Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?

Cristina Alcaraz, Pablo Najera, Javier Lopez, Rodrigo Roman
Computer Science Department
University of Malaga
Malaga, Spain
Email: {alcaraz,najera,jlm,roman}@lcc.uma.es

***Abstract*—Wireless sensor networks (WSN) behave as a digital skin, providing a virtual layer where the information about the physical world can be accessed by any computational system. As a result, they are an invaluable resource for realizing the vision of the Internet of Things (IoT). However, it is necessary to consider whether the devices of a WSN should be completely integrated into the Internet or not. In this paper, we tackle this question from the perspective of security. While we will mention the different security challenges that may arise in such integration process, we will focus on the issues that take place at the network level.**

***Index Terms*—Networks; Internet of Things; Internet; Security;**

I. Introduction

In the upcoming Internet of Things (IoT), the everyday objects that surround us will become proactive actors of the Internet, generating and consuming information. The elements of the IoT comprise not only those devices that are already deeply rooted in the technological world (such as cars or fridges), but also objects foreign to this environment (garments or perishable food), or even living beings (plantations, woods or livestock). By embedding computational capabilities in all kinds of objects and living beings, it will be possible to provide a qualitative and quantitative leap in several sectors: healthcare, logistics, domotics, entertainment, and so on.

In fact, one of the most important elements in the IoT paradigm is wireless sensor networks (WSN). The benefits of connecting both WSN and other IoT elements go beyond remote access, as heterogeneous information systems can be able to collaborate and provide common services. This integration is not mere speculation, but a fact supported by several international companies. Noteworthy examples are 'A Smarter Planet' [1], a strategy developed by IBM which considers sensors as fundamental pillars in intelligent water management systems and intelligent cities; and the CeNSE project by HP Labs, focused on the deployment of a worldwide sensor network in order to create a "central nervous system for the Earth". At the same time, the technologies that will enable the integration are being developed and tested. For example, the 6LowPAN standard, defined by IETF [2], allows the transmission of IPv6 packets through computationally restricted networks. Moreover, it is actually possible to link the data produced by the elements of a WSN (sensor nodes) with web services based on SOAP and REST [3], messaging mechanisms (such as emails and SMS) or social networks (e.g. Twitter) and blogs (e.g. Wordpress) [4].

However, having IP connectivity does not mean that every sensor node should be directly connected to the Internet. There are many challenges that must be carefully considered, and one of those challenges is security. While in this paper we will introduce some of the most important security integration challenges (integration of security mechanisms and services, data privacy) we will focus on one specific challenge: the actual connectivity model between the WSN and the Internet. Should sensor nodes delegate all Internet communications to a set of central management systems (e.g. base stations), or should sensor nodes become first-class citizens of the Internet by implementing all the TCP/IP stack plus other standards like web services?

II. Security Integration Challenges

In order to allow WSN to become an intrinsic part of the IoT in a secure way, several security challenges must be considered. As aforementioned, in this paper we focus on the connectivity at the network level. Nevertheless, there are additional security challenges that, even if they are not studied in this paper, must be highlighted to guide future work. These challenges are tightly related to WSN, but also can be applicable to other relevant technologies of the IoT.

Some of the most important challenges are the integration of security mechanisms and users' acceptance [5]. It is essential to consider the security of the IoT from a global perspective and not as a set of isolated issues related to specific technologies. Otherwise, we could reach a point where a technology (e.g. a WSN) satisfies a minimal set of security requirements, but its integration with other technologies (e.g. RFID) generates new requirements which had not been previously considered. Regarding the users perspective, the IoT must be able to satisfy their expectations without betraying their trust. Not only the IoT must be useful, but also users must perceive that they control any information that is related

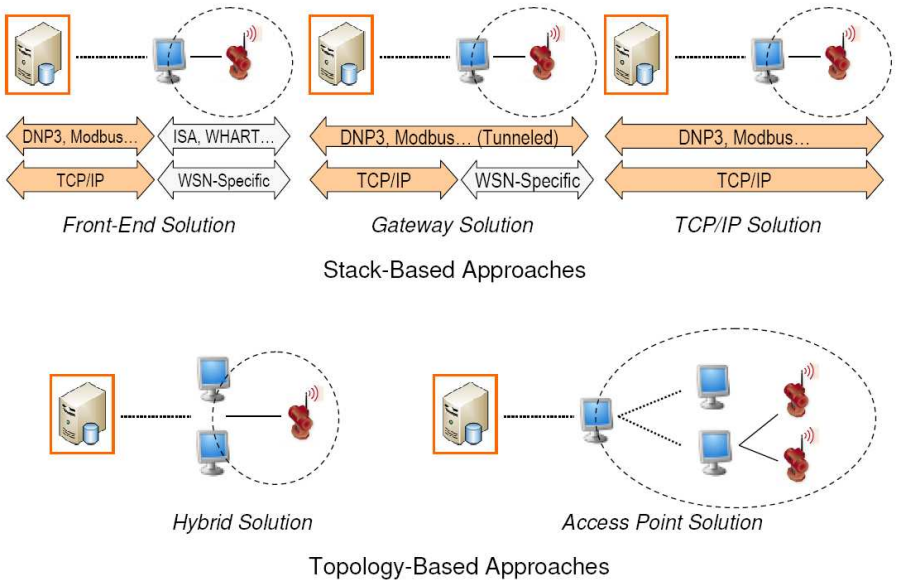

Fig. 1. Integration approaches

to them. If users feel that they are controlled by the system, or they have a false perception of security which is betrayed due to a violation of their rights, any advantage that the IoT can provide will be directly rejected.

Data privacy must also be seriously considered. The information available regarding a particular user will not only consist of his personal data, but also of any data generated by the objects (e.g. sensor nodes) surrounding the individual. In this situation, it is necessary to clarify who owns the data and how the user can be sure that the data is safe and will not be used without his consent. Moreover, there will be some scenarios where part of the data should be shared in order to provide a service. For example, in case of emergency, a person should provide her health data (e.g. personal history and allergies) to the ambulance and medical staff in a transparent way. Beyond individual users, data privacy is also a matter of concern for business scenarios. Any company that makes use of the mechanisms provided by the IoT will generate a huge data flow (e.g. human resources interaction, production processes). Such data must remain confidential, controlled by the company and accessible only when required.

Finally, another significant aspect that must be taken into account is the protection of the components of the IoT by means of adequate security mechanisms. This not only refers to the use of security protocols and mechanisms at the network level (which will be considered in the remainder of the paper), but also to the interactions between objects and services. As the IoT is a distributed, dynamic and heterogeneous infrastructure, it is necessary to combine several technologies, protocols and access models in order to provide services in an appropriate way. From a security perspective, the underlying objects and infrastructures must be able to handle several identification and security mechanisms in a transparent and scalable way. Although there will exist some isolated scenarios (e.g. a digital home, the headquarters of a company) where interactions between objects will be kept under control, there will exist different services (such as logistics) which will make use of several elements geographically dispersed all over the world. Due to this, reaching an equilibrium point in the secure interactions between objects and services is one of the most interesting challenges in the IoT [6].

III. Integration Approaches

From a network perspective, if we want to know whether a WSN should be completely integrated into the Internet or not, it is firstly necessary to know what kind of integration approaches can be used to connect both infrastructures. These approaches, which are shown in Fig. 1 can be classified in two different ways: stack-based [7] and topology-based [8]. In the stack-based classification, the level of integration between the Internet and a WSN depends on the similarities between their network stacks. A WSN can be completely independent from the Internet (*Front-End*), be able to exchange information with Internet hosts (*Gateway*), or share a compatible network-layer protocol (*TCP/IP*). On the other hand, in the topology-based classification the level of integration depends on the actual location of the nodes that provides access to the Internet. These nodes can be a few dual sensor nodes (e.g. base stations) located on the root of the WSN (*Hybrid*), or a full-fledged backbone of devices that allow sensing nodes to access the Internet in one hop (*Access Point*). For the sake of clarity, the different approaches will be explained in the following paragraphs.

In the **stack-based classification**, the first approach is the *Front-End solution*. In this solution, the external Internet hosts

and the sensor nodes never communicate directly with each other. In fact, the WSN is completely independent from the Internet, so it can implement its own set of protocols (e.g. WirelessHART [9] in SCADA environments). All interactions between the outside world and the sensor network will be managed by a centralized device, such as a base station. This base station can store all the data streams coming from the WSN, and it can also provide these data streams to external entities through well-known interfaces (e.g. Web Services [10]). In addition, any queries coming from Internet hosts will always traverse the base station.

The second approach, the *Gateway solution*, considers the existence of a device (e.g. base station) that acts as an application layer gateway, in charge of translating the lower layer protocols from both networks (e.g. TCP/IP and proprietary) and routing the information from one point to another. As a result, Internet hosts and sensor nodes can be able to address each other and exchange information without establishing a truly direct connection. In this solution, the WSN is still independent from the Internet, and all queries still need to traverse a gateway device. However, sensor nodes can be able to provide web service interfaces to external entities while maintaining their lower layer protocols.

As for the third approach, the *TCP/IP solution*, sensor nodes implement the TCP/IP stack (or a compatible set of protocols such as 6LoWPAN [2] in 802.15.4 networks), thus they can be considered as full-fledged elements of the Internet. Any Internet host can open a direct connection with them, and viceversa. In fact, this solution fully integrates the WSN with the IoT. A consequence of this approach is that sensor nodes are no longer able to use specific WSN protocols.

Regarding the **topology-based classification**, the *Hybrid solution* approach considers that there is a set of nodes within the WSN, usually located at the edge of the network, that are able to access the Internet in a direct way. In fact, these nodes can be easily mapped to base stations, since every sensor within the WSN needs to traverse them in order to connect the central system, and viceversa. The specific features of this type of approach are redundancy and network intelligence. By default, this approach considers that it is possible to provide more than one base station to access the functionality of the network. Besides, as those base stations have the capability to connect to the Internet, it means that the intelligence of the network (i.e. the implementation of the different substation protocols) is pushed onto a subset of the WSN.

This delegation of capabilities is further developed in the *Access Point solution* approach. Here, WSNs become unbalanced trees with multiple roots, where leaves are normal sensor nodes and all other elements of the tree are Internet-enabled nodes. As a result, all sensor nodes can be able to access the Internet in just one hop. One of the main features of this approach is the possibility to increase the capabilities of nodes that belong to the backbone network. For example, backbone nodes can have more resources than normal nodes, and can implement faster network standards (e.g. 802.11 vs 802.15.4).

It is important to note that the previously shown topology-based networks are usually combined with the approaches from the stack-based classification. For example, in a backbone-type network, the Internet-enabled nodes can behave i) as a front-end, effectively isolating the WSN sensors from the Internet, or ii) as gateways, allowing direct data exchange between sensors and the central system. There is an exception, though: it is essentially irrelevant to combine the TCP/IP solution with the hybrid and backbone solutions, as every node will be able to connect the Internet. In fact, the only task of the nodes that connect the Internet with the local network will be to behave as translators (e.g. between 6LoWPAN and IPv6).

IV. Demystifying the TCP/IP Solution Issues

After describing the different integration approaches, it would seem that the TCP/IP solution is the best solution to successfully integrate WSN and the Internet. Not only any external system can directly access the information provided by the nodes, but also the nodes are aware of the existence of the Internet and are able to query any of its services. In other solutions, such as the Front-End solution, the nodes can only access those services that are implemented in the central system. However, there are multiple factors that must be taken into account before choosing a certain integration approach.

The purpose of this section is to provide such factors, showing the existing issues that may affect a WSN whose nodes are completely integrated into the Internet. In fact, as mentioned in [7], it is actually more challenging to assure the security of WSN that make use of the TCP/IP solution. We summarize the main factors in the following paragraphs:

- *Resilience.* Any WSN that directly provides its services to external entities are quite vulnerable against attacks. For example, it could be very easy to perform a Denial of Service (DoS) attack due to the throughput of the transmission medium and the capabilities of the sensor nodes. Gateways and sensor nodes must be able to include security mechanisms that increase their robustness against such attacks.
- *User authentication and authorization.* It is essential for some Internet-enabled sensor nodes applications to implement security mechanisms that control who are accessing their services. Storing permissions inside the nodes might be not scalable for long-lived applications, thus it is necessary to consider the implementation of single sign-on systems like Kerberos [11].
- *Security of the communication channel.* It is currently considered that IPsec might be too "heavy" for constrained WSN [12]. Therefore, it is necessary to analyze how other mechanisms such as TLS could be used to offer an end-to-end secure channel. In fact, it is also necessary to study the different key exchange mechanisms that should be used in this context.
- *Accountability.* For an Internet-enabled WSN, it might be interesting to develop a distributed system that is able to record the interactions with the users of the system. By storing all interactions, we can be able to recreate security incidents and abnormal situations.

- *Functionality.* There might be some applications where the sensor nodes do not need to be aware of the Internet. For example, WSN whose tasks are limited to collect information and answer users' queries do not need to contact any Internet service.
- *Hardware.* A specially constrained sensor node might not be able to be directly connected to the Internet due to the memory requirements of the different security mechanisms (e.g. AES-128, Elliptic Curve Cryptography primitives, key negotiation protocols) and the Internet protocols and standards (e.g. HTTP, web services).
- *Inherent weaknesses.* Internet-enabled sensor nodes are vulnerable to many different types of attacks, ranging from DoS attacks to exploit attacks. This particular factor is actually quite important on choosing whether certain applications should completely isolate their sensor nodes from the Internet, filtering all traffic at the edge of the network.
- *Network redundancy.* A group of sensor nodes may offer the same functionality for redundancy purposes, but in a TCP/IP environment an external host will request services from specific nodes through their IP addresses. This means that it is necessary to develop specific mechanisms in TCP/IP environments to deal with exceptional circumstances (e.g. unreachable nodes).
- *Protocol optimizations.* Most WSN-specific protocols include certain mechanisms that allow a network to self-heal itself and to optimize its internal behaviour. These optimizations are yet to be found in 6LoWPAN networks.

V. Case Studies: SCADA Systems and First Responders

We have shown in the previous section that a pure TCP/IP integration solution has certain limitations, mainly in terms of security, that must be taken into account. However, the requirements of the specific applications will finally decide what type of integration solution is more suitable. To assess this statement, we will analyze two sensor network applications: *WSN-enabled SCADA* systems and *First Responder* systems.

A SCADA (Supervisory Control and Data Acquisition) system uses new technologies to monitor in real-time many of the critical infrastructures deployed in our society, such as energy systems, transport systems or oil/water distribution systems (see Figure 2). The main elements of a SCADA system are the central control systems, where human operators remotely monitor the different elements of the critical infrastructure, and the remote substations, which are located within the critical infrastructures themselves and provide the data streams generated by elements of such infrastructures. In other words, remote substations are mainly based on Remote Terminal Units (RTUs) which receive physical data (e.g. pressure or temperature readings) from infrastructures, and transmits the sensed data to the SCADA network using specific industrial protocols, such as Modbus/TCP [13], DNP3 [14] or IEC-104 [15].

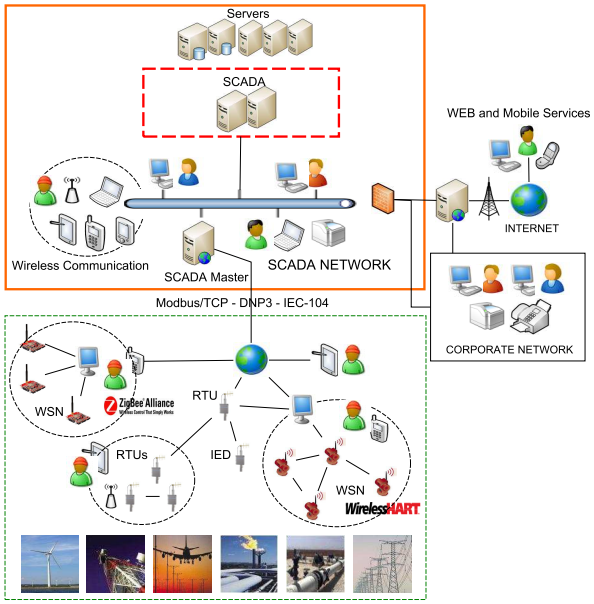

Fig. 2. A current SCADA network architecture

The migration to IP for monitoring and automation has become increasingly popular in this type of industrial sector, since the TCP/IP connections offer real-time monitoring and maintenance processes, peer-to-peer communication (between and among RTUs), multiple sessions, concurrency and security services. In addition, such a migration has meant the design of hybrid networks using the Internet for a remote monitoring and wireless technologies (e.g. Bluetooth, GSM, GPRS, WiMax, WiFi, ZigBee, Ultra-Wideband (UWB), microwave or WSNs) for a local monitoring. More specifically, the Internet can be as the communication link between the control systems and the substations, covering a set of important operational and commercial needs [16], whereas wireless technologies can offer mobility and interoperability at a low installation and maintenance cost [17].

As for the sensing elements of the remote substation, WSN are being increasingly embraced by industrial companies and vendors. These sensor nodes are smart and autonomous devices capable of processing any information acquired from their sensors and transmitting it to a central system with considerable hardware and software resources, such as a RTU working as a data collection device. In addition, they can offer auto-configuration, self-monitoring and self-healing capabilities, as well as detection/tracking of anomalous situations, alarm generation and reporting of any life-threatening situation [18]. These features have involved that WSNs are nowadays considered a key technology for the protection of many of our infrastructures and a suitable alternative of control.

Currently, there are some sensor nodes available in the market for being used in multitude critical and industrial applications. For example, MeshNetics nodes, a leading ZigBee technology provider, released the SensiLink integration

TABLE I
INTEGRATION SOLUTIONS AND APPLICATIONS

	Overview	SCADA	FIRST RESPONDERS
TCP/IP	→ Distributed mechanisms × Device overhead × Weak to external attackers ✓ Resilient to device failure ✓ Direct access to the devices	→ Long lifetime: must support multiple protocols → Devices do not need to be Internet-aware × Critical Environment × SCADA-specific protocols provide extra properties	✓ Short lifetime: deployment-specific protocols ✓ Devices can take advantage of Internet-awareness
FRONT-END	→ Centralized management × Single point of failure ✓ Store and Forward, Redundancy	→ Increase access points to improve robustness ✓ Isolation of the sensor devices	→ No need for redundancy → Extra access points might not be available × Node Isolation might be counterproductive
GATEWAY	→ Mixed Architecture × Single point of failure ✓ Application-Layer access	→ Increase access points to improve robustness → Some intelligence should be pushed to the devices	→ Extra access points might not be available

platform specifically addressed to plug in the data of WSNs into SCADA systems [19]. Electric power systems are feeling the need for real-time wide area monitoring, protection and control and are integrating solutions such as the Cooper Power Systems' wireless Outage advisor [20] to quickly and accurately detect faults and shorten response time. Wireless smart meters such as Sensus' FlexNet SmartPoints [21] are being widely adopted to achieve real-time visualization and advanced warning for power systems, to benchmark, validate and fine-tune system models, as well as to provide real-time congestion management.

The interoperability of all these products is based on recent industrial standards, such as ZigBee [22], WirelessHART [9] and ISA100.11a [23]. Note that, at present, the capabilities of these industrial sensor nodes are very similar to well-known research sensor nodes such as the MICAz [24]. For example, ISA100.11a-ready sensor nodes provide 96kB RAM (containing both instructions and data), 128KB serial flash memory, have 26MHz microcontrollers, and 80KB ROM [25]. Most of these wireless communication standards are based on the IEEE 802.15.4-2006 standard [26], which specifies the physical (PHY) and Media Access Control layer (MAC) layers of Wireless Personal Area Networks (WPANs). The main goal of these standards is to provide secure connectivity assuring energy saving using a wireless mesh network, interoperability with other systems and data reliability.

With respect to First Responders, this term is usually applied to the first individuals who arrive at a disaster scene (e.g. earthquakes, terrorist attacks), such as firefighters and emergency medical technicians. In these particular scenarios sensor networks can play a variety of disaster response roles, such as in-field patient triage, physical environment monitoring, and location tracking [27]. The dynamic and autonomous nature of WSN helps to create and maintain an information infrastructure in situations where other communication and support systems may not be available.

The integration of WSN-based first responder systems with the Internet can provide multiple benefits. The network located at the disaster scene can become a mirror world, helping people visualize distant events and situations [28]. Centralized decision support systems can also acquire such information, using it to gain a global view of a disaster situation and to establish a greater semblance of order [27]. Moreover, the elements of the network located at the disaster scene can interact with the central systems in order to achieve an optimal distribution of the tasks. It is important to point out that the benefits provided by these connected systems can also be used in less critical situations (e.g. car accidents) where first responders also need to act swiftly in order to save lives [29].

Once we have introduced the behaviour of Internet-enabled SCADA systems and First Responder applications, we can discuss the suitability of the existing integration approaches to these particular environments. The results of our analysis are summarized on Table I, together with a general overview of the advantages and disadvantages of every integration solution.

For *SCADA systems*, the actual benefits of using a pure TCP/IP solution for remote substations are not enough to warrant a total integration between WSN and the Internet. The sensing elements of remote substations may not need to know about the existence of the Internet and other substations, since they simply collect data and execute orders from the central system. In terms of security, it is necessary to protect the WSN from any kind of intrusion, as even an increase on the network traffic can become problematic for the sensor nodes due to their limited capabilities. Besides these security issues, there are other aspects in the TCP/IP solution that need to be considered. In particular, a TCP/IP-based WSN will not benefit from the specific optimizations of native WSN protocols like ISA100.11a. Moreover, the capabilities of the sensor nodes may not be enough to implement all the security protocols that can be used during the lifetime of the network (e.g. both transport-layer and application-layer security).

As a result, since SCADA systems do not need of a tight integration model, the Front-End solution and the Gateway

solution can be effectively used to allow external entities to access a SCADA system. The devices can make use of the properties provided by WSN-specific industrial protocols, such as ISA100.11a. In addition, if a device is not available, the gateway can implement different approaches to circumvent this problem, such as store and forward (wait until the device is back and running) and redundancy (access another device that is monitoring the same area). Note, however, that the existence of a central entry point makes this solution vulnerable against availability attacks. This can be solved by using the Hybrid and Access Point solutions (i.e. increase the number of access points to the network), although these solutions have their own specific problems (mainly due to the replication of resources) that must be resolved.

In contrast, the TCP/IP solution is actually quite suitable for *First Responder* systems. By being aware of the existence of the Internet, the elements of the network (e.g. temperature sensors located in patients, sensors worn by K9 - search and rescue dogs) can be able to proactively interact with selected Internet hosts. Besides, as these WSN are short-lived, it is possible to include a limited set of security protocols chosen for a particular emergency situation (e.g. only TLS/SSL), so the overhead on the sensor nodes will be limited. Note that the IP protocol only provides a best effort service, but it can be possible to implement specific protocols at the transport level or the application level to improve the service quality. Besides, the nodes of the network are still vulnerable to external attacks such as Denial of Service, but the risk is lower due to the dynamic nature of the network (i.e. it is short-lived and deployed only when needed) and the limited benefits of these kind of attacks.

The Front-End solution and the Gateway solution can still be used, but the benefits associated to these solutions are not so important in these emergency scenarios. For example, most of the nodes have a unique role, such as tracking the location of a K9. As a result, the only approach that can be used if a node is not available is store and forward. In addition, there are some points that must be carefully considered. As the nodes cannot access the Internet directly, they depend on the existence of the gateway. Due to the dynamic nature of the application, it might not be possible to have multiple gateways in order to improve the redundancy of the network.

VI. Technical Overview

In the previous section we have seen that certain applications need of a direct channel between Internet hosts and sensor nodes, while other applications isolate the WSN behind an Internet server. However, it would be interesting to provide an overview of the current state (as of 2010) of the different technologies that would allow these interactions to happen in a secure way. Firstly, we will state the different security technologies that are used to protect a WSN and its Internet-connected front-end. Secondly, we will provide a small overview of the current efforts on the development of security solutions for Internet-enabled sensor nodes.

A. Front-End Approaches

The research on WSN security is mature enough to provide solutions that can effectively protect the services of the network. Sensor nodes can make use of cryptographic primitives such as AES-128, who have been implemented in software [30] and are also available in hardware. There are also multiple key management systems that can distribute the keys needed by these primitives, providing efficient solutions for different types of applications [31]. In order to provide self-healing capabilities, the reliability and robustness of the WSN can be improved using different types of attestation and detection systems [32]. Other areas, such as secure routing [33], secure aggregation [34], secure time synchronization [35], and trust management [36], are not completely developed, but it is possible to make use of some of their approaches to assure a minimal set of security properties.

In fact, there are multiple WSN security standards that are currently being developed by various international standards bodies. For example, in the Telecommunication Standardization Sector (ITU-T) organization, group SG-17 is developing three recommendations that cover security frameworks (x.usnsec-1), secure middleware (x.usnsec-2), and secure routing (x.usnsec-3) [37]. Moreover, in the International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) organizations, committee JTC 1-SC 6 is preparing another standard that tries to provide a security framework for ubiquitous sensor networks [38]. Observer that all the previously mentioned industrial standards, such as ISA100.11a [23], implement their own security mechanisms provide some protection to the internal information flow.

It would seem that the internal WSN is well-protected against possible attacks. Therefore, it is time to examine the security of the Internet servers, which behave as external interfaces that provide access to the services of the WSN. Obviously, as these devices are full-fledged Internet hosts with no specific constraints, it can be possible to implement all existing standards that provide security from the network layer (e.g. IPsec) to the application layer (e.g. WS-Security). Still, there are some particular issues that must be taken into account. For example, as already mentioned in previous sections, in order to avoid the single point of failure vulnerability, there should be an array of redundant servers (i.e. hybrid solution) that provide access to the same set of services. For example, a server located in the middle of the deployment field could be accessed through 3G cellular networks, providing a backup system in case of failure of the main server. Observe that all these backup servers should provide their services only to authenticated clients. Also, it would be advisable to include a intrusion detection system that limits the number of messages that will launch queries to the WSN.

B. Direct Access

As we have stated in section IV, there are multiple issues that must be thoroughly studied in order to provide security to Internet-enabled sensor nodes. Nevertheless, we can provide here a small overview of the current efforts on this area,

together with some technological advances that could make this vision of an Internet-connected sensor node a reality. One of these advances is the implementation of efficient security primitives for limited devices. For example, some of the stream ciphers developed in the ECRYPT network [39], such as Rabbit, provide good results for sensor nodes [40]. There are also hardware implementations of Public Key Cryptography (PKC) primitives, based on Elliptic Curve Cryptography (ECC), that try to reduce as much as possible the execution time of a point multiplication operation [41]. Moreover, it might be possible to make use of some of the hash functions from the SHA-3 competition in the near future [42].

The implementation of efficient cryptographic primitives is only one of the steps that is necessary to establish a secure channel: it is also necessary to negotiate a shared key between an Internet host and a sensor node. A protocol like TLS can be used for this purpose. In fact, TLS is designed to be used with reliable transport channels such as TCP, but a datagram-compatible variant is also available [43]. However, most of the ciphersuites require of PKC in order to authenticate the server (and the client) and to derive the shared secret, although the negotiation can make use of a pre-shared key by using the TLS-PSK ciphersuite [44]. Still, it would be important to study the suitability of these and other ciphersuites in the IoT context, analyzing their device authentication, computational overhead, resilience and scalability properties.

As for the implementation of other services, there are ongoing standards that try to provide a routing standard for low power networks, such as ROLL [45], and other standards whose major purpose is to implement web services in the sensor nodes themselves, such as the Constrained Application Protocol or CoAP [46]. The security on these standards is being studied and developed as of 2010, and it is still unclear what kind of mechanisms will be used to protect these services. Finally, there are some preliminary works (such as [47]) that tries to develop specific mechanisms that will protect the probably constrained sensor nodes against external attackers. Nevertheless, the actual results on this particular field are insufficient, as it is essential to provide some protection to the nodes (within the nodes themselves or inside the routers / base stations) in order to increase the robustness of the network.

VII. Conclusions

It is clear that the potential of the wireless sensor networks (WSN) paradigm will be fully unleashed once it is connected to the Internet, becoming part of the Internet of Things (IoT). However, it is necessary to discuss whether a full integration at the network level (i.e. using direct TCP/IP connections) should be advisable for every application. After discussing both advantages and disadvantages in the course of this paper, we conclude that some applications should not connect their nodes directly to the Internet (e.g. SCADA systems), but other applications can benefit from using TCP/IP directly (e.g. first responder systems). Note, however, that there are more security issues that must be taken into account when integrating WSN with the IoT, such as integration of security mechanisms and services, users' acceptance, and management of data privacy. Some of these issues have been partially surveyed on this paper, but all of them must be considered in the future in order to make WSN a first-class citizen of the IoT.

Acknowledgment

This work has been partially supported by the Ministry of Science and Innovation through the ARES (CSD2007-00004) and SPRINT (TIN2009-09237) projects. The latter is cofinanced by FEDER (European Regional Development Fund).

References

[1] IBM: A Smarter Planet, http://www.ibm.com/smarterplanet/, Accessed on October 2010.
[2] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks. 2007.
[3] D. Guinard, M. Fischer, V. Trifa. Sharing Using Social Networks in a Composable Web of Things. IEEE International Workshop on the Web of Things, 2010.
[4] Libelium: Interfacing the Sensor Networks with the Web 2.0, http://www.libelium.com/, Accessed on October 2010.
[5] C.P. Mayer. Security and Privacy Challenges in the Internet of Things. KiVS Workshop on Global Sensor Network, 2009.
[6] J. Claessens. Trust, Security, Privacy, and Identity perspective. Panel on Future Internet Service Offer, 2008.
[7] R. Roman, J. Lopez. Integrating Wireless Sensor Networks and the Internet: a Security Analysis. Internet Research, Vol. 19, no. 2, pp. 246-259, 2009.
[8] D. Christin, A. Reinhardt, P.S. Mogre, R. Steinmetz. Wireless Sensor Networks and the Internet of Things: Selected Challenges. 8th GI/ITG KuVS Fachgesprch "Drahtlose Sensornetze", 2009.
[9] HART Communication Foundation, http://www.hartcomm.org/, Accessed on October 2010.
[10] A. Kansal, S. Nath, J. Liu, F. Zhao. SenseWeb: An Infrastructure for Shared Sensing. IEEE Multimedia, Vol. 14, no. 4, pp. 8-13, 2007.
[11] C. Neuman, T. Yu, S. Hartman, K. Raeburn. RFC 4129: The Kerberos Network Authentication Service, 2005.
[12] N. Kushalnagar, G. Montenegro, C. Schumacher. RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, 2007.
[13] Modbus-IDA,The Architecture for Distributed Automation, http://www.modbus.org/, accessed on October 2010.
[14] DNP3,DNP Users Group, http://www.dnp.org, accessed on October 2010.
[15] IEC 60870-5-104, Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles, Second edition 2006-06.
[16] M. Smith: Web-based Monitoring & Control for Oil/Gas Industry, Pipeline & Gas Journal, 2001.
[17] G. Irwin, J. Colandairaj and W. Scanlon, An Overview of Wireless Networks in Control and Monitoring, ICIC, Springer, LNAI 4114, pp 1061-1072, 2006.
[18] J. Lopez, R. Roman and C. Alcaraz, Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Network, Foundations of Security Analysis and Design V , LNCS 5705, pp. 289–338, Springer, 2009.
[19] Meshnetics, Meshnetics Demonstrated Integration of Wireless Sensor Data with SCADA System, http://www.meshnetics.com, accessed on October 2010.
[20] Cooper Power Systems' wireless Outage advisor, http://www.cooperpowereas.com/Products/SmartSensor/SmartSensors.cfm, accessed on October 2010.
[21] Sensus' FlexNet SmartPoints, http://na.sensus.com/flexnet, accessed on October 2010.
[22] ZigBee Alliance, http://www.zigbee.org/, accessed on October 2010.
[23] ISA100, Wireless Systems for Automation, http://www.isa.org/, Accessed on October 2010.

[24] MEMSIC Corporation, Inc. http://www.memsic.com, Accessed on October 2010.
[25] Nivis' VN210 sensor node, http://www.nivis.com/industrial_sensor_networks/VersaNode.php, Accessed on October 2010.
[26] IEEE Standard, 802.15.4-2006. Wireless medium access control and physical layer specifications for low-rate wireless personal area networks. ISBN 0-7381-4997-7, 2006.
[27] K. Lorincz, D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, S. Moulton. Sensor Networks for Emergency Response: Challenges and Opportunities. IEEE Pervasive Computing, Vol. 3, no. 4, pp. 16-23, 2004.
[28] National Intelligence Council: Disruptive Civil Technologies: Six Technologies with Potential Impacts on US Interests out to 2025. Appendix F: The Internet of Things, http://www.dni.gov/nic/confreports_disruptive_tech.html, Accessed on October 2010.
[29] G. Misuraca. Futuring e-Government: Governance and Policy implications for designing an ICT-enabled Knowledge Society, 3rd International Conference on Theory and Practice of Electronic Governance, pp. 83-90, 2009.
[30] S. Didla, A. Ault, S. Bagchi. Optimizing AES for Embedded Devices and Wireless Sensor Networks. Proceedings of the 4th International Conference on Testbeds and Research Infrastructures for the Development of Networks & Communities (TRIDENTCOM 2008), Innsbruck (Austria), March 2008.
[31] M.A. Simplcio Jr., P.S.L.M. Barreto, C.B. Margia, T.C.M.B. Carvalho. A survey on key management mechanisms for distributed Wireless Sensor Networks. Computer Networks, Vol. 54, no. 15, pp. 2591-2612, October 2010.
[32] T. Giannetsos, I. Krontiris, T. Dimitriou, F.C. Freiling. Intrusion Detection in Wireless Sensor Networks. On Security in RFID and Sensor Networks, Auerbach Publications, CRC Press, ISBN: 978-1420068-399, 2009.
[33] J. Ibriq, I. Mahgoub, M. Ilyas. Secure Routing in Wireless Sensor Networks. On Handbook of Information and Communication Security, Springer-Verlag, pp. 553-578, ISBN: 978-3-642-04116-7, 2010.
[34] S. Ozdemir, Y. Xiao. Secure data aggregation in wireless sensor networks: A comprehensive overview. Computer Networks, Vol. 53, no. 12, pp. 2022-2037, August 2009.
[35] A. Boukerche, D. Turgut. A Taxonomy of Secure Time Synchronization Algorithms for Wireless Sensor Networks. On Algorithms and Protocols for Wireless Sensor Networks, John Wiley & Sons, 2008.
[36] F. Gomez Marmol, G. Martinez Perez. Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems. Computer Standards & Interfaces, Vol. 32, no. 4, pp. 185-196, June 2010.
[37] ITU-T Study Group 17, http://www.itu.int/ITU-T/studygroups/com17/, Accessed on October 2010.
[38] ISO/IEC, Joint Technical Committee JTC 1/SC 6, http://www.iso.org/iso/iso_technical_committee.html?commid=45072, Accessed on October 2010.
[39] ECRYPT Network of Excellence. eSTREAM, the ECRYPT Stream Cipher Project. http://www.ecrypt.eu.org/stream/, Retrieved on October 2010.
[40] F. Kausar, A. Naureen. A Comparative Analysis of HC-128 and Rabbit Encryption Schemes for Pervasive Computing in WSN Environment. On Advances on Information Security and Assurance, LNCS 5576, pp. 682-691, 2009.
[41] L. Batina, K. Sakiyama, I.M.R. Verbauwhede. Compact Public-Key Implementations for RFID and Sensor Nodes. On Secure Integrated Circuits and Systems, Springer Science+Business Media, pp. 179-195, ISBN: 978-0-387-71829-3, 2010.
[42] NIST. Cryptographic Hash Algorithm Competition. http://csrc.nist.gov/groups/ST/hash/sha-3/, Retrieved on October 2010.
[43] E. Rescorla, N. Modadugu. Datagram Transport Layer Security. Request for Comments 4347. Accessible at http://tools.ietf.org/html/rfc4347, Retrieved on October 2010.
[44] P. Eronen, H. Tschofenig, Ed. Pre-Shared Key Ciphersuites for Transport Layer Security (TLS). Request for Comments 4279. Accessible at http://tools.ietf.org/html/rfc4279, Retrieved on October 2010.
[45] Routing Over Low power and Lossy networks (ROLL) Working Group. Internet Engineering Task Force (IETF). http://www.ietf.org/html.charters/roll-charter.html, Retrieved on October 2010.
[46] Constrained RESTful Environments (core) Working Group. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/wg/core/charter/, Retrieved on October 2010.
[47] S.O. Amin, Y.J. Young, M.S. Siddiqui, C.S. Hong. A Novel Intrusion Detection Framework for IP-Based Sensor Networks. International Conference on Information Networking (ICOIN 2009), pp. 1-3, April 2009.