always consider the highest level, which generally consumes energy. Thus, adaptive security aims at associating to each situation its required level of security. This is justified by the dynamics that affect the reasons for security. Several approaches are proposed in the literature [7]–[14]. However, the consideration of 5G as a communication architecture for the IoT introduces new dynamics that can be exploited to reduce energy overhead of security. As 5G is becoming the main communication standard for the IoT, such consideration would be vital for reducing energy consumption in IoT security.

Existing adaptive security approaches do not take into account the new trend of 5G. While they focus on performing the adaptation during the use of the security service, 5G-based architecture would allow performing it before. This paper proposes an end-to-end adaptive security approach for 5G architecture-based IoT. The adaptation is first performed at the security establishment phase, where the security level is assigned according to the duration of the service. The adaptation is then performed at the use phase by the IoT nodes, depending on the treat level. This end-to-end adaptation would significantly contribute in saving the energy of the objects while performing security services. Major contributions of the paper are the following:

A preliminary version of this work has been published at the IEEE Conference on Local Computer Networks (LCN) 2016 [1].

H. Hellaoui is with the Department of Communications and Networking, School of Electrical Engineering, Aalto University, FI-00076 Aalto, Finland, also with Ecole nationale Supérieure d'Informatique (ESI), LMCS Laboratory, BP 68 M 16309 Oued Smar, El Harrach, Algiers, Algeria (e-mail: hamed.hellaoui@aalto.fi).

M. Koudil is with Ecole nationale Supérieure d'Informatique (ESI), LMCS Laboratory, BP 68 M 16309 Oued Smar, El Harrach, Algiers, Algeria (e-mail: m_koudil@esi.dz).

A. Bouabdallah is with Sorbonne Universités, Université de Technologie de Compiègne UTC, CNRS, Heudiasyc UMR 7253 CS 60 319, 60 203 Compiègne cedex, France (e-mail: abdelmadjid.bouabdallah@hds.utc.fr).

- The authors advance the concept of end-to-end adaptive security, which allows performing security adaptation during the establishment phase and the use phase. This concept is motivated by considering the dynamics of IoT and 5G.
- A strategy is introduced to formulate the security level required for each node at the security establishment phase. Moreover, a coalitional game solution is proposed to associate objects with the optimized security levels. A player transfer function is defined and the stability of the game is proved.
- A trust management model is proposed to evaluate threats and adapt security during the use phase. The model accounts for direct interactions, observations and also recommendations. Moreover, the model advances the principle of relevance of the trust to deal with the dynamic of the trust value and the principle of the future nearest experiences/observations to cope with the credibility of the recommendations.
- The authors provide analysis and performance evaluations of the proposed solution. The results reveal that considering different security levels can lead to enhanced energy-saving only when it is associated with an optimized solution and prove the effectiveness of the coalitional game proposition. Moreover, the authors provide an implementation of the proposed trust management scheme on the top IoT communication standards and discuss the obtained results.

The rest of this paper is organized in the following fashion. A background on adaptive security approaches is provided in Section II. Section III discusses the dynamic nature in IoT based on 5G architecture. The basic idea behind end-to-end adaptive security and the considered system model are presented in Section IV. The two proposed security adaptation solutions at the establishment phase and at the use phase are respectively introduced in Section V and Section VI. Performance evaluations are provided in Section VII. Finally, section VIII draws conclusions of this work.

II. Background on adaptive security approaches

Adaptive security provides an efficient means to reduce energy consumption. As it is based on adjusting the security level depending on the context, the main issue is to determine the required level without compromising security. Different approaches are proposed in the literature. These solutions can be classified in two categories: threat-centered and data-centered (Fig. 1) [6].

A. Threat-centered adaptive security

Threat-centered adaptive security approaches rely on evaluating threats in order to dynamically adapt security. Rather than systematically considering the highest level, security is adapted according to the threat level. For instance, Hamdi and Abie propose in [7] a Markov game-based adaptive solution for the IoT. They provide a mathematical framework that models the dynamic context (including threats and resources) and enables adapting security.

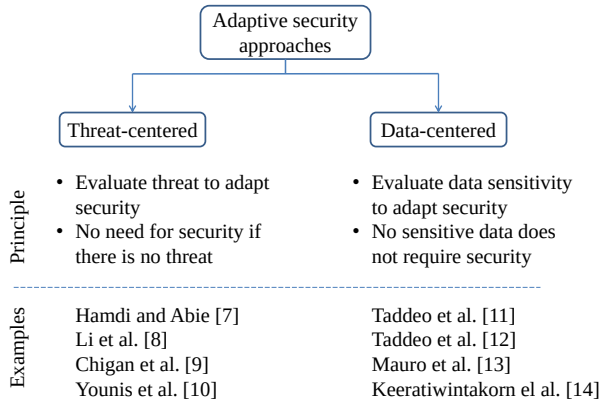

Fig. 1: Adaptive security classes.

Other solutions are based on trust management to evaluate threats in the surrounding. In [8] Li et al. propose a trust-based model that adapts routing security in Mobile Ad-hoc Networks (MANETs). It reduces verifying certificates at every routing step when a node trusts the one it interacts with. The framework proposed in [9] allows adapting security services in MANETs. It provides a self-adaptation module to adapt the security depending on the trust evaluation of the surrounding. Younis et al. tackle in [10] data routing security in Wireless Sensor Networks (WSNs). The proposed model allows to adapt encrypting level of the data being transmitted according to the trust of the path. This trust is determined by the least trusted node in the path. In our paper, we advance the existing works on trust management for adaptive security by considering the inherent dynamics characterizing the IoT. Moreover, we also deal with the issues of the relevance of the trust and the credibility of the recommendations which are not tackled in the previous works.

B. Data-centered adaptive security

Unlike the first category, data-centered approaches focus on the data to secure to take adaptation decisions. The goal is to adapt security according to data sensitivity rather than always considering the highest level. In [11], Taddeo et al. propose an adaptive solution for WSNs. Each application is associated to security requirements. When the current energy constraints cannot satisfy application requirements, the security is gradually decreased. In another work, Taddeo et al. [12] propose an adaptive model for Energy-Harvesting Wireless Sensor Networks (EH-WSNs). Each packet has a security suit that represents the supported measures. Security lowering is performed only when the system energy constraints cannot be satisfied. However, as raised by the authors, lowering the security of the communication increases the potential of attacks for data that are transmitted in these periods.

In [13], Mauro et al. propose an adaptive security approach for EH-WSNs. Depending on its energy level, a node can dynamically adapt its security mode and inform its neighbors about the current mode. A sender can choose its next hop based on packet's criticality.

The approach proposed in [14] introduces an adaptive model for wireless devices. It allows to adjust the strength of security

services according to the number of years information need to be protected. This is based on the assumption that the number of years during which information need to be protected is known.

C. Discussion

The two adaptive approaches are distinguished based on the consideration used to take adaptation decisions. While threat-centered security focus on evaluating threats in the surrounding (no need for security if there is no threat), data-centered approaches are interested in the data to secure (if the data are not sensitive, no need for security). We can note that these approaches perform adaptation during the use of the security service. While the security service is being in use, it will be adapted depending the threat level or the data sensitivity. However, the authors argue that adaptation can be considered even before the use of the security services. The emergence of 5G along with the different applications of the IoT introduce novel architecture with new dynamics. Efficient consideration of these dynamics would allow more adaptation of security, which will result in better energy saving for objects and longer duration of their services.

III. Dynamic nature in 5G-based IoT

With the huge expansion the Internet of Things is knowing, the forthcoming generation of mobile networks, 5G, is becoming the standard to be used for communication. This gives rise to new dynamics that come from these two networks. Indeed, the IoT is a very dynamic environment by nature. Some objects might join the network for a long time, while others may stay for a while then leave. This is the case for group communication which reflects many collaboration aspects in the IoT [15]. In such scenarios, a node joins the communication of a group with the purpose of providing or consuming services. Once its goals are achieved, the node will no longer be interested in the communication and leave the group (e.g., video on demand, multi-cast media streaming, etc.). This represents a dynamic in terms of the participation of the node in the communication. In addition, due to the battery-powered nature, an object might leave the network when its battery is empty. Changing the batteries is difficult in many situation, where the objects are operating in hostile environment without any human intervention. As consequence, battery depletion is associated in many cases to the halt of the services provided by the corresponding object.

In its turn, 5G is introducing a novel dimension of dynamic in networks, which is mainly enabled by the softwarization of the network. Network Function Virtualization (NFV), and Software Defined Networking (SDN) are key technologies for 5G [4]. The concept of NFV is based on running network functions as softwares on the top of standard Virtual Machines (VMs) and through a virtualization platforms. As for SDN, it is based on the separation between the control plane and the data plane, and enables interworking of different Virtual Network Functions (VNFs) running on different VMs. These two technologies together enable the dynamic creation and orchestration of many services on demand. 5G also relies on the concept

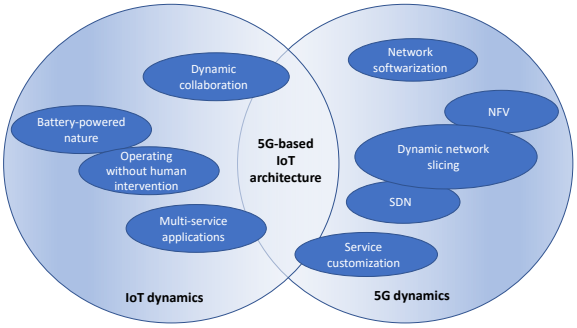

Fig. 2: Dynamic nature in 5G architecture-based IoT.

of network slicing. The latter is based on creating virtual network slices on the top of a common physical infrastructure. Each slice represents an independent virtualized network and is composed of multiple virtual resources customized to deliver an optimized solution [16]. All those technologies will provide the required functionalities to ensure 5G principles in terms of dynamic configuration, flexibility, scalability, and elasticity, allowing therefore network administrators to orchestrate and manage the different services [17].

Beside the fact that these 5G functionalities started at transport network, they are becoming involved in the Internet of Things and among IoT devices. The softwarization and the programmability of the network has been also proposed for use in the IoT. The consideration of the principle of SDN, along with NFV, would ease the configuration and the management of the different objects, as well as their related services. This would also enable the network to evolve as new objects and their services can be introduced to the network. Mobile networks are nowadays accommodating more and more heterogeneous devices with different QoS requirements [18]. Such requirements include the duration of the provided services. Moreover, different scenarios in opportunistic networks are also associated with a huge dynamic in terms of the related duration of the executed services (e.g., data dissemination and delivery [19], [20]). In addition, the communication between the involved devices is opportunistic and dynamic. This can pave the way for performing security adaptation. Recent works have tackled software defined networking for IoT operating systems such as TinyOS and Contiki [21], [22]. Slicing the IoT would also enable the adaptation to the different characteristics that vary depending the end-user requirements and the plethora of vertical applications the IoT is involved in [23]. This would be translated into on-demand and dynamic participation of nodes in communication. Therefore, in addition to the dynamics that characterize the IoT, 5G dynamics need also to be considered when used as a communication infrastructure for the Internet of Things. Fig. 2 schematizes the dynamics that characterize 5G-based IoT.

IV. Vision of end-to-end adaptive security & system model

While existing works on adaptive security perform adaptation during the use phase, the authors argue that this can be

considered even before. The proposed solution in this paper provides an end-to-end approach for security adaptation. In addition to the use phase, adaptation is also performed during the security establishment phase, leveraging both IoT and 5G dynamics. The security level related to the cryptographic keys is adapted during the establishment phase according to the estimated duration of the services to be provided by the objects. As discussed previously, the objects can offer their services on demand and are very dynamic in terms of their participation in the communication. The idea is to make the security level following this dynamic. In addition, the security level is adapted even during the use phase. This double adaptation will allow preserving more energy in 5G-based IoT networks.

The consideration of 5G as a communication infrastructure allows introducing more dynamic in the network in a way to reach application requirements. Thanks to the underlying softwarization and the programmability of the data plane, it has become possible to update nodes' contributions in the routing process. This can be issued by a control plane such as an SDN controller. As stated in the previous section, the programmability of the data plane has been considered for different IoT and WSN operating systems, such as TinyOS and Contiki, to cope with changes and dynamic of the applications. Such characteristics, which are not available in legacy WSN, enable more dynamic in the network, but also provide the necessary information about the service duration. Moreover, virtualization is also being considered for IoT objects, enabling to run different and isolated services on the top of the same IoT object. This further increases the dynamic of the provided services by the IoT nodes. The proposed end-to-end adaptive approach take advantage of the availability of different services and of their duration to adapt security accordingly in the establishment phase (in addition to the use phase).

We consider an IoT environment consisting of heterogeneous nodes. Let $\mathcal{P}$ be the set of the deployed objects. A summary of employed notations is provided in Table I (different notations are also shown in Fig. 3 and Fig. 4). The underlying communication is based on the 5G architecture. The management of the network and the underlying services are ensured by the orchestrator. This is performed as per the requirements of the different applications. To efficiently ensure its functions, the orchestrator is aware of the different information related to the objects (their type, capacity, resources, offered services, etc.). Fig. 3 provides a general overview of the considered architecture.

As for security, we consider a widely adopted scenario (used in many related works as [7], [8], [10], [13]) related to data origin authentication. Request messages are only issued by nodes authorized to do so, and can be very critical. Examples of such messages are requesting a node to change its position, asking a node to perform actions on the environment, etc. Given the nature of the IoT, some nodes could be compromised and target the malfunctioning of the network. Adversary nodes are interested in injecting bug messages in the network pretending to be from authorized nodes. If succeeded, this would have catastrophic consequences on the network and beyond. Therefore, a node associates an authenticator to each

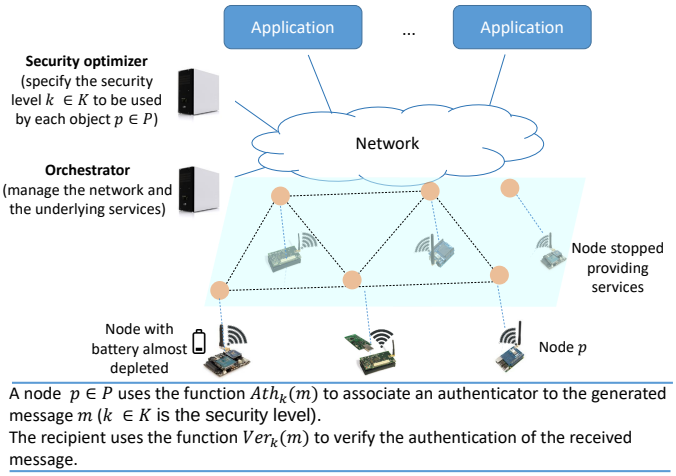

Fig. 3: General architecture for the proposed solution.

Notation	Description
$\mathcal{P}$	Set of objects; $\lvert\mathcal{P}\rvert = P$.
$\mathcal{N}(p)$	Neighbors of the object $p \in \mathcal{P}$.
$\mathcal{K}$	Set of security levels; $\lvert\mathcal{K}\rvert = K$.
$Ath_k(m)$	The authentication function of message m generated by p using its security level k.
$Ver_k(m)$	The function of verifying the authentication of p's message, m, using its security level k.
$\mathcal{V}(p)$	Nodes which will verify p's messages.
$\mathcal{V}^{-1}(p)$	Nodes which p will very their messages.
$\phi(p)$	Lifespan associated the service provided by p.
$\varphi(k)$	Lifespan associated to the security level k.
Δt	Time between security expiration and renewing.
C_p	Tolerable security renewing times for the object p.
$\mathcal{S}$	Set of coalition; $\mathcal{S} = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_K\}$.
$\mathcal{S}_k$	A coalition; Set of players using the security level $k \in \mathcal{K}$.
$\Pi_{\mathcal{S}_k}(p)$	Payoff of the player $p \in \mathcal{S}_k$.
$w(\mathcal{S}_k)$	Characteristic function of the coalition $\mathcal{S}_k$.
$\mathcal{S}_k \triangleright^p \mathcal{S}_{k'}$	The transfer operation of the player $p \in \mathcal{S}_k$ to the coalition $\mathcal{S}_{k'}$.
T_{pq}	Trust level that $p \in \mathcal{P}$ associates to $q \in \mathcal{P}$.
E_{pq}	The experience component of the trust T_{pq}.
O_{pq}	The observation component of the trust T_{pq}.
R_{pq}	Recommendation component of the trust T_{pq}.

TABLE I: Table of notations.

message it generates. The recipient node can therefore verify the authentication the received message and ensure its origin before considering executing its content. In addition, in order to prevent spreading bug messages in the network, the message sent by a node $p \in \mathcal{P}$ are also authenticated over its path to the destination by the relay nodes. Although this will prevent spreading bug messages in the network, preforming this process systematically is energy consuming. We denote by $\mathcal{V}(p)$ the nodes which will verify p's messages and by $\mathcal{V}^{-1}(p)$ the nodes which p will verify their messages. As shown in Fig. 3, a security optimizer entity is used in the considered architecture. It holds the logic allowing to specify the security level to be used for each object in the network. It also coordinates with the orchestrator to get the required information to perform security optimization. Different security levels are supported by the objects. The set of security levels is denoted by $\mathcal{K}$. The authentication and verification of the message m sent by p depends on its assigned security level. Let $Ath_k(m)$ and $Ver_k(m)$ denote respectively the function of authenticating

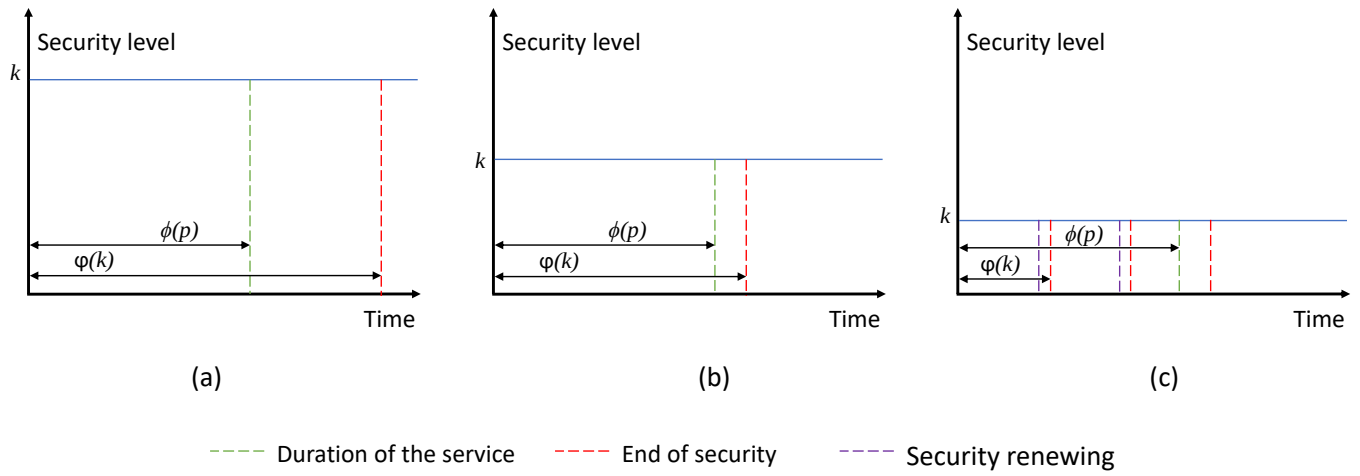

Fig. 4: Security adaptation at the establishment phase.

and verifying the authentication of the message m generated by p using its assigned security level $k \in \mathcal{K}$.

The provided solution in this paper proposes an end-to-end adaptive approach of two phases; the establishment phase and the use phase. The details about the two phases are respectively provided in the next two sections.

V. Security adaptation at the establishment phase

The aim of this phase is to adapt the security level at the establishment stage. When it comes to cryptographic keys, their sizes reflect the security level. The more the size is big, the more the security level is high. Indeed, each key is associated with a lifespan. The latter represents the estimated time required to recover the key using the efficient algorithms and machines. For instance, RSA cryptosystem security is based on the hardness of the Integer Factorization Problem (IFP). The latter can be solved (recovering the the private key from the public one) using Pollard's rho algorithm. The more the key size is big the more time would be required to complete the process. We define a security level by a cryptographic algorithm and a key, and we use the set $\mathcal{K}$ to refer to the set of the supported security levels by the objects. However, high security levels consume more resources compared to lower ones, for both nodes verifying and authenticating the messages. When an object is intended to remain in the system or provide its services for a small duration, employing high security levels for authentication would consume unnecessary resources. The idea behind the proposed security adaptation during the establishment phase relies on optimizing the security levels associated to each node.

When it comes to specifying security levels, static security must always consider the highest one. This does not take advantage of the nature and the characteristics of 5G-based IoT. The burden associated to a such strategy can be understood from Fig. 4 (a). Here, $\phi(p)$ and $\varphi(k)$ stand respectively for the estimated lifespan for the service provided by the object p and the security level k employed by p. Beside the fact that the highest level ensures the enough security, the latter is maintained a long time after the end of the offered service. This is indeed qualified as unnecessary. Intelligent optimization of the security level could reduce the overhead while maintaining the security for the connected objects.

In the proposed scheme, the security level is established according the service duration of the related object. The association is performed by the security optimizer module. The latter coordinates with the orchestrator to get the required information about the provided services in order to establish the optimized security levels. Indeed, the lifespan of the service provided by the object p can be estimated considering two situations: known service duration and unknown service duration. The first case reflects the situation where the service duration is known in advance. For instance, a deployed object, p, could be requested to provide a service for a fixed duration. In contrast, the unknown service duration corresponds to the situation where the lifespan of the service is not known in advance. In this situation, the service duration can be maximized by the object's lifetime. Indeed, many IoT objects are battery powered and their lifetime is limited. The depletion of the battery directly implies stopping the provided services. Without losing in generality, the authors consider that the service duration can always be provided by the orchestrator. Bounding the object's lifetime, a topic which has been addressed in other works such as [24]–[26], is not within the scope of this article.

Given the service duration of an object, providing the latter with a minimum security level that can ensure the entire service duration would maintain security. Fig. 4 (b) illustrates this principle where the chosen level k ensures the enough security for the services provided by the object p. In this case, as the security service is performed with that level, the related energy consumption is reduced compared to the highest level. Moreover, we argue that the security level can even be issued with a lifespan less than the entire service duration of the object. Before the end of security level's lifespan, a security renewing process must be triggered. We consider that security renewing implies renewing the key. This process should be repeated until the end of the service provided by the object. An illustration of this principle is provided in Fig. 4 (c). As

the security operations are performed with a lower level, the related energy consumption could be more reduced compared to the use of bigger ones. However, security renewing is associated to an overhead which is related to generating and securely distributing the cryptographic keys. Consequently, a trade-off must be established to associate security levels while ensuring the lowest energy consumption. In addition, we also consider that the service provided by an object p can tolerate a maximum number, C_p, of renewing operations, which is determined by the service requirement. The effective number of renewing operations an object p will be subject to can therefore be approached by $\frac{\phi(p)}{\varphi(k)-\Delta t}$, where Δt is the time between security expiration and renewing. Consequently, the security optimization solution must maintain the following condition:

$$\begin{cases} \eta_p^k < C_p \\ \eta_p^k = \frac{\phi(p)}{\varphi(k)-\Delta t}. \end{cases} \tag{1}$$

The energy consumption, ξ_p, of an object p is expressed as the sum of energy allocated to each operation performed by the node; processing, communicating, sensing and actuating. This is materialized by equation (2). The consumption associated to sensing and actuating operations are defined in terms of the amount of data related to these operations (resp. π_p^S and π_p^A) and the related energy consumption per bit (resp. ϖ_p^S and ϖ_p^A). The energy consumption associated to communication includes the parts related to transmitting data ($\pi_p^{Tx}\varpi_p^{Tx}$), receiving data from $\mathcal{V}^{-1}(p)$ ($\sum_{p'\in\mathcal{V}^{-1}(p)} \pi_{p'}^{Tx}\varpi_p^{Rx}$), and the communication part inherent from renewing security for both p and $\mathcal{V}^{-1}(p)$ ($\eta_p^k\xi_p^{Cnw_k} + \sum_{p'\in\mathcal{V}^{-1}(p)} \eta_{p'}^{k'}\xi_p^{Cnw_{k'}}$); $\xi_p^{Cnw_k}$ and $\xi_p^{Cnw_{k'}}$ refer respectively to the inherent energy consumption for a single renewing operation for p and $\mathcal{V}^{-1}(p)$. As for the energy consumption associated to processing, it includes the parts related to authenticating messages to be sent ($\pi_p^{Tx}\varpi_p^{Ath_k}$), verifying messages from $\mathcal{V}^{-1}(p)$ ($\sum_{p'\in\mathcal{V}^{-1}(p)} \pi_{p'}^{Tx}\varpi_p^{Ver_{k'}}$), and the processing part inherent from renewing security for both p and $\mathcal{V}^{-1}(p)$ ($\eta_p^k\xi_p^{Pnw_k} + \sum_{p'\in\mathcal{V}^{-1}(p)} \eta_{p'}^{k'}\xi_p^{Pnw_{k'}}$).

$$\begin{aligned} \xi_p &= \sum \xi_p^{tasks} \\ &= \underbrace{\pi_p^S\varpi_p^S + \pi_p^A\varpi_p^A}_{Sensing\ \&\ actuating} \\ &+ \underbrace{\pi_p^{Tx}\varpi_p^{Tx} + \sum_{p'\in\mathcal{V}^{-1}(p)} \pi_{p'}^{Tx}\varpi_p^{Rx} + \eta_p^k\xi_p^{Cnw_k} + \sum_{p'\in\mathcal{V}^{-1}(p)} \eta_{p'}^{k'}\xi_p^{Cnw_{k'}}}_{Communicating} \\ &+ \underbrace{\pi_p^{Tx}\varpi_p^{Ath_k} + \sum_{p'\in\mathcal{V}^{-1}(p)} \pi_{p'}^{Tx}\varpi_p^{Ver_{k'}} + \eta_p^k\xi_p^{Pnw_k} + \sum_{p'\in\mathcal{V}^{-1}(p)} \eta_{p'}^{k'}\xi_p^{Pnw_{k'}}}_{Processing} \end{aligned} \tag{2}$$

The underlying consumption of a node p depends on several parameters, including the employed security level k, but also the security level k' employed by the node $p' \in \mathcal{V}^{-1}(p)$. Both affect the authentication and the verification operations, and also the number of key renewing operations (reflected by the variables η_p^k and $\eta_{p'}^{k'}$). This shows an interdependence between the security levels to be established for the network nodes. Considering the fact that the security optimizer module aims to establish the optimized security level for each node, this problem complex to solve especially for a large network.

In order to efficiently select the security level for each node, this paper proposes a solution based on the framework of coalitional game. The game is defined among the set of objects, $\mathcal{P}$, which are considered as players. A coalition $\mathcal{S}_k$ groups the players which will be associated with the security level k. The goal is to form the coalitions in a way that the profit of the underlying players will be increased.

Having said the above, we can deduce that the number of coalitions is exactly the number of security levels. Let $\mathcal{S} = \{\mathcal{S}_1, \ldots, \mathcal{S}_K\}$ be the set of coalitions. As each player (IoT object) will be associated with one security level, the set of coalitions will involve separate players; i.e., $\forall \mathcal{S}_k, \mathcal{S}_{k'} \in \mathcal{S} : \mathcal{S}_k \neq \mathcal{S}_{k'} \implies \mathcal{S}_k \bigcap \mathcal{S}_{k'} = \emptyset$. The payoff of a player is defined to reflect the problem to optimize, which is based on the energy consumption as depicted in equation (3). Here, ξ_p^{max} represents the maximum energy that can be consumed by the node p. Thus, increasing the payoff of a node is translated in reducing its energy consumption.

$$\Pi_{\mathcal{S}_k}(p) = \xi_p^{max} - \xi_p \quad , p \in \mathcal{S}_k. \tag{3}$$

Each coalition $\mathcal{S}_k$ is associated with a characteristic function $w(\mathcal{S}_k)$. The latter is based on the payoff of the underlying players. To define the characteristic function of a coalition, the sum of the payoff of the associated players is used, as shown in equation (4);

$$w(\mathcal{S}_k) = \sum_{p\in\mathcal{S}_k} \Pi_{\mathcal{S}_k}(p). \tag{4}$$

In order to form the coalitions in a way to optimize the payoff of the associated players, coalitional games are characterised by a dynamic allowing the players to change their coalitions. The players are selfish and each one aims to increase its payoff without caring about the other players. To enable this dynamic in the proposed game, the authors define a transfer operation which allows a player to be transferred from one coalition to another. The underlying rule is provided in the following definition.

***Definition** 1: A player $p \in \mathcal{S}_k$ would be transferred to another coalition $\mathcal{S}_{k'}$, resulting in a new set of coalitions $\mathcal{S}' = \{\mathcal{S}_1, \ldots, \mathcal{S}_k \backslash \{p\}, \ldots, \mathcal{S}_{k'} \cup \{p\}, \ldots, \mathcal{S}_K\}$, iff:*

$$\mathcal{S}_k \rhd^p \mathcal{S}_{k'} \Leftrightarrow \begin{cases} \Pi_{\mathcal{S}'_{k'}}(p) > \Pi_{\mathcal{S}_k}(p) & (5.1) \\ \quad and & \\ \sum_{\tilde{p}\in\mathcal{V}(p)} \left[\Pi_{\mathcal{S}'_{\tilde{k}}}(\tilde{p}) - \Pi_{\mathcal{S}_{\tilde{k}}}(\tilde{p})\right] \geq 0 & (5.2) \\ \quad and & \\ \eta_p^{k'} < C_p & (5.3) \end{cases} \tag{5}$$

where $\tilde{k}$ is the security level employed by $\tilde{p}$.

Equation (5) of the above definition specifies the transfer rule. It is derived to allow players to increase their payoffs by changing their coalitions; a player p can be transferred from its current coalition $\mathcal{S}_k$ to another one $\mathcal{S}_{k'}$, if its payoff would be increased after performing the transfer (5.1), while

this operation does not have a negative effect on the verifying nodes in the set $\mathcal{V}(p)$ (5.2). Indeed, the security level of a node p also affects the energy consumption of the verifying nodes $\mathcal{V}(p)$, as stated earlier. Therefore, condition (5.2) ensures that if a transfer would happen, the associated gain of this operation on the verifying nodes is greater than the loss. As the object p would be transferred to a another coalition $\mathcal{S}_{k'}$, (5.3) aims to maintain condition (1) for the same node in the new coalition.

Considering this operation, the players will keep changing their coalitions and increasing their payoffs. The execution of the game is performed as described in Algorithm 1.

Algorithm 1 Coalitional game algorithm for the partition of the security levels.

Require: $\mathcal{S} = \{\mathcal{S}_1, \ldots, \mathcal{S}_K\}$
1: **while** True **do**
2: Stable = True
3: **for** each two coalitions $\mathcal{S}_k, \mathcal{S}_{k'} \in \mathcal{S}$ **do**
4: **for** each player $p \in \mathcal{S}_k$ **do**
5: **if** $\mathcal{S}_k \rhd^p \mathcal{S}_{k'}$ **then**
6: $\mathcal{S}_k = \mathcal{S}_k \backslash \{p\}$
7: $\mathcal{S}_{k'} = \mathcal{S}_{k'} \cup \{p\}$
8: Stable = False
9: **end if**
10: **end for**
11: **end for**
12: **if** Stable **then**
13: break
14: **end if**
15: **end while**

The execution of the coalitional game starts with an initial partition of the players on the coalitions. Thereafter, the transfer operation will be evaluated for each player (lines [3-5] of Algorithm 1). If this operation would lead to increased payoff, as per equation (5) of Definition 1, the transfer will be approved. The associated coalitions will thus be updated as shown in lines [6-7]. This process will be repeated by the players leading therefore to enhanced payoffs.

A crucial notion in coalitional game is the stability. It reflects a state where no player can increase its payoff any more by changing its coalition. It is highly important that a coalitional game is able to converge to a final (stable) partition. Formally, the stability of the proposed coalitional game can be defined as follows.

***Definition** 2:*

A state of the coalitions $S = \{\mathcal{S}_1, \ldots, \mathcal{S}_K\}$ is said to be stable, if the transfer operation can not be applied; i.e.,

$$\forall \mathcal{S}_k, \mathcal{S}_{k'} \in \mathcal{S}; \quad \nexists p \in \mathcal{S}_k | \ \mathcal{S}_k \rhd^p \mathcal{S}_{k'}. \tag{6}$$

It is worth noting that when the coalitional game does not always lead to a stable partition, the players might not stop changing their coalitions (infinite loop). For this reason, the authors provide the following theorem.

***Theorem** 1:*

Starting from an initial partition where condition (1) is satisfied, the coalitional game provided in Algorithm 1 is guaranteed to converge towards a stable and optimal partition.

Proof:

Let $\mathcal{S} = \{\mathcal{S}_1, \ldots, \mathcal{S}_K\}$ be an initial partition of the players on the coalitions, where condition (1) is satisfied. This partition will sequentially be subject of player transfer operations, as depicted in Algorithm 1. It should be noted that condition (1) will be maintained along these operations. Let us denote this transformation by the following formula:

$$\mathcal{S}^{(0)} \rightarrow \mathcal{S}^{(1)} \rightarrow \mathcal{S}^{(2)} \rightarrow ... \tag{7}$$

where $\mathcal{S}^{(i)}$ is the state of the coalitions (a partition) after performing the i^{th} player transfer operation, and $\mathcal{S}^{(0)}$ is the initial one. The symbol $\rightarrow$ refers to the transition from one partition to another. Based on this formula, we can formulate the following lemma.

***Lemma** 1:*

To prove the convergence of Algorithm 1, it suffices to prove that the transfer operation does not lead to repeated partitions.

The above theorem captures the fact that the set of players and coalitions are limited, and so is the possible combinations. Consequently, if the transfer operation does not lead to repeated partitions, the sequence defined in (7) must achieve a final state. The transition in this sequence is ruled by the transfer operation defined in equation (5). The latter can also be written as follows:

$$\mathcal{S}_k \rhd^p \mathcal{S}_{k'} \Leftrightarrow \begin{cases} \Pi_{\mathcal{S'}_{k'}}(p) > \Pi_{\mathcal{S}_k}(p) & (8.1) \\ \quad and & \\ \sum\limits_{\tilde{p} \in \mathcal{V}(p)} \Pi_{\mathcal{S'}_{\tilde{k}}}(\tilde{p}) \geq \sum\limits_{\tilde{p} \in \mathcal{V}(p)} \Pi_{\mathcal{S}_{\tilde{k}}}(\tilde{p}) & (8.2) \\ \quad and & \\ \eta_p^{k'} < C_p & (8.3) \end{cases} \tag{8}$$

Considering (8.1) and (8.2), we can see that the players $\{p\} \cup \mathcal{V}(p)$ have greater sum of payoffs in the new partition than what they had in the old one. In addition, the transfer operation does not affect the payoff of the rest of the node in the network (i.e., the set $\mathcal{P} \setminus \{p\} \setminus \mathcal{V}(p)$). Consequently, we can write the following:

$$S^{(i)} \rightarrow S^{(j)} \Rightarrow \exists S_k^{(i)}, S_{k'}^{(i)} \in S^{(i)}, p \in S_k^{(i)} | \ S_k^{(i)} \rhd^p S_{k'}^{(i)} \tag{9}$$

$$\Rightarrow \begin{cases} \Pi_{\mathcal{S}_k^{(i)}}(p) + \sum\limits_{\tilde{p} \in \mathcal{V}(p)} \Pi_{\mathcal{S}_{\tilde{k}}^{(i)}}(\tilde{p}) < \\ \Pi_{\mathcal{S}_{k'}^{(j)}}(p) + \sum\limits_{\tilde{p} \in \mathcal{V}(p)} \Pi_{\mathcal{S}_{\tilde{k}}^{(j)}}(\tilde{p}) \end{cases} \tag{10}$$

$$\Rightarrow \begin{cases} \sum\limits_{S_k^{(i)} \in S^{(i)}} \sum\limits_{p \in S_k^{(i)}} \Pi_{\mathcal{S}_k^{(i)}}(p) < \\ \sum\limits_{S_{k'}^{(j)} \in S^{(j)}} \sum\limits_{p \in S_{k'}^{(j)}} \Pi_{\mathcal{S}_{k'}^{(j)}}(p) \end{cases} \tag{11}$$

$$\Rightarrow \sum_{S_k^{(i)} \in S^{(i)}} w(S_k^{(i)}) < \sum_{S_{k'}^{(j)} \in S^{(j)}} w(S_{k'}^{(j)}). \tag{12}$$

Therefore, each resulting partition in the sequence (7) is different from the previous ones. This means that the transfer operation does not lead to repeated partitions. As per Lemma 1, the coalitional game described in Algorithm 1 converges to a stable partition. Moreover, the sum of the players' payoffs is increased at each partition. This allows

achieving an optimized partition of the security levels on the objects in a way to reduce the energy consumption. ■

The optimization performed in the establishment phase allows optimized assignment of the security levels on the nodes, in a way to reduce the energy consumption. This optimization will be boosted during the use phase. Indeed, while the energy consumption related to performing the verification operation is considered over all the path, security adaptation at the use phase intends to reduce this process, which would further improve the saved energy of the network. The next section introduces the proposed adaptive security solution at the use phase.

VI. Security adaptation at the use phase

This phase aims at adapting security during the use stage. Indeed, relay nodes verify the authentication of the transmitted messages in order to prevent spreading bug ones. However, performing this action systematically is very energy consuming. Therefore, the adaptation is considered with the perspective of adjusting the security level, by reducing the application of the verification service to the situations where it is required. Indeed, if the network nodes operate as it is expected, data origin authentication would consume unnecessary computing resources. It may happen that some nodes would be compromised, so in this case, the verification has to be performed by nodes receiving packets from suspicious ones. In the proposed scheme, each node decides locally to verify the authentication of the received message or not. The function $\mathcal{N}(p)$ is used to refer to the neighbors of $p \in \mathcal{P}$. Trust management, which has widely been used for dealing with selfish behavior and internal attacks, is employed to decide for applying the verification service.

Algorithm 2 captures the packet relaying logic, for a node p, of a message m' (originated by p') and received from the last hop $q \in \mathcal{N}(p)$. Here, T_{pq} refers to the trust level that p (receiver) associates to q (last relay) and f is the function that decides whether to apply the verification service or not. In the following, the trust management model that allows nodes to assess each others is detailed. This model will be used by the adaptive function f.

Algorithm 2 The relaying logic for a node p ($Receive$).

Require: m', p', q
1: **if** $(f(T_{pq}))$ **then**
2: $Send(m', NextHop)$
3: **else**
4: **if** $(Ver_{k'}(m'))$ **then**
5: $Send(m', NextHop)$
6: **else**
7: $Drop(m')$
8: **end if**
9: **end if**

In Algorithm 2, T_{pq} represents the trust level that p associates to q. It is a real number that takes value between 0 (which means that no trust is given to the trustee node) and 1 (complete trust). Three complementary components are considered to compute T_{pq}: p's own experiences E_{pq}, its own observations O_{pq}, and recommendations R_{pq} received about q. The related formula is provided in equation (13);

$$T_{pq} = \alpha_{pq} E_{pq} + \beta_{pq} O_{pq} + \gamma_{pq} R_{pq}, \tag{13}$$

where α_{pq}, β_{pq} and γ_{pq} are three parameters that keep the trust value between 0 and 1 by satisfying the relation $\alpha_{pq} + \beta_{pq} + \gamma_{pq} = 1$. In addition, they serve as weighting factors for the trust components. For example a great value of α_{pq} means that the trust evaluation will rely more on node experiences to compute T_{pq}. Moreover, the weighting parameters we propose are adaptive not only to each trustor node, but also to the trustee one. We argue that the three components should be adapted according to their relevance. For example, when p does not receive any recommendation about q or the received recommendations are so obsolete compared to the experiences and the observations, γ_{pq} should be very small. The authors introduce a relevance function $Rel^x_{pq}(n)$ that computes the relevance of the component x, as shown in equation (14). Here, x refers to the type of the trust component and can be e, o, or r (for experience, observation, or recommendation respectively). We denote by $\{t^x_1, t^x_2, ..., t^x_n\}$ the n last times at which the value of the component x has been updated by p about q. The more the updates are recent (i.e. $t_{now} - t^x_h$ is small), the more $Rel^x_{pq}(n)$ is big and the more x is relevant. Note that n is used to consider multiple updates as the trust cannot be relevant with one update.

$$Rel^x_{pq}(n) = \frac{1}{\sum_{h=1}^{n}(t_{now} - t^x_h)}. \tag{14}$$

Based on the relevance function of each component, the parameters α_{pq}, β_{pq}, and γ_{pq} can be computer as shown in equations (15). When there is no update for the component x we consider $Rel^x_{pq}(n) = 0$. Also, we consider that at the beginning T_{pq} is null (no updates).

$$\begin{cases} \alpha_{pq} = \frac{Rel^e_{pq}(n)}{Rel^e_{pq}(n)+Rel^o_{pq}(n)+Rel^r_{pq}(n)} \\ \beta_{pq} = \frac{Rel^o_{pq}(n)}{Rel^e_{pq}(n)+Rel^o_{pq}(n)+Rel^r_{pq}(n)} \\ \gamma_{pq} = \frac{Rel^r_{pq}(n)}{Rel^e_{pq}(n)+Rel^o_{pq}(n)+Rel^r_{pq}(n)}. \end{cases} \tag{15}$$

The following explains how to compute each component of the trust scheme: experiences, observations, and recommendations.

The trust level a node p perceives from the direct experience with a node q is represented by E_{pq}. The latter is constructed based on the result of the verification operation. Indeed, when p receives a packet from q, it may decide to verify the authentication of the received message (depending on the function f). If the packet is authenticated, this would have a positive impact on E_{pq}. However, when the packet is not authenticated means either q is compromised and has just sent an undesired message, or it is a clean node that retransmitted the message without verifying it. The last situation could be more recurrent when q is constrained in terms of resources.

The heterogeneity between nodes is considered in the proposed model and materialized through a relation of order. We denote by G_p the category of the node p. $G_p < G_q$ means that node p is more constrained than node q. Equation (16) provides the expression of the E_{pq} component. It is derived by taking into account the contributions of the old experiences, $E^{'}_{pq}$, and also the current one. This is respectively reflected by the first and the second terms in the right hand side of (16). The current experience can have the value 1 when the received message is authenticated, a value a ($0 < a < E^{'}_{pq}$) to tolerate an unauthenticated message from constrained node which is yet trusted (τ and g are thresholds), or the value 0 otherwise. As it can be noticed, the tolerance option decreases the value of E_{pq}, and so that of T_{pq}. Thus, even a trusty constrained node that keeps sending unauthenticated messages will be untrusted. The parameter δ^e_{pq} has two objectives. It aims to keep E_{pq} between 0 and 1 ($\delta^e_{pq} \in$]0, 1[) and weight the contributions of the new and old values. A small δ^e_{pq} means that E_{pq} would relies more on new experiences than old ones. A such situation can be considered when old experiences are not very relevant for evaluation (e.g., the time between two experiences is long or the node keeps changing its behavior frequently overtime). Note that when $\delta^e_{pq} = \frac{NB-1}{NB}$, E_{pq} becomes the average of the NB experiences of p with q.

$$E_{pq} = \delta^e_{pq} E^{'}_{pq} + (1 - \delta^e_{pq}) \times \begin{cases} 1 & \text{if } Ver_{k'}(m') \\ a & \big(\text{if not } Ver_{k'}(m') \text{ and} \\ & \quad T_{pq} > \tau \text{ and } G_q < g\big) \\ 0 & \text{otherwise.} \end{cases} \tag{16}$$

The trust level that p associates to q from observing its behavior is referred to as O_{pq}. It is based on the node's ability to overhear messages forwarded by other nodes in its communication range. More precisely, when p sends an authenticated message to q for relaying, the latter is supposed to forward it without changing the ciphertext part. In addition, when q receives a message from another node, it may not retransmit it as it could be unauthenticated. However, if q relays the received message, this should be without changing the ciphertext part. If it is not the case, the component O_{pq} will be affected negatively. Note that this is based on ciphertext comparison and does not require decryption or authentication of the message, which is an energy consuming operation.

Let $Rly_{qp}(m')$ denotes the function that returns the result of ciphertext comparing of the message m' sent by p to q for relaying (m' is originated by p'). The returned value can be 1 if q relayed the message without changing its content, 0 if it did not relay the message, and -1 if q relayed the message but changed its content. In the same way as E_{pq}, equation (17) provides the expression of the O_{pq} component and is derived to account for the contributions of the old observations, $O^{'}_{pq}$ (reflected by the first term of the right hand side of this equation) and the current one (represented by the the second term of the equation). The value of the current value can be 1 if q relayed the message correctly, a value b ($0 < b < O^{'}_{pq}$) for a constrained node that did not relay the message, and 0 if q is not constrained and did not relay the message or relayed a received message, from p or another node q', but changed its content. δ^o_{pq} is used for the same purpose as δ^e_{pq}; It weighs old and new observations, and keeps O_{pq} between 0 and 1 ($\delta^e_{pq} \in]0, 1[$).

$$O_{pq} = \delta^o_{pq} O^{'}_{pq} + (1 - \delta^o_{pq}) \times \begin{cases} 1 & if\, Rly_{qp}(m') == 1 \\ b & if\, (Rly_{qp}(m') == 0 \\ & \quad \text{and } G_q < g) \\ 0 & if\, (Rly_{qp}(m') == 0 \\ & \quad \text{and } G_q \geq g) \text{ or} \\ & (Rly_{qq'}(m') == -1). \end{cases} \tag{17}$$

Computing E_{pq} and O_{pq} does not imply the participation of other nodes. In contrast, R_{pq} represents recommendations of q's neighbors and has to be computed from notes sent by those neighbors (i.e. $\{q' \mid q' \in \mathcal{N}(q)\}$). However, if a node sends incorrect recommendations, this may impact the trust evaluation. Therefore, it is important to consider malicious witnesses when computing R_{pq}. Also, a node keeps authenticating recommendation messages it receives to avoid spoofing, which could affect the parameter R_{pq}.

We define $W_{pq'}$ as the weight of recommendation that p associates to q'. $W_{pq'}$ takes value between -1 and 1. The value 1 refers to a good witness, 0 to a bad one, and -1 to some one that says exactly the opposite. Note that in our solution node's trust level is completely independent of its weight of recommendation. The trust level gives the level a node can send authenticated messages regardless of its quality of recommendations.

When p receives a recommendation r from q' about q, it updates its R_{pq} component. The latter is derived by taking into account the old recommendations $R^{'}_{pq}$ and the current one r, as shown in equation (18). A recommendation r represents a real number between 0 and 1 (the next paragraph explains how to calculate r and when it can be sent). The parameter δ^r_{pq} weighs old and new values, and keeps R_{pq} between 0 and 1 ($0 < \delta^r_{pq} < 1$). When $W_{pq'}$ is near to 1 (good witness) r is directly considered as the current value. When it approaches -1 (node says the opposite), the value $1 - r$ is considered. When the weight is near to 0 (liar and unstable node), r should not be taken into consideration and no update is required. A threshold $0 < d < 1$ is used as shown in equation (18);

$$R_{pq} = \delta^r_{pq} R^{'}_{pq} + (1 - \delta^r_{pq}) \times \begin{cases} r & if\, W_{pq'} \geq d \\ (1 - r) & if\, W_{pq'} \leq -d. \end{cases} \tag{18}$$

When q' sends recommendations to p about q, it uses its $E_{q'q}$ and $O_{q'q}$ components as they reflect a direct perception (equation (19)). $\delta_{q'q}$ is a parameter that weighs between $E_{q'q}$ and $O_{q'q}$. As mentioned earlier, the weighting between the components is related to their relevance. We express in equation (20) a manner to compute $\delta_{q'q}$ in terms of $Rel^e_{q'q}(n)$ and $Rel^o_{q'q}(n)$. If $Rel^e_{q'q}(n) = Rel^o_{q'q}(n) = 0$ (at the beginning), we consider $r = 0$. To reduce energy consumption due to sending recommendation messages, this operation is trigged by a change threshold $0 < ct < 1$, i.e. r is sent when the difference between the actual and old value exceeds ct.

$$r = \delta_{q'q} E_{q'q} + (1 - \delta_{q'q}) O_{q'q} \tag{19}$$

$$\delta_{q'q} = \frac{Rel^{e}_{q'q}(n)}{Rel^{e}_{q'q}(n) + Rel^{o}_{q'q}(n)}. \quad (20)$$

To measure the weight of recommendations, we use a practical approach that enables exploiting even bad witnesses. in human society, when some one gives a recommendation, than it turns out to be not true, the person's credibility will decrease. In the same manner, to update the $W_{pq'}$ parameter we compare q' last recommendations about q with the near future experiences and observations about the same node. Indeed, node's experiences and observations are not affected by notes of witnesses and represent a direct perception. When a node q' gives a bad note about another node, then the latter proves to behave well, p should decrease $W_{pq'}$. If the node turns out that it is not trusted, $W_{pq'}$ should be increased. The same thing can be said for good notes. Therefore, when a node gives good recommendations, its weight parameter will tend to 1. When it gives opposite recommendations, its parameter will approach -1. If it is unstable (it changes between correct and incorrect reports), its weight parameter will be near to 0. $W_{pq'}$ is computed as shown in equation (21), while the derivation of the formula is explained in the following paragraph;

$$W_{pq'} = \frac{1}{u}\sum_{l=1}^{u}\left(\frac{1}{v_l}\sum_{z=1}^{v_l}(1 - 2|r_l - y_{lz}|)\right). \quad (21)$$

Equation (21) is derived in a way to associate the weight of recommendation to the node q' based on its credibility (near to 1 if it provides good recommendations, near to -1 if it gives opposite recommendations, and near to 0 if it is unstable). This is performed by comparing the recommendations of q' about q with what can be perceived by p about the same node. Let $\{r_1, r_2, ..., r_u\}$ be the u last recommendations sent by q' about q, and $\{y_{w1}, y_{w2}, ..., y_{wv_w}\}$ the v_w first nearest experiences/observations perceived by p about q after the recommendation r_w. Fig. 5 illustrates the idea of the first nearest experiences/observations. The term $|r_l - y_{lz}|$ in the equation (21) allows comparing each recommendation r_l with the values of y_{lz} ($1 \leq l \leq u, 1 \leq z \leq v_l$). Consequently, the term $1 - 2|r_l - y_{lz}|$ will be near to 1 when r_l approaches y_{lz} and near to -1 when the two values are distant. The operation is performed for u last recommendations. If some values of this operation are near to 1 and others are near to -1 , the total sum would approach 0 (unstable recommendations) and the reports sent by the relative node will not be considered to update R_{pq} as mentioned in the previous paragraph. Obviously, the comparison between r_l and y_{lz} will be relevant only if there is a short time between them, which is the reason behind taking the v_l nearest y_{lz} to r_l. At the beginning of the network life time, the $W_{pq'}$ cannot be constructed by equation (21) as q' recommendations have to be compared with the next observations/experiences. For that, it is possible to assign an initial value (for example 0.5) which will adapted progressively.

Based on the trust evaluation, T_{pq}, the function f decides on whether to verify the authentication of the received message or not, as shown in Algorithm 2. The proposed expression of the adaptive function f is provided in equation (22). When T_{pq} does not exceed a given threshold, $\bar{T}$, the value of the adaptive function will be 0 ($false$). This reflects the fact that node q is not trusted yet and the received messages should be verified. If T_{pq} exceeds the threshold, f will return the value of $\mathcal{U}$, where the latter is a random variable that follows a discrete uniform distribution between 0 and μ_q. This means that even when the T_{pq} exceeds the threshold, f will be returning 0 in a random manner. This would prevent the attack where a node tries to win the trust than changes to send bug messages. This enables p to detect malicious nodes that have already won its trust (this is commonly known as on-off attack). The value of parameter μ_q can vary depending on the behavior of the q. For instance, if it turns out that the node q is performing on-off attack, the value of μ_q can be decreased.

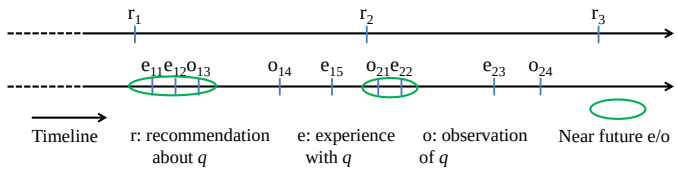

Fig. 5: Illustration of the future nearest experiences/observations.

$$f(T_{pq}) = \begin{cases} 0 & \text{if } T_{pq} < \bar{T} \\ \mathcal{U}(0, \mu_q) & \text{otherwise} \end{cases} \quad (22)$$

Finally, when a node q keeps sending unauthenticated messages, the parameter T_{pq} of p will be decreased, as consequence of the trust evaluation, and the verification method will be performed. In addition, if that node proves to be malicious over a long time, p decides to stop observing its behavior and sending recommendation about it (experiences remain considered). Indeed, if p always authenticate q's message, observing its behavior and sending recommendations about it would consume more energy than the basic model.

VII. Performance evaluation

This section provides the performance evaluations of the proposed end-to-end adaptive security. The coalitional game, to be running on the security optimizer entity, is implemented in python programming language. The NetworkX library [27] is used to model the network topology and get the different parameters (e.g., neighbors, path, etc.). The scenario consists in deploying a varying number of IoT nodes, where half of the objects are issuing request messages. The provided results are obtained by averaging 10 simulation trials. Different energy parameters considered in our evaluation can be found in [28]. We set ϖ_p^S and ϖ_p^A between 10 and 20 nJ/bit, π_p^S and π_p^A randomly between 100000 and 200000 bits, π_p^{Tx} between 10000000 and 20000000 bits, ϖ_p^{Tx} between 40 and 50 nJ/bit, ϖ_p^{Rx} between 30 and 40 nJ/bit, $\xi_p^{Cnw_k}$ and $\xi_p^{Pnw_k}$ between 400000 and 500000 nJ. Three security levels are considered where $\varpi_p^{Ath_k}$ and $\varpi_p^{Ver_{k'}}$ are set between 30 and 40 nJ/bit for the first level, then doubled and tripled for the second and the third levels respectively. The service duration of the objects are set to have a number of security renewing less than 4 times

for the first level, less than 3 times for the second level, and less than 2 times for the third level. The different parameters can be adjusted depending on the network characteristics. A random initial assignment, of the security levels of the players, is considered where condition (1) is satisfied.

Fig. 6 provides the average energy consumption per node under the different security levels. We can see that the average consumption increases as per the number of deployed IoT objects. This is due to the considered scenario where half of the nodes are issuing request messages, which makes nodes relaying more data when the number of deployed objects increases. We can also see that the proposed coalitional game provides better results compared to the initial assignment. Indeed, the coalitional game starts with the initial assignment, then consider transferring the players from one coalition to another (security levels). The transfer operation is performed only when the player's payoff is enhanced, leading to optimized energy consumption. It is to highlight that without considering the proposed coalitional game, the average energy consumption increases as per the number of considered security levels. For instance, when considering two security levels (red lines in Fig. 6 (b) and Fig. 6 (c)), despite that some nodes are not using the highest security level, the average energy consumption is bigger compared to when considering only the highest level (red line Fig. 6 (a)). The overhead related to the rekying process can cause more energy consumption. This concludes that considering different security levels can provide enhanced energy consumption only when optimized solution is adopted. The obtained results also prove the effectiveness of the proposed solution. Moreover, the evaluation also shows that more different security levels are considered the more energy consumption can be reduced. While the consideration of two security levels (Fig. 6 (b) and Fig. 6 (c)) allowed to achieve reduced energy consumption compared to the case of one security level (Fig. 6 (a)), the evaluation using three security levels (Fig. 6 (d)) allowed to reach more reduced energy consumption for the IoT nodes. Indeed, more number

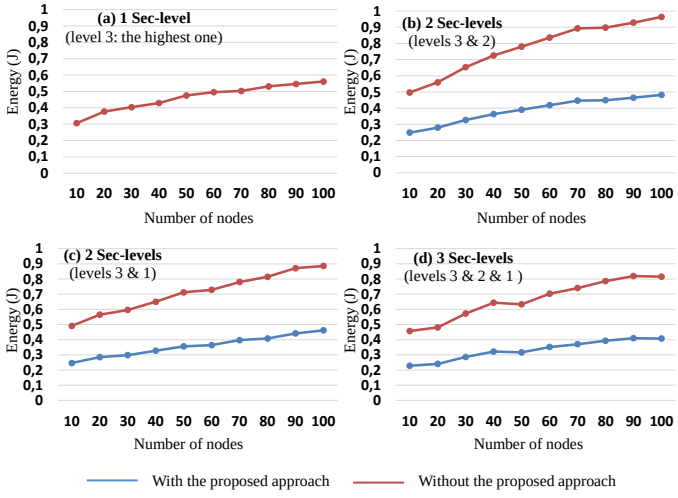

Fig. 6: Evaluation of the average energy consumption under different security levels.

of security levels is translated into more number of coalitions, allowing the players to explore more possibilities and to converge towards a better optimized partition.

In order to evaluate the complexity of the proposed coalitional game, the the authors have measured the number of transfer operations required to reach the stability. This also reflects the time needed to solve the coalitional game allowing to associate the optimized security level to each node in the network. The obtained results are depicted in Fig. 7. We can see that the number of transfer operations, and so is the time required for reaching the stability, increases as per the number of considered security levels. In addition, it also increases as per the number of deployed nodes. Indeed, these two parameters, respectively, reflect the number of coalitions and the number of players in the game. The more these parameters are big, the more transfer operations are required to reach the stability. We can also note that the evaluation of the same number of security levels with different types (lines (b) and (c) in Fig. 7) has provided almost the same result. This is due to the fact the number of coalitions is the parameter affecting the number of transfer operation. However, as the coalitional game is running on the security optimizer server, more resources can be dedicated to perform the security adaptation during the establishment phase. This would allow associating optimized security levels to the IoT devices without consuming their energy resources. The energy consumption will be further optimized during the use phase.

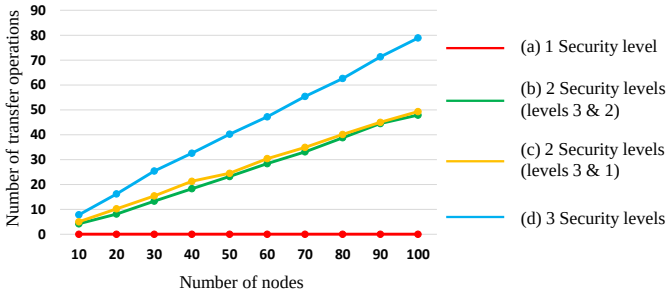

Fig. 7: Evaluation of the number of transfer operations.

In order to complement the evaluation of the solution, we carried out simulation related to the use phase using Cooja, the Contiki OS simulator [29]. The solution is implemented based on well-known and dedicated communication standards. More precisely, 6LoWPAN for adapting IPv6 packets to ZigBee frames, RPL for routing over objects, and UDP for data transport. As for the application layer, a simple service is implemented to generate a random message and sends it with its corresponding digest (authenticator) over the network. The library tinyDTLS [30] was used to produce the digest and perform data origin authentication. In addition to correct nodes, malicious nodes have also been implemented in this environment. More precisely, those that send unauthenticated data and those that send bad recommendations. The implementation choice on the top of well-known tools and standards aims to prove effectiveness of the proposed solution for IoT

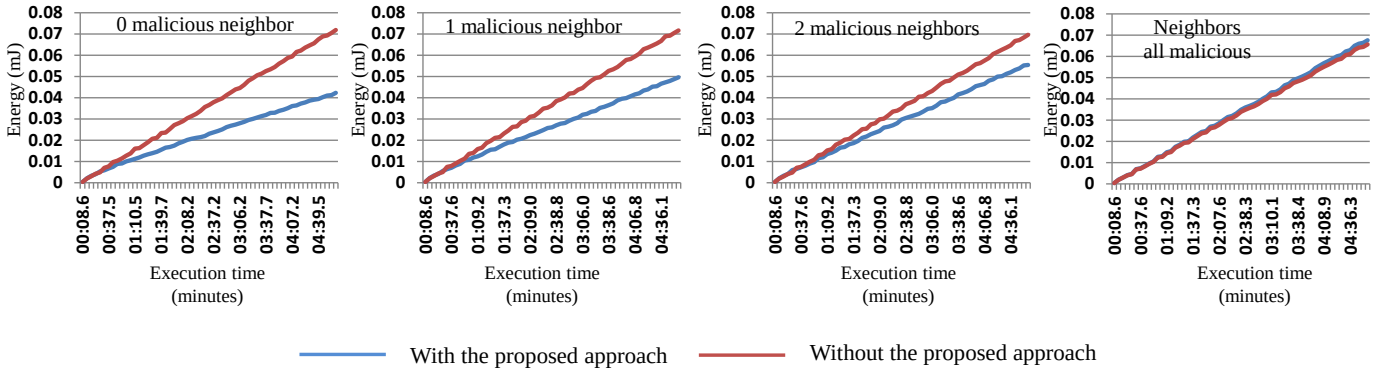

Fig. 8: Evaluation of the average energy consumption in the use phase of a node having five neighbors.

and WSN environments.

Messages related to our proposed scheme can contain data or recommendations. Nodes use the latter to inform other nodes about the trust level of its neighbors. This information helps to determine trustworthy nodes and exclude bad ones. We consider recommendation packets as control messages and we define for that an ICMPv6 information message that we call RIO (Recommendation Information Object). Indeed, in trust management solutions, recommendations are always used to inform network nodes about the trust level of another node, which requires a dedicated message. Therefore, in addition to RPL control messages (DIO, DAO, and DIS [31]), RIO is employed in the purpose of sending recommendations.

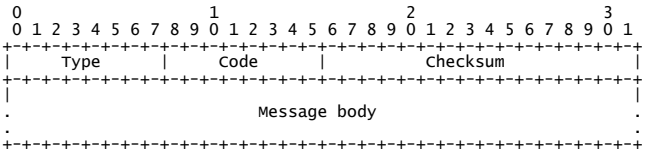

Fig. 9: ICMPv6 information message format [32].

Fig. 9 shows the general format of an ICMPv6 information message. *Type* specifies the type of the message. We assign it the value 200 which indicates private experimentation [32]. *Code* create more granularity for a given message type. We set it to 0 as we have only one message. The *Checksum* is used in ICMP control messages to detect errors which may have been introduced during transmission or storage. The *Message body* field depends on each control message. For RIO, it contains the trustee node's IP address and the recommendation value. An RPL control message contains possibly a number of options as specified in [31]. It is also possible to define a secure RIO variant, with the code 0x85, to provide integrity and replay protection as well as optional confidentiality and delay protection as it is specified in the RFC 6550. As stated in Section VI, transmission of a RIO message is triggered by the change threshold ct.

To represent object's category, the solution presented in the RFC 6551 [33] is considered, which consists in using the DAG Metric Container option of the message DIO (a RPL control message used for discovery) to encode three types of nodes: battery powered, energy harvesting, or line powered node. The evaluation was performed using the random topology of 30 nodes. α_{pq}, β_{pq} and γ_{pq} were set as per equation (15), with n=3. $\delta_{q'q}$ was set as per equation (20). We also set $a = E^{'}_{pq}/2$, $b = O^{'}_{pq}/2$, $\delta^{e}_{pq} = \delta^{o}_{pq} = \delta^{r}_{pq} = 1/2$, $ct = 1/4$, and $\bar{T} = 9/10$.

We evaluated the average energy consumption under the proposed trust based solution and the basic security model. The library "energest.h" is used to estimate the energy consumption. The obtained results depends on the number of malicious nodes. To capture the changes, Fig. 8 presents the results for a node having five neighbors. As can be seen, if no neighbor is compromised there is an important difference in terms of the energy consumption between the proposed scheme the basic model. When no neighbor is compromised, the corresponding node can reduce its energy consumption by 40.39%. Our evaluations showed that energy consumption can be reduced by more than 100% for nodes receiving an important number of packets. The gain of energy using the proposed solution remains considerable even when some neighbors are compromised.

In the other hand, we can observe that the energy consumption under the proposed trust model exceeds the baseline solution when all the neighbors are malicious. Indeed, this reflects the worst case where the highest security level should be used. The associated increase in terms of energy consumption is related to the operations needed for computing the trust. However, as advanced solution proposes to stop observing and sending recommendations about nodes that proved to be definitively malicious, the energy consumption when all neighbors are compromised is slightly increased to the baseline model, which is mainly due to the computing of the trust at the beginning.

In addition to nodes' lifetime, we carried out simulations to measure the relevance of the proposed scheme in terms of trust and transmitting authenticated messages. We considered for that commonly known attacks that may occur in trust management systems, which are bad behaving and bad witnessing.

When a node becomes malicious and sends systematically unauthenticated messages, the trustor node can detect it even if this node is trusted, as the function f returns the value 0 ($false$) following a random distribution (discrete uniform

distribution). Therefore, we considered a scenario where the trustee node performs an on-off attack after being trusted. Fig. 10 shows the trust evolution for the trustor. As it can be seen, the trustee node can mislead the trustor and send unauthenticated messages. However, because the adaptive function returns the value 0 following a random distribution, the trustee can't know when this event will happen. In addition, even if the trustee tries to regain the trust and send authenticated messages (on-off attack), the decision function considers reducing the value of the parameter μ_q of the uniform distribution, which is translated into small period for returning the value 0. The period will increase if the trustee behaves well for a long time. The proposed solution provides a key contribution by keeping trace of node's behavior.

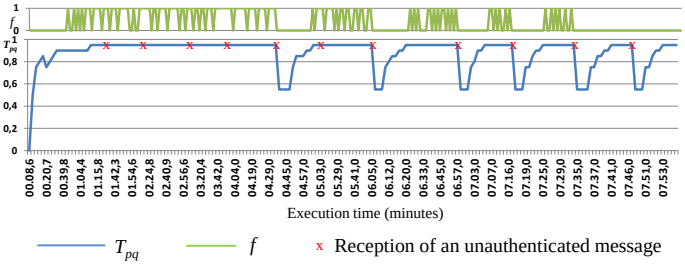

Fig. 10: Trust evaluation under on-off attack.

We introduced in our scheme the concept of the relevance of the component and we proposed a relevance function to weigh dynamically each component. To show the added value of this principal, evaluations are performed with and without the relevance function. Fig. 11 shows the evolution of the trust. When $Rel^x_{pq}(n)$ is not used, we considered that $\alpha_{pq} = \beta_{pq} = \gamma_{pq} = 1/3$. Indeed, without the relevance function, all components are weighted statically. In the studied works on trust management for adaptive security, the considered components are weighted statically. If, for one reason or another, a component is not enough updated, the trust evaluation will be inefficient (the threshold $\overline{T} = 9/10$). Indeed, such situation could be present given the dynamic nature of the IoT. For example, when the witnesses do not send recommendations or the trustor stops observing the trustees to save its energy, the relevance function ensures an efficient weighting.

To deal with the problem of bad witnesses, the authors presented a technique that measures node's weight of recommendation based on the first nearest experiences/observations principal. To measure the effectiveness of this approach, simulations were carried out with and without this technique. Fig. 12 shows the evolution of the trust. For this experimentation, we considered a scenario in which the trustee behaves good than badly. In addition, two witnesses are considered where one send opposite recommendations and the other unstable recommendations. At the beginning, bad witnesses can affect the trust evaluation as the trustor has not yet computed their weight of recommendation. Once it is done, the trustor can ignore unstable recommendations and exploit those that say the opposite. When $W_{pq'}$ is not used, bad witnesses

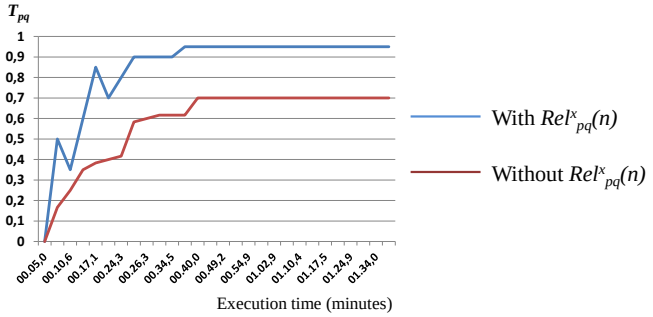

Fig. 11: Trust evaluation with and without the relevance function.

can influence the trust evaluation considerably. Furthermore, as the proposed solution distinguishes between weight of recommendations and trust level, even a malicious node that sends authenticated message and bad recommendations at the same time can be detected. This allows to deal with the credibility of the recommendations which is not tackled in the existing works on trust management for adaptive security, and is one of the key contributions of the our work.

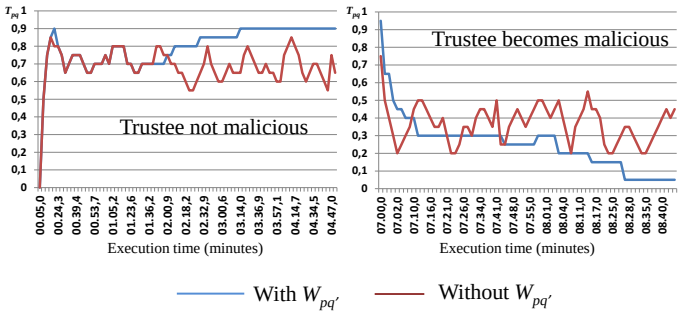

Fig. 12: Trust evaluation under bad witnessing.

VIII. Conclusion

Energy-efficiency has always been a challenging problem in security. While security services are more known for being resource-intensive, the IoT can involve constrained devices that might not support such consumption. The authors proposed in this paper a solution for energy-efficiency in security of the IoT. The contribution is based on the concept of adaptive security and considers the dynamics inherent from both the IoT and 5G, wich is expected to be the main communication infrastructure. The introduced solution advances the existing work by enabling end-to-end adaptation. At the establishment phase, the security level of each node is adapted to match with the duration of the service. The problem is formulated using the framework of coalitional game to associated each object with the optimized security level. At the use phase, the security service is adapted according to the threat level in the network. The framework of trust management is employed to evaluate the level of threat. This double adaptation allows to preserve more energy and increase objects lifetime.

REFERENCES

[1] H. Hellaoui, A. Bouabdallah, and M. Koudil, "Tas-iot: Trust-based adaptive security in the iot," in *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, Nov 2016, pp. 599–602.

[2] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct 2017.

[3] B. Insider, "report on how the internet of things will explode by 2020," http://www.businessinsider.com/, 2015.

[4] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5g be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[5] B. Insider, "report on how 5g will revolutionize the internet of things," http://www.businessinsider.com/, 2017.

[6] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy-efficient mechanisms in security of the internet of things: A survey," *Computer Networks*, vol. 127, no. Supplement C, pp. 173 – 189, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128617303146

[7] M. Hamdi and H. Abie, "Game-based adaptive security in the internet of things for ehealth," in *Communications (ICC), 2014 IEEE International Conference on*, June 2014, pp. 920–925. [Online]. Available: http://dx.doi.org/10.1109/ICC.2014.6883437

[8] X. Li, M. R. Lyu, and J. Liu, "A trust model based routing protocol for secure ad hoc networks," in *Aerospace Conference, 2004. Proceedings. 2004 IEEE*, vol. 2, March 2004, pp. 1286–1295 Vol.2.

[9] C. Chigan, L. Li, and Y. Ye, "Resource-aware self-adaptive security provisioning in mobile ad hoc networks," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 4. IEEE, 2005, pp. 2118–2124.

[10] M. Younis, N. Krajewski, and O. Farrag, "Adaptive security provision for increased energy efficiency in wireless sensor networks," in *2009 IEEE 34th Conference on Local Computer Networks*, Oct 2009, pp. 999–1005.

[11] A. V. Taddeo, L. Micconi, and A. Ferrante, "Gradual adaptation of security for sensor networks," in *World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a*, June 2010, pp. 1–9.

[12] A. Taddeo, M. Mura, and A. Ferrante, "Qos and security in energy-harvesting wireless sensor networks," in *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*, July 2010, pp. 1–10.

[13] A. D. Mauro, X. Fafoutis, and N. Dragoni, "Adaptive security in odmac for multihop energy harvesting wireless sensor networks," *Int. J. Distrib. Sen. Netw.*, vol. 2015, pp. 68:68–68:68, Jan. 2015. [Online]. Available: http://dx.doi.org/10.1155/2015/760302

[14] P. Keeratiwintakorn and P. Krishnamurthy, "Energy efficient security services for limited wireless devices," in *2006 1st International Symposium on Wireless Pervasive Computing*, Jan 2006, pp. 1–6.

[15] G. Tsoukaneri, M. Condoluci, T. Mahmoodi, M. Dohler, and M. K. Marina, "Group communications in narrowband-iot: Architecture, procedures, and evaluation," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2018.

[16] P. Rost, C. Mannweiler, D. S. Michalopoulos, C. Sartori, V. Sciancalepore, N. Sastry, O. Holland, S. Tayade, B. Han, D. Bega, D. Aziz, and H. Bakker, "Network slicing to enable scalability and flexibility in 5g mobile networks," *IEEE Communications Magazine*, vol. 55, no. 5, pp. 72–79, May 2017.

[17] T. Taleb, A. Ksentini, and R. Jantti, ""anything as a service" for 5g mobile systems," *IEEE Network*, vol. 30, no. 6, pp. 84–91, November 2016.

[18] Y. Liu, L. Hao, Z. Liu, K. Sharif, Y. Wang, and S. K. Das, "Mitigating interference via power control for two-tier femtocell networks: A hierarchical game approach," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 7194–7198, July 2019.

[19] Y. Liu, W. Quan, T. Wang, and Y. Wang, "Delay-constrained utility maximization for video ads push in mobile opportunistic d2d networks," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 4088–4099, Oct 2018.

[20] Y. Liu, H. Wu, Y. Xia, Y. Wang, F. Li, and P. Yang, "Optimal online data dissemination for resource constrained mobile opportunistic networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 5301–5315, June 2017.

[21] T. Luo, H. P. Tan, and T. Q. S. Quek, "Sensor openflow: Enabling software-defined wireless sensor networks," *IEEE Communications Letters*, vol. 16, no. 11, pp. 1896–1899, November 2012.

[22] S. Costanzo, L. Galluccio, G. Morabito, and S. Palazzo, "Software defined wireless networks: Unbridling sdns," in *2012 European Workshop on Software Defined Networking*, Oct 2012, pp. 1–6.

[23] L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "Sdn-wise: Design, prototyping and experimentation of a stateful sdn solution for wireless sensor networks," in *2015 IEEE Conference on Computer Communications (INFOCOM)*, April 2015, pp. 513–521.

[24] M. Bhardwaj and A. P. Chandrakasan, "Bounding the lifetime of sensor networks via optimal role assignments," in *Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, vol. 3, June 2002, pp. 1587–1596 vol.3.

[25] H. Zhang and J. Hou, "On deriving the upper bound of α-lifetime for large sensor networks," in *Proceedings of the 5th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '04. New York, NY, USA: ACM, 2004, pp. 121–132. [Online]. Available: http://doi.acm.org/10.1145/989459.989475

[26] Y. Chen and Q. Zhao, "On the lifetime of wireless sensor networks," *IEEE Communications Letters*, vol. 9, no. 11, pp. 976–978, Nov 2005.

[27] "NetworkX networkx library for python," https://networkx.github.io/, accessed: 2019-07-30.

[28] J. Huang, Y. Meng, X. Gong, Y. Liu, and Q. Duan, "A novel deployment scheme for green internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 196–205, April 2014.

[29] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *31st IEEE Conference on Local Computer Networks, Proceedings 2006*, Nov 2006, pp. 641–648.

[30] O. Bergmann. Tinydtls: a library for datagram transport layer security. [Online]. Available: https://sourceforge.net/projects/tinydtls/

[31] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550 (Proposed Standard), Mar. 2012. [Online]. Available: http://www.ietf.org/rfc/rfc6550.txt

[32] A. Conta, S. Deering, and M. Gupta, "Internet control message protocol (icmpv6) for the internet protocol version 6 (ipv6) specification, rfc4443," *IETF, March*, 2006.

[33] J. Vasseur, M. Kim, K. Pister, N. Dejean, and D. Barthel, "Routing metrics used for path calculation in low-power and lossy networks [online] available: https://tools. ietf. org/html/rfc6551," *IETF: April*, 2017.