A Survey on Wireless Sensors Networks Security Based on a Layered Approach

Raul A. Fuentes-Samaniego, Ana Rosa Cavalli, Juan A. Nolazco-Flores, Javier Baliosian

A Survey on Wireless Sensors Networks Security based on a Layered Approach

Raul A. Fuentes-Samaniego[1], Ana Rosa Cavalli[1], Juan A. Nolazco-Flores[2], and Javier Baliosian[3]

[1] Telecom SudParis, Evry, France,
fuentess@telecom-sudparis.eu and ana.cavalli@telecom-sudparis.eu,
[2] ITESM Tec de Monterrey, Monterrey, Mexico
jnolazco@itesm.mx,
[3] Universidad de la Republica, Montevideo, Uruguay
baliosian@fing.edu.uy

Abstract. The Internet of Things (IoT) is one of the most novel networking paradigms and there are yet too many technologies defining themselves as IoT complicating the scenario for developing a fully IoT environment. The situation becomes even harder when security and privacy are considered. In this paper, we present a survey on the security aspects of an IoT conformed by wireless sensors communicating through the IEEE 802.15.4 standard. This survey follows a revision of the state of art in a layer-by-layer systematic analysis.

Keywords: IoT WSN 6LoWPAN CoAP 802.15.4

1 Introduction

The Internet of Things (IoT) is "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols" [1]. The IoT is composed by "interconnected objects", which usually have a wireless network device as a medium of communication, the objects (or things) include a great variety of technologies for an equally diverse list of objectives. Additionally, the IoT needs a "standard communication protocol" to be able to connect the different types of nodes. The different types of nodes are a "world-wide network" as it can be composed of hundreds of nodes conforming one or more networks throughout the world. It is required to consider the three aspects mentioned above at the same time to be able to develop applications for the IoT [2]. Aside from them, the legal implications of the data collected from the objects and the security concerns that have to be handled by the applications are necessary to be considered. The sum of the five previous aspects for the development of an IoT application is referred in this work as a fully IoT environment as shown in the Fig. 1.

The IoT can be composed by a great variety of objects, with different origins, using different schemes for their identification and for handling information, examples are the Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, between others. Applications under IoT are varied such as smart homes, smart cities, traffic congestion monitoring, waste management. Given its ubiquity, very sensible and personal information may travel across this network, security and privacy in the IoT are of paramount importance. Still, many IoT devices have shown to have vulnerabilities that are easy to exploit [3]. Even more, standards widely used by IoT implementations, such as Wireless Sensor Network (WSN) and RFID, were not designed with security in mind [4–6].

The survey has as objective to produce a review of the state of the art regarding to the IoT, taking as a platform the WSN whose sensors works with the IEEE 802.15.4 standard.

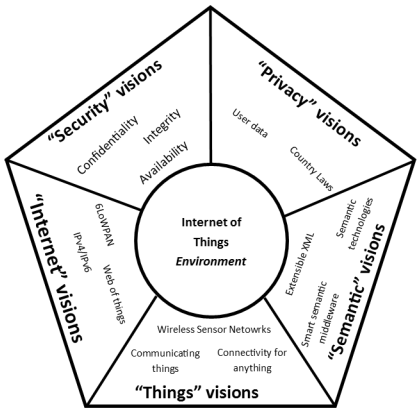


Fig. 1. "Internet of Things" paradigm as a result of the convergence of different visions.

The sections 2 to 4 reviews the state of art respect to the OSI layered model. Specifically the Section 2 is a review of the two lowest layers: Physical and Data-link layers which correspond to the IEEE 802.15.4 standard. The Section 3 is dedicated to the Network layer, which is focused on IPv6 and its constrained version for WSN networks. The Section 4 is the review of the upper layers, and finally in the Section 5 the conclusions are presented.

2 Physical & Data-Link Layers

The work on the lower layers of sensor networks has been centered around their performance issues. However, as they started to be an important part of the IoT, their security issues have gained in importance. To bound the scope of this work, when reviewing the work made for the low network layers, this survey focus on the IEEE 802.15.4-2006 standard due to its ubiquity and its good control of unreliable transmissions, latency and freshness of the messages, as well as by its MAC layer security mechanism with Advanced Encryption Standard (AES) 128-bits, and its native support for IPv6.

2.1 PHY layer

Vulnerability Analysis. The main vulnerabilities that any WSN node can face at the PHY layer are [7]: (i) Conflicts due to the nature of the wireless communication allows jam situations to happen, where two or more nodes begin to transmit provoking the overlapping of their signals. (ii) The exhaustion of the limited power supply of the nodes. Too many transmissions can lead to a faster exhaustion. The traffic can be originated by malicious attackers or by the hot-spot problem as shown in the Fig. 2. (iii) The tampering of the sensor brings the risk of subtracting information or hardware that is vital for its correct operation or even acquiring control over it. (iv) A shutdown of one or more nodes, for any given reason, can cause a loss of redundancy, bringing up the risk to lose the connectivity on different parts of the WSN topology.

Threat analysis. The following are some examples of threats at the PHY layer: (i) Bit errors caused by devices that flood the same area of sensors and with signals transmitted on the 2.4GHz channel (jamming). If the nodes try to retransmit while are in a JAM situation they can exhaust their power supply prematurely. (ii) Physical damage or stealing of sensors and sink nodes: the keys in the memory of the nodes could be subtracted, as well as the

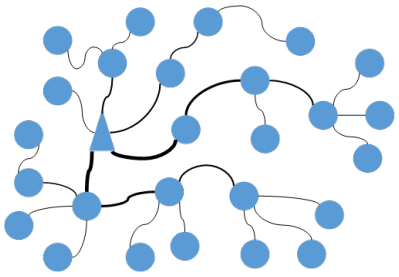


Fig. 2. Hot-spot dilemma: Certain nodes will carry the messages to others nodes, thus, transmitting more often and spending faster their power supply. [8].

data collected in them. (iii) The read of the wireless data (Sniffing) with the risk of the credentials stealing or private information acquiring.

2.2 MAC Layer

Vulnerabilities Analysis. The main vulnerabilities that any WSN node can face at the MAC layer are: (i) An unreliable transfer since the upper protocols are connectionless, the risk of having a higher channel error rate exist; thus forcing the allocation of resources to error handling in this layer. (ii) Unauthorized nodes joining to the WSN network. (iii) Latency in the multi-hop routing, the network congestion and the node processing can lead to a greater latency in the network, thus making it difficult to achieve synchronization among sensors [6]. (iv) The collision of messages due to a bad control of the message flow or an excess of nodes for the control to be executed successfully. (v) The exhaustion of the medium due to continuous transmission, with the risk of depleting the power supply of the sensors.

Threat analysis. Following is a list of the possible threats on this layer, mainly the DoS attacks. (i) Bits errors by denial of services (DoS) attacks. Under a DoS persistent attack, the sensor's authentication could fail leaving them isolated. Additionally, the DoS will reduce the bandwidth for all the nodes. (ii) Read wireless packets (Sniffing): Malicious nodes could be able to steal credentials for the AES mechanism on this layer. (iii) Impersonate other WSN nodes as the sink nodes, for taking partial or total control over the network. The communication can be compromised as the nodes could get and process traffic that should not be getting.

2.3 Discussion

The risks associated with the Data-Link layer such as collisions, exhaustion and the uneven access to the medium can be mitigated by the use of encryption on the MAC layer because it is able to separate unauthorized nodes from the network. For tampering attacks, the selection of sensor hardware and how they are placed define their resistance against those attacks. However, this selection may probably cause a higher sensors cost. The importance of the data which is held or forwarded by the sensors must help to decide between price and security.

The most obvious alternative to prolong the network lifetime is placing a higher capacity battery on key nodes. However, the work in [8] proposed mobile sink nodes for reducing the hot-spot risk, and it concluded that using a path-constrained mobile sink may improve the network lifetime. However, it is not always possible to create mobile sink points. In the

case they are used, their velocity has to be carefully considered, the work in [9] shows that the IEEE 802.15.4 standard is not able to maintain a node's connectivity for fast moving nodes.

It is possible to defend the network against jamming using various forms of spread-spectrum or frequency hopping communication. However, those mechanisms require more complex hardware and permanent power supply, the low-cost and low-power sensors are quite limited in this aspect [7, 10]. Still, the same work concluded than a well designed antenna polarization can properly handle some jamming attacks. The work in [11] also suggests a series of measures to control jamming attacks: (i) Detection techniques: deploying elements for discovering instantly a jamming attack. (ii) Proactive countermeasures: software measures, such as changing the MAC protocol for adding FHSS. Some of the techniques are compatible with the IEEE 802.15.4 standard. (iii) Reactive countermeasures: enable reactions only when a jamming attack is detected, many techniques are compatible with the IEEE 802.15.4 standard. (iv) Mobile Agent-based solution: Special mobile-agents are defined and used as autonomous programs with the ability to move from host to host, in this case for finding new paths free of jamming attacks.

The passive and active protection can handle the risk of tampering [6, 10]. The passive mechanisms are those who do not need additional power and include technologies that protect a circuit from being detected. Examples are the protective coatings and the tamper seals. The active defenses are related to special hardware circuits to prevent sensitive data from being exposed. Due to the cost of the active defenses, it will hardly be seen in the sensors [10].

The suggestions in [6] related to hardware choices can have an impact against the tampering attacks, for instance: (i) periodical checking of the location for detecting any tampered sensor. (ii) Acquiring hardware capable of self-termination. This can be very useful for avoiding any risk of shared keys or data, falling into the wrong hands. (iii) Low-cost protection countermeasures as a randomized clock signal, randomized multi-threading, robust low-frequency sensor which kills the processor at the first tamper try, restricted program counter and top-layer sensor meshes for being an annoyance to micro-probing attackers.

The authentication mechanism can begin on the Data-Link layer, the greatest benefit is that, almost everything inside the IoT environment will be hidden from passive observers (sniffing) as the MAC layer has Advanced Encryption Standard (AES) 128-bits. Some platforms as ZigBee already implement a system based in PANA for authentication, meanwhile open-source, such as Contik, offers a similar alternative.

3 Network: IPv6 and routing protocol

With the IEEE 802.15.4-2006 standard, the nodes inside of the WSN subnetwork use the 6LoWPAN protocol meanwhile the other nodes use the IPv6 protocol. Before handling the analysis of the vulnerabilities and threats, we will first focus on two areas related to the adaptation of IPv6 to WSN: the techniques for the compression of IPv6 with its secondary protocols. And, the types of communication between nodes that are inside the IoT environment.

3.1 6LowPAN

The 6LowPAN specifications are defined in [12, 13]. The UDP header, the IPv6 protocol, the ICMPv6 sub-protocol and the Neighbor Discovery protocol, which is part of ICMPv6, are severely modified for adapting them to an environment where multicast is not desired and the size of the messages must be small.

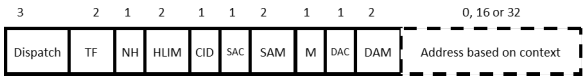


Fig. 3. A general overview of the 6LoWPAN header.

The IPv6 header is strongly modified to compress it from 40 bytes to 3 bytes using the Header Compression technique (HC1) [14]. *Because the version field is removed, it is mandatory to use only 6LowPAN inside of the WSN subnetwork.* If only one address is used, the header will have a length of 40 bits (5 bytes) otherwise will be of 48 bits (6 bytes). The Fig. 3 shows a 6LoWPAN header. The terms 6LoWPAN subnetwork and WSN subnetwork are interchangeable in this work.

A new IPv6 header is defined as *RH4 routing header* [15] used by the routing protocol defined in [16] called IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL). The RPL is an addresses-based mechanism instead of location-based.

Neighbor Discovery Protocol The ICMPv6 sub-protocol Neighbor Discovery (ND) is a key element of IPv6. It allows the nodes to perform an auto-configuration without the need of a third service as DHCP. The standard ND uses the stateless auto-configuration (SLAAC) and the stateful configuration which is equivalent to the normal configuration on IPv4. The ND protocol for 6LoWPAN was redesigned in [13] deprecating some elements stated in [12]: The Duplicate Address Detection (DAD) messages are reduced to a minimum, the multicast is taken away, and special messages for nodes on duty sleep are introduced to ND. Additionally, the order of messages sent is changed giving priority only to RA ones.

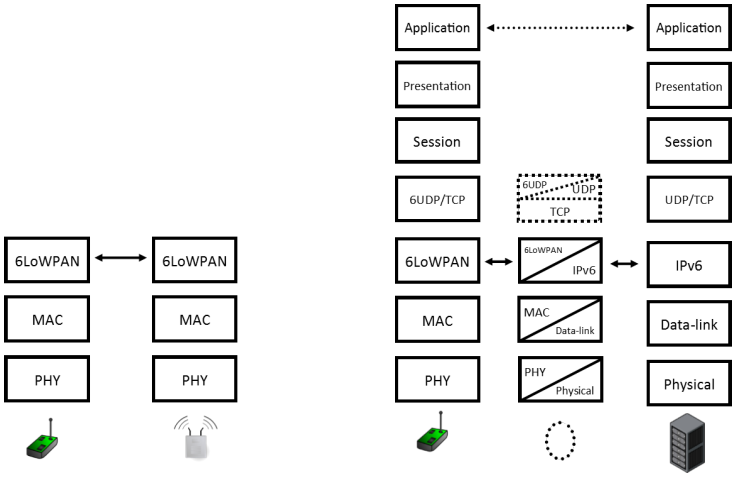
Routing Protocol for Low-Power and Lossy Networks (RPL) The RPL routing protocol is used to route messages between nodes on a mesh topology or star topology. The work in [17] concluded that RPL is able to deliver messages on multipoint-to-sink and sink-to-multipoint, including point-to-point but is not optimal for the last, due to the RPL nature. The routing protocol is defined in [16] and is stated that RPL can work in "unsecured", "pre-installed" and "authenticated" mode for authentication purposes. The first mode consists of RPL messages without any security mechanism. On the second mode, the nodes have pre-installed keys for RPL. And finally, in the third mode the nodes use pre-installed keys to request to a third authority server for a new key.

The RPL protocol has been designed for 6LoWPAN and was released in March 2012. Therefore, RPL needs to have more experiments to measure the actual performance of ZigBee IP or Contiki in real environments. As well, more security analyses must be realized, particularly, how it reacts to malicious or malfunctioning nodes, and against wormhole attacks [10].

3.2 Type of communication

The most important types of communication between the IoT environment entities are: (i) Sensor-Sensor & Sensor-Sink: It will carry data and commands for the sensor. Sink and sensors will pass the information as shown on the Fig. 4a. (ii) Sensor & Border router: The translation from the IEEE 802.15.4 subnetwork with 6LoWPAN to another subnetwork, as Ethernet with IPv6, is made with a special gateway as shown in the Fig. 4b.

Vulnerabilities analysis All the well-known risks of vulnerabilities on IP networks still apply, however, 6LowPAN bring new challenges and risks that can be exploited. More work



(a) Communication Sensor - Sink

(b) Communication Sensor - outsider server

Fig. 4. Type of communication based in layers.

is needed for developing a well-defined list of risks for 6LoWPAN. Yet, the following risks are identified:

- The nodes answer to fake ND messages, adding extra scopes to their configuration.
- Malicious nodes transmitting poisoning messages against the RPL protocol.
- Malicious nodes trying to pass by other nodes, by example the ZigBee IP coordinator.
- Heavy reconnaissance scans on the 6LoWPAN network can lead to deplete the power supply as they force the sensors to transmit more often.
- The hot-spot problem could still be traced on this layer.
- WSN nodes using IPv6, IPv4 or other type of network layer protocol instead of 6LoWPAN, as this can provoke unexpected behaviors.

The SLAAC configuration in the nodes generates a specific weak point for the 6LoWPAN nodes: *The sensors are very weak against reconnaissance attacks.* Of the 64 bits space, only 16 will be used, and always on the lowest part. Once the node generates a valid address, it will never use another one. Therefore, a reconnaissance attack on the WNS subnetwork would be trivial.

Our threat analysis The following list enumerated a series of DoS attacks that can afflict any type of WSN, with respect of to the network layer [10]:

- DoS neglect and greed: When a malicious node is giving false information to other nodes, trying to trick them to route all the messages to it, as spoofing a sink point, and then just drop the messages or reduces their priority values of the fields if any.
- DoS homing or hot-spot problem: It is possible to localize specific nodes inside of the WSN subnetwork. In other WSN protocols, this can lead to geo-localization as well.
- DoS misdirection and black hole: A malicious node can spoof routes or even pass as a sink point, and then drop all the incoming messages.
- Sybil attacks: defined as a "malicious device illegitimately taking on multiple identities" [6] with the objective of destroying the redundancy for distributed systems, routing algorithm, data aggregation, fair resource allocation and foiling misbehavior detection.

3.3 Discussion

After surveying the literature we conclude that, currently, the best defense against a DoS such as *sybil*, *neglect*, and *greed* attacks is having redundancy paths [10] that RPL is able to provide. However, the hot-spot problem persists [8].

The most effective defense against remote reconnaissance attacks, is avoiding the reconnaissance probes to reach the network by placing proper protection on edge nodes. For reconnaissance attacks that originate inside the network, it is needed to consider the use of other mechanisms, such as IDS and firewalls, or rely completely on the authentication process following the techniques suggested in [10].

The work in [13] suggests that is a good idea to have a strong link-layer protection mechanism such as SEcure Neighbor Discovery (SEND) protocol. Works related to WSN sensors proposed different mechanisms for authentication on this layer, e.g. Tesla, TIK and TRANS [10]. For standardization, the use of the RPL protocol is suggested.

If in the previous layer the authentication of the nodes is not handled the authentication must occur in this layer. The key nodes in this layer, such as the border router, must have a better physical security than the other sensors, if they are lost all the nodes will be jeopardized.

4 Upper layers: Trust and data handling

The standardization, format, and integrity of data are aspects that will be defined in the transport, session, presentation and application layers. The transport layer for the Internet is conformed by TCP and UDP. The 6LowPAN protocol supports both of them and adds a third one called 6LoWPAN UDP (6UDP), which is a constrained version of UDP. *As TCP implies a heavy overhead for the sensors, all the communications inside of the 6LoWPAN subnetwork should be using the 6UDP protocol.* Because of the previous restrictions, the protocol HTTP is not a candidate for the standardization of a secure channel between the sensors and the clients; nevertheless, there exist protocols that are friendly with 6UPD, one of them is the Constrained Application Protocol (CoAP) that, roughly speaking, is the equivalent of HTTP for 6UPD. Additionally, the Extensible Markup Language (EXI) protocol has been selected for the Machine to Machine communications (M2M) between sensors. CoAP and EXI are explained in more detail in 4.1 and are followed by an analysis in 4.2 of the current state of the art for developing trust mechanisms into constrained networks, finally a review in the handling of the data under the IoT environment is made in 4.3.

4.1 CoAP and EXI

Protocols based on the paradigm Representational State Transfer (ReST) have been developed in the last years to reach a reliable communication using an intrinsic unreliable protocol, such as UDP. They are, usually, similar to HTTP but are designed for constrained networks requirements, for instance 6LoWPAN [18]. They are ideal for the M2M communication.

The CoAP is a protocol based in ReST and defined by the IETF [19]. CoAP has the same type of messages as HTTP (GET, PUT, POST and DELETE) making them compatibles. It uses a constrained version of TLS called Datagram Transport Layer Security (DTLS) for achieving confidentiality for end-to-end communication over 6UDP. CoAP helps defining both, the session and the way for sending data. A structured way of representing the data helps to standardize a successful M2M communication. The Extensible Markup Language (XML) has been used for that purpose on traditional devices [18] as well as other structured

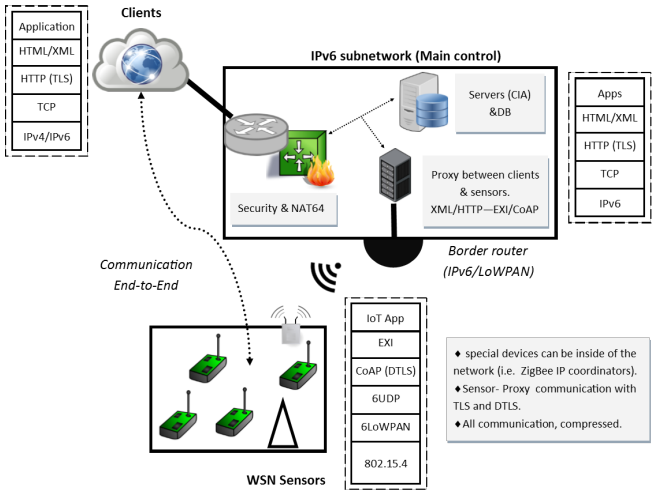


Fig. 5. Representation of one communication ent-to-end

protocols, such as Protobuf developed and used by Google for their own index servers [20]. A weakness of XML is its "verbosity" for defining the data, as it is not ideal for constrained networks. However, the organization W3C released the EXI protocol as a compact representation of XML for constrained environments [21]. ZigBee IP and Contiki have native support for CoAP and DTLS. ZigBee IP has native support for EXI, but Contiki seems not to have it, though the work in [22] has defined an implementation based on the W3 EXI standard [23]. Nevertheless, the work is from 2012 and the definition on [23] has been updated since then.

As stated before, the fully IoT environment need to consider issues well known from typical networks, therefore the IPv6 subnetwork needs to have an access control mechanism and advanced security against attacks. The Implementation of IDS as an option, although implementing one IDS in the 6LoWPAN subnetwork could be challenging. Besides of any other devices that by law or administrative criteria are needed to guarantee a secure performance of the network; and a NAT64 gateway for giving support to clients with only IPv4.

4.2 Analysis of the state of the art on trustiness for IoT

Many well-known mechanisms exist to reach the trustiness of the applications on development. However, the limited resources on the sensors oblige to consider new mechanisms which bring new challenges for achieving the following goals: (i) A Trust mechanism for all the nodes on the IoT environment. (ii) Privacy of the data being transmitted. (iii) A reliable M2M communication between the sensors and other non-human members.

On the other hand, the implementation of more advanced trust management systems for detecting aberrant nodes (those with malfunctions or compromised) and revoking their trust should be considered [5]. However the limitation of the hardware and the memory in the sensors limits this possibility. But at least, a trust management system with authentication, authorization and accounting (AAA) should be implemented. Additionally to the trustworthy nodes, the way in which the node will treat the data and how it will be transmitted are factors that need to be defined. Yet, for the transmission, are required cryptographic techniques but the sensors only have as a valid option the block or stream ciphers due to their limited resources [6].

Trust mechanism Providing the sensors with DTLS guarantee a secure end-to-end communication. Yet, it is no guaranteed that the sensor has the rights to communicate with other nodes.

Other works as [24] suggest to use the authentication mechanisms from real solutions for IP. They suggest Extensible Authentication Protocol (EAP), as well as IPsec with Internet Key Exchange version 2 (IKEv2), Transport Layer Secure with Secure Sokeet Layer (TLS/SSL), DTLS, Host Identity Protocol (HIP) and ID-Moskowitz. But 6LoWPAN does not natively support IPsec and TLS is not optimal in 6LoWPAN. The HIP protocol is an alternative to EAP, an experimental draft defined in the [25] which is intended to be an end-to-end authentication and key establishment protocol, working on the network layer or above. HIP bases its work on special tags of 128 bits and uses DH key management as RSA/SHA1 and DSA. Although HIP was not designed for constrained networks an adaptation called HIP Diet EXchange (HIP-DEX) has been made.

Other works for implementing HIP or HIP-DEX in the IoT are [26–29]. But they are either a specific adaptation, or are focused on RFID instead of WSN, or do not use 6LoWPAN or a mix of those, making them not ideal for standardization. The work in [30] focuses on adapting HIP-DEX to 6LoWPAN, using Contiki as a platform. It operates at the MAC layer, similar to ZigBee IP with PANA, and according to the work, seems to be more efficient than PANA with the use of resources. Yet, they consider that more work is needed to create a more lightweight solution.

HIP and EAP are strong candidates to be used as AAA mechanisms as they are very well known on IP domains. However, an AAA mechanism can be considered as the lowest trust system available. Due to the constraints of the sensors for the IoT environment, many of the best known trust management systems are not available, at least not with the current technology.

Another alternative is the project of Usable Trust in the Internet of Things (uTRUSTit) which has two objectives [31–34]: (i) Create a guideline to identify, produce and manage trustiness on the IoT environments. (ii) Developing the trust feedback toolkit (TFT) which aims to be embedded in smartphones and IoT applications for providing privacy settings and feedbacks to the final user.

In addition to uTRUSTit exists the Social Internet of Things (SIoT) as a change of paradigm to the IoT. With SIoT, the "smart" device "evolves" to "social" device with the objective of fostering resource visibility from the devices [35]. SIoT not only wants the devices to be able to communicate inside of a specific IoT environment, but between multiple environments. Allowing the nodes to interact between themselves, as people do, for delivering data and finding paths [36]. Also, SIoT has developed a trustiness based on social interaction and P2P techniques [37].

The main limitations with SIoT are that all their works are theoretical and only based on simulations. They assume a mix of devices - RFID, mobile devices, sensors, etc. - and the nodes without enough resources can retrieve them from other nodes. Consequently, all the simulations are made without considering the hardware limitations.

In [38] an adaptation to SIoT for adding Quality of Service (QoS) is proposed. Similarly to the original work on SIoT, the testing does not consider the current hardware limitations. Also, 6LoWPAN has removed key elements for QoS, therefore it is needed more work to define how to handle QoS on 6LoWPAN networks. Similar to SIoT, the work in [39] is able to interconnect devices of different environments, however it takes into consideration the privacy of data as a part of Quality of Context (QoC) for defining the trustiness of the nodes. Yet, again, this work is still on simulation and does not consider the current hardware constraints.

Table 1. Comparative of [44] with a TelosB (48Kb ROM, 10Kb RAM, 16-bit RISC MSP 430).

	PreShared	PreRaw	Certificate[1]
% Memory RAM/ROM	56.2/88.5	88.6/139.2	53.0/78.9[2]
Energy requirement (mJ)	0.0002	10.8900	0.0019
Computational time (mS)	3.6	2019.6	21.9
Max packets/sec	132.1	0.49	38.7

In [38] a key management system similar to PANA is proposed, making it redundant. One approach to a fuzzy trust based access control is defined in [40], however, their trust system is a concept tested with only simulations.

There are other works related to the authentication process, as cited in [41, 42] but their implementations are not standardized and several weaknesses in their works can be found. In [41] is proposed an authentication mechanism aimed for mobile devices on IoT, where a pair of public and private keys are generated based on the nodes and their current network, with a third server used for generating the entropy of the keys. However, we have found their algorithm very susceptible to middleman attacks, as the entropy number does not change, and is sent in an insecure way. The work of [42] is an authorization mechanism based in control lists where each node has a list of the privileges for all the existing nodes on the network. If a node gets a message and the receptor is not authorized in the list, the node will drop the message. However, the IPv6 address is the only way to identify the nodes, and even with the 6LoWPAN short version of 16 bits this will deplete the node memory very quickly as can be thousands of nodes. Also, it is possible to bypass this with only changing the source and destination address.

Data privacy CoAP using DTLS guarantee the privacy of the data, due that any pair of nodes is able to configure a unique and temporary symmetric key through the session lifespan. CoAP has four modes for configuring DTLS: `NoSec`, `PreSharedKey`, `RawPublicKey` and `Certificate`. Each one of them operates in different ways and has different scenarios in mind [43]. `NoSec` has DTLS disabled. When using `PreSharedKey` a list of pre-shared keys exists where each key includes a list of nodes. The relation in the list can be used 1:1 to identify each node in the network; the relation can vary for identifying certain nodes as members of specific groups. For this configuration the cipher suite `TLS_PSK_WITH_AES_128_CCM_8` is used.

The `RawPublicKey` mode uses an asymmetric key pairing, without a certificate, that will be validated using the cipher suite `TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8`. For the mode `Certificate`, the protocol X.509 will be used for certifying the keys. This mode also uses the cipher suite as `RawPublicKey` but applying the hash algorithm SHA-256 for the key. Is important to note that previous versions of the SoAP draft stated that the `Certificate` mode should implement the cipher suite `TLS_RSA_PSK_WITH_AES_128_CBC_SHA` instead of the current one.

The work in [44] is focused on identifying the cost of many cryptographic suites for 6LoWPAN networks, including SoAP with DTLS, and their own compression technique: Encapsulated Security Payload (ESP) for 6LoWPAN. ESP uses triple Data Encryption Standard (3DES) and AES with keys of 96 bits, a tradeoff between security and performance of the constrained devices. ESP is discarded because its trade-off is too much for the current technology. Yet, the results of its tests with the 3 modes of DTLS are displayed in the Table 1, although the `Certificate` results are deprecated as they used a previous version of SoAP.

The work in [45] supports the notion of using DTLS, besides they recommend using a Trusted Platform Module (TPM) embedded chip, which performs the RSA algorithm operations in hardware, as is the case for the `Certificate` mode. The chip helps to reduce the times displayed in the Table 1. The TPM also provides hardware protection against tampering attacks, but the price of 20 USD or more per unit and the potential amount of nodes to be used might not be feasible.

Another alternative is suggested in [46] where virtual machines (V.M.) are implemented in the sensors. This is justified as a way to reduce the problem of hardware compatibility, as the application developers will not be concerned anymore about the particulars of the hardware since this is the V.M. duty. However, the use of V.M. comes with the overhead of resources, yet their work suggests that this is a temporary problem, as new and more powerful sensors will become available in the near future. Finally, the DTLS implementation and its performance are not considered in this work.

Data structure How the data get stored on the sensors and servers should follow the already defined standards of privacy, and be subject to the regulations and legal framework of the country where it is deployed. Special emphasis must be given to the IoT, as it has received many critiques due to its potential privacy invasion [47–49]. Different works, as [50, 51] are useful for handling the selection, storage and manipulation of data.

Another alternative is the EXI structure with the works in [20, 22, 52] that have validated its use for constrained devices. EXI uses two different schemes for defining the XML structures: schema-less encoding and schema-informed encoding [18]. The first is generated from the XML data allowing other nodes to decode it without prior knowledge about the structure. The second, by contrast, requires that the nodes share the same XML schema to be able to encode and decode the transmitted data.

There exist other works as [53], which propose changes to the EXI protocol; however, this does not seem to be adequate, since it reduces the wished standardization. In [20] an evaluation of EXI and the Protobuf protocols is made and it is concluded that Protobuf is a better candidate for the IoT, due to its better use of energy and bandwidth optimization. Still, more work is needed for justifying a different approach that risks the standardization.

Vulnerability analysis A wrong use of ports by the application can entail the loss of communication. As the 6UDP is a compressed version, the port address fields are reduced from 16 bits to 8 bits, and under certain configuration to 4 bits. A wrong formatted EXI on any part of the communication could provide fake information to the receptor, risking an unexpected behavior from the sensors or clients.

Our threat analysis The clients and sensors will be communicating in at least two possible ways: (i) sending compatible messages between CoAP and HTTPS or (ii) in some point of the IPv6 network, a translation occurs from one protocol to the other and vice versa. The clients should be able to use a standardized application for requesting the information from the IoT environment, as a web browser. However, this brings many threats from the client side, for instance: (i) the data can be captured from the client application, (ii) arbitrary orders could be sent from or to the client, (iii) Similar to former case, but in huge quantities for provoking a DoS.

[2] As estimated based on the ROM of the devices used on the testing.

[1] Current CoAP draft uses TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 for Certificate and RawPublic.

4.3 Discussion

Although IoT implementations have been appearing since 2001, almost all the work has been made on proprietary protocols, which need special devices for translating from the WSN network to the Internet. The protocols listed in this survey are relatively new, 6LoWPAN was first announced in 2009 and products supporting it began to appear since 2012. Something similar occurs with the ReST protocols, such as CoAP that is still a draft. EXI is from 2007, but it was not designed for the IoT. Therefore, *more work for testing the performance of all those protocols combined is needed.*

In the Fig. 5 is shown a generic model for the IoT environment. The clients have IPv6 or IPv4, and they request the data using a typical HTTP/S communication meanwhile the sensors communicate using CoAP, 6LoWPAN and the 802.15.4 standard. As all the communication and operations occur over the Internet, all the inherited security concerns need to be taken into consideration, such as the ones related to HTTP.

5 Conclusions

The objective of the work is to present a review of the state of the art on the secure design for IoT environments. Taking as a starting point the 802.15.4 standard for the WSN platform, and having as primary concerns the security, trust and privacy of each component of the environment. Emphasis is given to those protocols that let the intercommunication between WSNs and the current Internet (e.g. IPv6). The number of works in the surveyed field is still limited, their achievements are modest, and there is plenty of space to investigate further.

References

1. N. D. N. Enterprise, R. I. G. Micro, Nanosystems, Internet of things in 2020, roadmap for the future, Tech. Rep. Version 1.1. (May 2008).
2. L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, Computer Networks 54 (15) (2010) 2787–2805.
3. K. Haley, 2014 predictions from symantec, http://www.symantec.com/connect/blogs/2014-predictions-symantec-0, accessed: 31/03/2014 (november 2013).
4. F. B. Abreu, A. Morais, A. Cavalli, B. Wehbi, E. Montes de Oca, An Effective Attack Detection Approach in Wireless Mesh Networks, in: 27th International Conference on Advanced Information Networking and Applications Workshops, IEEE, 2013, pp. 1450–1455.
5. J. Undercoffer, S. Avancha, A. Joshi, J. Pinkston, Security for Sensor Networks, Kluwer Academic Publishers Norwell (2004) 253–275.
6. J. P. Walters, Z. Liang, W. Shi, V. Chaudhary, Wireless sensor network security: A survey, Security in distributed, grid and pervasive computingChapter 17.
7. A. Wood, J. Stankovic, Denial of service in sensor networks, Computer 35 (10) (2002) 54–62.
8. N. Vlajic, D. Stevanovic, Performance Analysis of ZigBee-Based Wireless Sensor Networks with Path-Constrained Mobile Sink(s), 2009 Third International Conference on Sensor Technologies and Applications (2009) 61–68.
9. K. Zen, D. Habibi, S. Member, A. Rassau, I. Ahmad, Performance Evaluation of IEEE 802 . 15 . 4 for Mobile Sensor Networks, Tech. rep., School of Engineering, Edith Cowan University, Joondalup, Australia (2008).
10. X. Chen, K. Makki, K. Yen, N. Pissinou, Sensor network security: a survey, IEEE Communications Surveys & Tutorials 11 (2) (2009) 52–73.
11. A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. Pantziou, A survey on jamming attacks and countermeasures in WSNs, IEEE Communications Surveys & Tutorials 11 (4) (2009) 42–56.

12. G. Montenegro, N. Kushalnagar, J. Hui, D. Culler, Rfc 4944: Transmission of ipv6 packets over ieee 802.15, Tech. rep., IETF, accessed 28/04/2012 (September 2007).
13. Z. Shelby, S. Chakrabarti, E. Nordmark, C. Borman, Rfc 6775: Neighbor discovery optimization for ipv6 over low-power wireless personal area networks (6lowpans), Tech. rep., IETF, accessed 28/04/2012 (November 2012).
14. A. A. Hasbollah, S. H. S. Ariffin, J. Bahru, Performance Analysis For 6loWPAN IEEE 802 . 15 . 4 with IPv6 Network, in: TENCON, 2009, pp. 4–8.
15. R. Maley, The new zigbee ip specification: Ipv6 control for low-power, low-cost devices, Tech. rep., 2400 Camino Ramon, San Ramon, CA 94583, accessed 22/04/2013 (abril 2013).
16. T. Winter, P. Thubert, A. Brand, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, R. Alexander, Rfc 6550: Rpl: Ipv6 routing protocol for low-power and lossy networks, Tech. rep., IETF, accessed 23/05/2012 (Abril 2008).
17. C. Gomez, J. Paradells, Wireless Home Automation Networks : A Survey of Architectures and Technologies, IEEE Communications Magazine (June) (2010) 92–101.
18. A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of Things for Smart Cities, IEEE Internet of things 1 (1) (2014) 22–32.
19. A. F. Skarmeta, J. L. Hernandez-Ramos, M. V. Moreno, A decentralized approach for security and privacy challenges in the Internet of Things, 2014 IEEE World Forum on Internet of Things (WF-IoT) (2014) 67–72.
20. N. Gligori, I. Dejanovi, S. Krco, Performance Evaluation of Compact Binary XML Representation for Constrained Devices, in: Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on, IEEE, Baercelona, 2011, pp. 1–5.
21. Efficient xml interchange (exi) format 1.0 (second edition), Tech. rep., W3C, accessed 10/05/2012 (february 2014).
URL http://www.w3.org/TR/exi/
22. D. Caputo, L. Mainetti, L. Patrono, A. Vilei, Implementation of the EXI Schema on Wireless Sensor Nodes Using Contiki, 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (2012) 770–774.
23. Embeddable exi processor in c, Tech. rep., Embedded Internet Systems Laboratory (EISLAB), accessed 10/05/2012 (october 2013).
URL http://www.w3.org/TR/exi/
24. O. Garcia Morchon, S. Kumar, R. Hummen, R. Struik, Security Considerations in the IP-based Internet of Things draft-garcia-core-security-06, Tech. rep., IETF (2014).
25. R. Moskowitz, P. Nikander, P. Jokela, T. Hederson, Rfc 5201: Host identity protocol, Tech. rep., IETF, accessed 23/05/2012 (Abril 2008).
26. P. Urien, S. Elrharbi, D. Nyamy, H. Chabanne, T. Icart, F. Lecocq, C. Pepin, K. Toumi, M. Bouet, G. Pujolle, P. Krzanik, J.-F. Susini, Hip-tags architecture implementation for the internet of things, in: Internet, 2009. AH-ICI 2009. First Asian Himalayas International Conference on, 2009, pp. 1–5.
27. P. Urien, D. Nyami, S. Elrharbi, H. Chabanne, T. Icart, C. Pepin, M. Bouet, D. Cunha, V. Guyot, G. Pujolle, E. Gressier-Soudan, J. F. Susini, Hip tags privacy architecture, in: Systems and Networks Communications, 2008. ICSNC '08. 3rd International Conference on, 2008, pp. 179–184.
28. Hummen, Hiller, Henze, Wehrle, A hip dex compression layer for the ip-based internet of things, in: Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on, 2013, pp. 259–266.
29. D. Nyamy, P. Urien, Hip-tag, a new paradigm for the internet of things, in: Consumer Communications and Networking Conference (CCNC), 2011 IEEE, 2011, pp. 49–54.
30. F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, S. L. Keoh, HIP Security Architecture for the IP Based Internet of Things, 2013 27th International Conference on Advanced Information Networking and Applications Workshops (2013) 1331–1336.
31. C. Hochleitner, C. Graf, D. Unger, M. Tscheligi, Making Devices Trustworthy : Security and Trust Feedback in the Internet of Things, in: Pervasive'12 Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, Newcastle, UK, 2012.
32. W. Leister, T. Schulz, Ideas for a Trust Indicator in the Internet of Things, in: SMART, no. c, IARIA, 2012, pp. 31–34.

33. D. Pietro, Security and Trust Challenges in the Area of IoT, in: INNOSUMMIT, 2012.
34. A. Dunkels, utrustit website, accessed: 11/05/2014 (2013).
URL www.utrustit.eu
35. L. Atzori, A. Iera, G. Morabito, From Smart Objects to Social Objects: The Next Evolutionary Step of the Internet of Things, Communications Magazine 52 (January) (2014) 97–105.
36. M. Nitti, L. Atzori, I. P. Cvijikj, Network navigability in the social Internet of Things, in: 2014 IEEE World Forum on Internet of Things (WF-IoT), Ieee, Seoul, Korea, 2014, pp. 405–410.
37. M. Nitti, R. Girau, L. Atzori, S. Member, Trustworthiness Management in the Social Internet of Things, Knowledge and Data Engineering, IEEE Transactions on 26 (5) (2014) 1253–1266.
38. H. Nasiraee, J. B. Mohasefi, A Novel Three Party Key Establishment Scheme in the Context of Internet-of-Things, in: Information Security and Cryptology (ISCISC), IEEE, Yazd, 2013, pp. 1–5.
39. S. Machara, S. Chabridon, C. Taconet, Trust-Based Context Contract Models for the Internet of Things, 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing (2013) 557–562.
40. P. N. Mahalle, P. A. Thakre, N. R. Prasad, R. Prasad, A fuzzy approach to trust based access control in internet of things, in: Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), IEEE, Atlantic city, 2013, pp. 2–6.
41. An Authentication and Key Establishment Scheme for the IP-Based Wireless Sensor Networks, Procedia Computer Science 10 (2012) 1039–1045.
42. L. M. Oliveira, J. J. Rodrigues, C. Neto, A. F. de Sousa, Network Admission Control Solution for 6LoWPAN Networks, 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (2013) 472–477.
43. Z. Shelby, K. Hartke, C. Bormann, Constrained application protocol (coap) draft-ietf-core-coap-18, Tech. rep., IETF, accessed 23/05/2012 (june 2013).
44. J. Granjal, E. Monteiro, J. S. Silva, On the Effectiveness of End-to-End Security for Internet-Integrated Sensing Applications, 2012 IEEE International Conference on Green Computing and Communications (2012) 87–93.
45. T. Kothmayr, C. Schmitt, W. Hu, M. Br, A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-Way Authentication, in: Local Computer Networks Workshops (LCN Workshops), IEEE, Clearwater, Florida, 2012, pp. 956–963.
46. A. Azzara, D. Alessandrelli, S. Bocchino, P. Pagano, M. Petracca, Architecture, Functional Requirements, and Early Implementation of an Instrumentation Grid for the IoT, 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (2012) 320–327.
47. S. LOHR, The age of big data, New York Times the opinion pages: Sunday Review, accessed 27/05/2014 (February 2012).
48. L. Fried, Minimizing risk is easy: Adopt a bill of rights, New York Times the opinion pages: Room for debate, accessed 27/05/2014 (May 2014).
49. M. Bennett, The internet of things will kill privacy, Website TheInquirerDebate.net, accessed 27/05/2014 (March 2014).
50. J. Sanchez Alcon, L. Lopez, J.-F. Martinez, P. Castillejo, Automated determination of security services to ensure personal data protection in the internet of things applications, in: Innovative Computing Technology (INTECH), 2013 Third International Conference on, 2013, pp. 71–76.
51. O. Vermesan, P. Friess, Internet of things - Converging technologies for smart environments and integrated ecosystems, River Publishers' Series in Information Science and Technology, River Publishers, PO box 1657 Algade 43, 9000 Aalborg, Denmark, 2013, accesed by the EU IoT research website.
52. A. Castellani, M. Gheda, N. Bui, M. Rossi, M. Zorzi, Web services for the internet of things through coap and exi, in: Communications Workshops (ICC), 2011 IEEE International Conference on, 2011, pp. 1–6.
53. Y. Doi, Y. Sato, M. Ishiyama, Y. Ohba, K. Teramoto, XML-less EXI with code generation for integration of embedded devices in web based systems, 2012 3rd IEEE International Conference on the Internet of Things (2012) 76–83.