Do Wireless Sensor Networks Need to be Completely Integrated into the Internet?

Rodrigo Roman, Javier Lopez, and Cristina Alcaraz

Computer Science Department
University of Malaga, Spain
{roman, jlm, alcaraz}@lcc.uma.es

Abstract. Wireless sensor networks are considered as an integral part of the Internet of Things paradigm. Not only they provide a virtual presence to elements of the real world, but also allow any computational system to know about the physical state of those elements thanks to the use of embedded sensors. In order to belong to the Internet of Things, the elements of a sensor network can implement Internet protocols and services such as the TCP/IP stack and web services. Still, a question that must be raised at this point of time is whether all sensor network applications should be completely integrated into the Internet or not. The purpose of this paper is to analyze this question, reviewing the challenges and security requirements of Internet-enabled sensor networks.

1 Introduction

Not so long ago, wireless sensor networks (WSN) were being presented to the scientific community with small variations of the following sentence: "Recent advancement in wireless communications and electronics has enabled the development of low-cost sensor networks..." [1]. Things have evolved. As of 2009, these networks of constrained devices capable of *living* (by means of batteries), *feeling* (through sensors), *thinking* (using microcontrollers), and *speaking* (via wireless communication) are slowly leaving the research testbeds, providing meaningful services to the real world. Not only these networks have reached some of their expected markets such as environmental monitoring and precision agriculture [2], but also have been applied to specialized industrial environments such as SCADA systems [3].

The evolution is far from over. Sensor networks are considered as an integral part of the Internet of Things paradigm, since they can provide a digital interface to the elements of the real world. This integration goes beyond the traditional view of sensor networks, where multiple sensor nodes that belong to one single domain provide physical information through a central base station system. In this future interconnected world, multiple sensors will be able to dynamically exchange information all over the world in semantically interoperable ways. Note that both the traditional approach and the future sensor networks can coexist at the same time, as there will be applications where more static nodes and dynamic entities can collaborate towards a common goal (e.g. Home environments).

In order to belong to the Internet of Things, sensor nodes must become virtual citizens of the Internet, establishing connections with any other Internet host. Technologies and protocols such as 6LoWPAN [4] will make this dream possible. However, there is one point that must be carefully considered before taking any step: the actual connectivity model between the sensors 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? The purpose of this article is to show that there is no trivial answer to this question when we take into account the security requirements and challenges of Internet-enabled applications.

2 Integration Strategies

It is possible to classify the integration approaches between the Internet and Wireless Sensor Networks in two different ways: stack-based [5] and topology-based [6]. 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 sensor network is completely independent from the Internet, so it can implement its own set of protocols (e.g. WirelessHART [7] in SCADA environments). All interactions between the 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 wireless sensor network, and it can also provide these data streams to external entities through well-known interfaces (e.g. Web Services [8]). 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 sensor network 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 services 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 [4] 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 sensor networks with the Internet of Things. A consequence of this approach is that sensor nodes are no longer able of using specific WSN protocols.

Regarding the **topology-based classification**, the *Hybrid solution* approach considers that there are a set of nodes within the WSN, usually located in 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 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).

3 Choosing an Integration Approach

It would seem that the TCP/IP solution is the best solution to successfully integrate sensor networks 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 strategy, and one of those factors is security.

As mentioned in [5], it is more challenging to assure the security of sensor networks that make use of the TCP/IP solution. In terms of *resilience*, the sensor network is very vulnerable to external attacks that try to exploit the inherent constraints of the nodes and the wireless channel. For example, an adversary can easily perform a DoS attack against the sensor network as the overall throughput of the transmission medium is quite low (e.g. 250 kbps in IEEE 802.15.4 networks). Not only the gateways that route the information to the sensor network must implement new detection rules, but also the sensor nodes themselves must be able to detect and react against possible attackers that try to subvert them.

Another interesting issue that must be considered in the TCP/IP solution is *user authentication and authorization*. As the sensor nodes themselves provide services to any Internet hosts, it is necessary to control who is accessing the information and if it is authorized to do so. While it can be possible to store the user permissions inside the nodes, it would be very complex to maintain the consistency of the network. Consequently, TCP/IP-enabled nodes should be able to use single sign-on systems like Kerberos [9]. Note that certain sensor nodes are still constrained in terms of memory and computational capabilities, thus application designers must be careful when implementing these single sign-on infrastructures.

Regarding the *security of the communication channel*, in the TCP/IP solution it is usually not possible to use IPsec due to constraints on the WSN nodes [10], so it is necessary to use other mechanisms such as SSL/TLS at the transport layer or WS-SecureConversation at the application layer if web services are used. Note that the TCP/IP solution can offer an end-to-end secure channel by using these protocols. Finally, in order to maintain the *accountability* of the system it is necessary to develop a distributed system that is able to record the interactions with the users of the system. By storing all interactions, we can recreate security incidents and abnormal situations.

All the challenges we have mentioned in the previous paragraphs are yet to be solved as of 2009. Nevertheless, it is fairly certain that, in the future, novel security mechanisms will be developed for the TCP/IP solution by the research community. As a result, it will be possible to assure a complete and secure integration between sensor networks and the Internet. However, in certain cases it may not be necessary to aim for a complete integration. In order to understand this point, we have to review certain factors such as the network functionality, the hardware capabilities of the nodes, and others.

The *functionality* of the sensor network plays an important role on the suitability of the integration strategies. As aforementioned, in the TCP/IP solution the sensor nodes can query any Internet service by using standard mechanisms

such as web services. This behaviour is very useful not only in sensor applications that follow the P2P paradigm, but also in any application whose sensor nodes need to know the state of a certain external subsystem. However, there will be some applications where the sensor nodes may not need to be aware of the Internet. For example, sensor networks whose tasks are limited to collect information and answer users' queries do not need to contact any Internet service. In these client/server applications, it may be better to use other integration strategies that do not have the overhead associated to the security mechanisms of the TCP/IP solution.

The *hardware capabilities* of sensor nodes also have an important influence over the integration strategies. Any node that belong to the TCP/IP solution must implement the 6LoWPAN stack, a library of security primitives (e.g. AES-128, ECC-based PKC), security protocols such as TLS/SSL, support for single sing-on mechanisms, and other security mechanisms like detection rules. However, it is not clear whether sensor nodes with limited RAM can afford to implement all these protocols. Moreover, while sensor nodes are increasingly becoming more powerful, it is probable that some types of nodes nodes will maintain their present capabilities in the future due to factors such as cost and node size. As a consequence, in applications whose nodes are not very powerful, the pure TCP/IP solution may not be entirely suitable.

Another factor that must be carefully considered is the *inherent weaknesses* of Internet-enabled applications. As Internet-enabled sensor nodes can be accessed directly by any external host, they are vulnerable to many different types of attacks, ranging from Denial of Service attacks to exploit attacks. In pure TCP/IP networks, all the elements of the network (e.g. the sensor network gateway, the sensor nodes themselves) must be prepared and properly configured to withstand these attacks. Such efforts may be necessary for certain applications, but there might be other applications (e.g. critical environments) where the sensor nodes should be completely isolated from the Internet, with all Internet traffic being filtered at the edge of the network.

Finally, we can mention other factors such as *network redundancy* and *protocol optimizations*. 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). As for protocol optimization, most sensor network protocols include specific 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.

4 A Case Study: SCADA Systems

We have shown in the previous section that there exist certain applications that may not need of the TCP/IP solution to provide their services through the Internet. In this section, we will test our conclusions by analyzing a specific

sensor network application: WSN-enabled SCADA 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. 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.

The Internet can be used as the communication link between the control systems and the substations, covering a set of important operational and commercial needs [11]. As for the sensing elements of the remote substation, wireless sensor networks are being increasingly embraced by industrial companies and vendors. For example, MeshNetics, a leading ZigBee technology provider, released the SensiLink integration platform specifically addressed to plug in the data of WSNs into SCADA systems [12]. All these products are based on recent industrial standards, such as WirelessHart [7] and ISA100.11a [15]. Note that, at present, the capabilities of these industrial sensor nodes are very similar to well-known research sensor nodes such as the MICAz [13]. 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 [14].

Once we have introduced the behaviour of Internet-enabled SCADA systems and the specific protocols and hardware platforms used in remote substations, we will discuss the suitability of the existing integration approaches for this particular industrial environment. Due to the importance of the TCP/IP solution for the Internet of Thing paradigm, this solution will be discussed first, followed by the Front-End solution and the Gateway solution.

The TCP/IP solution guarantees that the WSN located in remote substations are fully integrated with the Internet, but it is not clear whether this can be considered as an advantage or not. Actually, the sensing elements of a 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. Other security aspects like user authentication and authorization have no established solution, but may be solved using mechanisms like Kerberos. 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. Besides, the capabilities of the sensor nodes may not be enough to implement the required protocols. Nevertheless, the TCP/IP solution also have some specific advantages, such as resilience to device failure (i.e. a failure in one node will probably not endanger the whole network).

In contrast, the Front-End solution solves some of the problems of the TCP/IP solution, although it also have issues of its own. Existing standards can be used to implement the security mechanisms, although the existence of a central entry point makes this solution quite vulnerable against availability attacks. This can be solved by using the Hybrid and Access Point solutions, but these solutions have their own specific problems (mainly due to the replication of resources). Another important benefit of the Front-End solution is the use of the WSN-specific optimizations (e.g. if one node is not available, the front-end device can query another one or access an internal cache).

The Gateway solution provides a middle ground between the TCP/IP solution and the Front-End solution. It has some of the Front-End solution benefits (e.g. use of WSN-specific optimizations), and it allows the central system to query the sensor nodes directly. Nevertheless, it also pushes some complexity to the sensor nodes, and it also need to solve certain security details such as the implementation of the authentication and authorization mechanisms. Moreover, the gateway device should parse all incoming messages in order to analyze the queries and to avoid application-specific attacks. Note that this solution can also be combined with the Hybrid and Access Point solutions to obtain benefits such as redundancy, although the specific problems of these solutions (e.g. distribution of tables and resources) need to be taken into account.

From the previous discussions, it would seem that 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 in industrial networks. As control systems simply want to access data streams and to issue control commands, other solutions (e.g. Front-End) combined with approaches that provide extra redundancy may be good enough for the present needs of the industry.

5 Conclusions

The potential of the wireless sensor networks paradigm will be fully unleashed once it is connected to the Internet, becoming part of the Internet of Things. Still, this paper has shown that there might exist certain situation where a full integration (i.e. sensor nodes with the TCP/IP stack, public IP address, and embedded web services) is not needed, as other integration strategies will provide the necessary functionality. Nevertheless, it should be noted that there exist other applications (e.g. dynamic applications with elements that collaborate in a P2P fashion) that will benefit enormously from a full integration approach. Therefore, the research community must consider that every integration approach may become necessary, and work towards the development of Internet-enabled secure sensor networks.

Acknowledgements

This work has been partially supported by the ARES CONSOLIDER project (CSD2007-00004) and the CRISIS project (TIN2006-09242).

References

1. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci. *Wireless sensor networks: a survey.* Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 38, no. 4, pp. 393-422, March 2002.
2. Crossbow Technology, Inc. *eKo Pro Precision Agriculture.* `http://www.xbow.com/eko/`, accessed on June 2009.
3. X. Bai, X. Meng, Z. Du, M. Gong and Z. Hu, *Design of Wireless Sensor Network in SCADA system for wind power plant.* Automation and Logistics (ICAL), pp. 3023-3027, 2008.
4. G. Montenegro, N. Kushalnagar, J. Hui and D. Culler. *RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, Request for Comments, September 2007.
5. R. Roman and J. Lopez, *Integrating Wireless Sensor Networks and the Internet: a Security Analysis*, Internet Research: Electronic Networking Applications and Policy, vol. 19, no. 2, 2009.
6. D. Christin, A. Reinhardt, P.S. Mogre and R. Steinmetz, *Wireless Sensor Networks and the Internet of Things: Selected Challenges*, Proceedings of the 8th GI/ITG KuVS Fachgespräch "Drahtlose Sensornetze", 2009.
7. HART Communication Foundation, `http://www.hartcomm.org/`, accessed on November, 2009.
8. A. Kansal, S. Nath, J. Liu, F. Zhao. *SenseWeb: An Infrastructure for Shared Sensing*, IEEE Multimedia, vol. 14, no. 4, pp. 8-13, 2007.
9. C. Neuman, T. Yu, S. Hartman, and K. Raeburn, *RFC 4129: The Kerberos Network Authentication Service (V5)*, Request for Comments, July 2005.
10. N. Kushalnagar, G. Montenegro and C. Schumacher, *RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*, Request for Comments, August 2007.
11. M. Smith, *Web-based Monitoring & Control for Oil Gas Industry*, SCADA's Next Step Forward, Pipeline & Gas Journal, 2001.
12. Meshnetics, *Meshnetics Demonstrated Integration of Wireless Sensor Data with SCADA System*, available at: `http://www.meshnetics.com/press_releases/MeshNetics_SensiLink_Press_Release_25Jun06.pdf`, accessed on November, 2009.
13. Crossbow Technology, Inc. `http://www.xbow.com/`
14. Nivis' VN210 sensor node datasheet, `http://www.nivis.com/Docs/Nivis_VersaNode_VN210.pdf`, accessed on November, 2009.
15. ISA100, *Wireless Systems for Automation*, `http://www.isa.org/`, accessed on November, 2009.