R. Roman, C. Alcaraz, and J. Lopez, "The Role of Wireless Sensor Networks in the Area of Critical Information Infrastructure", *Information Security Technical Report*, vol. 12, pp. 24-31, 2007.
http://doi.org/10.1016/j.istr.2007.02.003
NICS Lab. Publications: https://www.nics.uma.es/publications

The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protection

Rodrigo Roman, Cristina Alcaraz, and Javier Lopeaz

Computer Science Department - University of Malaga,
29071 - Malaga, Spain
{roman,alcaraz,jlm}@lcc.uma.es

Abstract. Critical Infrastructures, such as energy, banking, and transport, are an essential pillar to the well-being of the national and international economy, security and quality of life. These infrastructures are dependent on a spectrum of highly-interconnected information infrastructures for their smooth, reliable and continuous operation. The field of protecting such Critical Information Infrastructures, or CIIP, faces numerous challenges, such as managing the secure interaction between peers, assuring the resilience and robustness of the overall system, and deploying warning and alert systems, amongst others. In this tapestry of CIIP, Wireless Sensor Networks can be used as an invaluable tool due to their intelligent distributed control capabilities, alongside with their capability to work under severe conditions. In this paper, we justify why Wireless Sensor Networks technology is suitable for providing security for these scenarios, describing both their advantages and research issues and their role in the overall scheme of protecting the Critical Information Infrastructures.

Keywords - *Wireless Sensor Networks, Critical Information Infrastructure Protection, Network Security*

1 Introduction

The challenges on protecting a Critical Information Infrastructure are numerous and complex, since they are composed by highly interconnected national (and international) software-based control systems where a single isolated disturbances can cascade through the system with unexpected consequences. It is then indispensable to have a resilient and robust information infrastructure that could deal with any situation and assure the security of the information, which is of critical importance from a political, economic, financial or social standpoint. It is also important to provide a monitoring system that can issue alerts and warnings even if a problematic situation has yet to occur. Besides, it becomes imperative

to create models and simulations that could show how the system should behave in presence of problems, avoiding problems in upgraded systems that could hinder the continuity of the services.

One of the technologies that can be applied for protecting those critical information infrastructures are wireless sensor networks (Akyildiz et.al. (2002)). A Wireless Sensor Network can be abstracted as the "skin" of a computer system, where hundreds or thousands of inexpensive nodes are able to sense the physical events of their surroundings. Since a sensor node is independent, has computational capabilities, and is able to communicate with its surroundings using a wireless antenna, it is possible to use the network as a redundant and resilient system that can provide, either continuously or when needed, an accurate diagnosis of a certain context. Even more, it can also provide the foundation of an intelligent distributed control system.

It is on these final points that this paper will concentrate, arguing that while there are some research issues that a sensor network must face in order to protect a critical information infrastructure, it does provide interesting and essential protection properties due to their intelligent distributed control capabilities alongside with their capability to work under severe conditions. The paper proceeds to show what is the general concept of critical information infrastructures and its protection, together with the actual state of the art and research issues, in section 2. The paper then introduces the concept of wireless sensor networks, providing a survey on the hardware platforms and the most important applications, in section 3. An study of the suitability of sensor networks as an technology for CIIP is presented in section 4, followed by an analysis of the existent research issues in section 5. Finally, the paper shows its conclusions in section 6.

2 CIIP and Challenges

According to the European Commission, *Critical Infrastructures* consist of *"those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical Infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services"* (EC (2004)). These infrastructures depend on a spectrum of highly in-

terconnected national (and international) software-based control systems for their smooth, reliable, and continuous operation. This information infrastructure underpins many elements of the aforementioned Critical Infrastructures, and is hence called *Critical Information Infrastructures* (CII). As a result, key sectors of modern society that are vital to the national security and the essential functioning of industrialized economies are dependent of the well-being of these CII, making Critical Information Infrastructure Protection (CIIP) a priority.

CII usually requires multiple high-data-rate communication links, a powerful central computing facility, and an elaborate operations control center. The operations of these elements are characterized by unique requirements for communications performance, including timing, redundancy, centers control and protection, and equipment control and diagnostics. Unfortunately, CII are susceptible to a wide array of disturbances. Its communication links and control centers are especially vulnerable when they are needed most - during serious system stresses or disruptions. And the interconnected nature of networks means that single, isolated disturbances can cascade through and between networks with potentially disastrous consequences.

Therefore, it is indispensable to have a resilient and robust information infrastructure that could deal with any situation, being a physical or computational attack to the system or an abnormal behavior of any component inside the overall system. Not only the robustness of the services has to be assured at all times, but also the security of information, which is of critical importance from a political, economic, financial or social standpoint, must be guaranteed. On this issue, adding Information Security provisions such as authorization, authentication, encryption, and other basic security services is not enough to manage these complex scenarios and applications, due to the complex and dynamic nature of these infrastructures. Thus, it becomes strongly necessary to provide advanced security technologies, such as a set of policies and methods to allow an effective and secure interaction of the elements of a CII, both internal and external.

Independently of the source and dimension of the problem, the infrastructure has to be able to issue alerts and warnings in order to help both human users and the information subsystems to react against any possible abnormal situation. Avoiding a problematic situation once it has happened is not enough for protecting the system, though. It is an essential part of any CIIP to monitor the state of the systems and issue an early warning in case a certain subsystem gives symptoms of an ab-

normal situation that has yet to occur. In order to correctly model these type of decision-making tools, it is also of vital importance to analyze an infrastructure and quantify the possible problems that could happen. As a result, it will be possible for the information infrastructure and its human operators to accurately react and protect itself in real time, assuring the seamless continuation of its services.

The protection of a CII must not be limited to the safeguard of a fully functional system. It is crucial to assure that the information infrastructure and its response mechanisms will be able to work under any kind of context both before its deployment and after any kind of modification. However, it is usually not feasible to test and obtain results about a CII without endangering the operation of the entire system itself, because in most cases the services provided by such system must be provided continually, and they can not be disconnected or modified without affecting their ongoing operations. Therefore, it becomes imperative to create models and simulations that could show how the system, either unmodified or upgraded, should behave in presence of problems.

2.1 CIIP Research Issues: State of the Art

Although CIP/CIIP have attracted the attention of governments and international organizations due to their importance in the actual socio-economic context, it is only recently when specific actions have been taking place, such as the funding of many CIIP-related research projects and the explicit consideration of this topic in the 7th European Framework Programme (FP). However, there is not yet a real community of researches and experts working on this field, even if there is an increasing large number of actors. This is partially because of the absence of a clear policy about CIP/CIIP and a clear vision of what "concretely" are CIP/CIIP, their goals, constraints and boundaries (Bologna et.al. (2006)).

Despite these barriers, there are many identified research topics and open issues that have to be solved in order to provide the foundations of a secure and robust critical information infrastructure, as seen in the previous section. Moreover, as it is easy to figure out, the challenges in this field are influenced by its interdisciplinary nature, where problems in individual and homogeneous systems, that can feature a large number of legacy subsystems and non-computer standard components such as controllers and actuators, evolve into complex problems in heterogeneous environments. In such heterogeneous environments, it is crucial to provide a set of policies and methods to allow an effective and secure interaction of the elements of a CII, both internal and external. In the

literature we can find works focusing on the creation of high-level policies (Hammerli (2005)) or the creation of an architecture for interconnected realms (Verissimo et.al. (2006)), but little research has been put into areas such as the security policies of a CII.

On the other hand, resilience and robustness are important matters of a CII. Every part of the system and the infrastructure as a whole must be resilient and robust against any type of problem or attack, and must be able to react and protect itself in real time. There are some tools that can help in the mitigation of these problems by alerting and helping the human user (Carlier et.al. (2003)), and solutions like Intrusion Detection and Recovery Systems could also be of use, although they are underdeveloped in this context with minor exceptions (D'Antonio et.al. (2006)). A key mechanism that, amongst other things, can help the previous tools to distinguish what are the attacks it may face is risk assessment - the process of analyzing an infrastructure and quantify the possible problems in order to correctly model the protection systems. At this moment, risk management and quantification in CII are in a very early stage, and only recent works are available in the literature (Sahinoglu (2005)) (Adar, Wuchner (2005)).

Alerts and Warnings are also an essential piece of a resilient and robust infrastructure, since they help the human user and the information system to react against possible difficult situations before (or after) they occur. This is a hot topic that will be greatly useful for a CII, allowing the generation of advanced systems such as Early Warning Systems and Dynamic Reconfiguration Systems. Last, but not least, it is important to point out that the knowledge of the structure and behavior of the individual elements of the CII does not mean a complete understanding of how the CII could work as a whole. Simulating and analyzing these large and complex systems is a real challenge because of their nonlinear and time-dependent behavior. Furthermore, these simulation environments are necessary, because it is usually not feasible to test and obtain results about a CII without endangering the operation of the entire system itself. Although there are a couple of interesting works in the literature, this is not a well-developed topic yet (Rinaldi (2004)) (Wolthusen (2004)) (Schmitz (2003)).

3 Wireless Sensor Networks

The advances on miniaturization techniques have made possible the development of a new network paradigm, the *Wireless Sensor Networks*

(WSN). The main purpose of a Wireless Sensor Network as a whole is to serve as an interface to the real world, providing physical information such as temperature, light, radiation, and others, to a computer system. These type of networks have a simple structure: there are dozens or hundreds of elements, called "sensor nodes", that are able to sense the physical features of their surroundings. After such information is processed by these nodes, it is sent through a wireless channel to a central system, called "Base Station". It is possible to abstract the nodes as the "sensing cells" of a living system, where the base station can be considered as the "central brain".

One of the key advantages of wireless sensor networks consists on the capabilities of their sensor nodes. All sensor nodes are powered by batteries, but they can subsist long periods of time (e.g. a year) if configured correctly. Moreover, although constrained, they have sufficient computational and storage capabilities (e.g. a 8 Mhz microprocessor with 1 Megabyte of Flash memory). As a result, they are totally independent and are able to act autonomously if the context requires them to do so, collaborating with other nodes in pursuing a common goal using their wireless channel. Even more, thanks to their potential to self-configure themselves, it is an easy task to set up a sensor network in a physical context where it is needed without needing any previously existent infrastructure.

The services offered by a WSN can be classified into three major categories: Monitoring, Alerting, and information "On-Demand". Sensor nodes can continuously monitor certain features of their surroundings (e.g. measuring the radiation level). Sensors can also check whether certain physical conditions (e.g. a radiation leak) are taking place, alerting the users of the system if an alarm is triggered. Finally, the network can be queried about the actual levels of a certain feature, providing information "On-Demand". It is important to note that the computational capabilities of the nodes allows to automatically reconfigure their internal operation during the lifetime of the network, or even use them as a distributed computing platform or communication platform under extreme circumstances.

It has been pointed out that the users of the network, being human beings or a computer infrastructure, will not directly access to the information coming from the sensor nodes. Instead, they will use the Base Station as an interface for accessing to the services provided by the sensor network. If the Base Station is not present due to power failure or other issues, the sensor network is independent enough to continue pro-

viding its services without any problem, although there will be no point of access to immediately use those services. However, it is still possible to have more than one base station for redundancy purposes. Additionally, it is still possible to use a PDA-like device handed by a human user with the purpose of accessing to the information of the network on the spot, or to have an fully independent device working as a Base Station that positions itself to obtain samples of the environment based on the information supplied by the sensor nodes.

On a more technical point of view, sensor networks have two basic architectures, called hierarchical and flat, that specify how the sensors group themselves for achieving their goals. In flat configurations, all the nodes participate in both the decision-making processes and the internal protocols, like routing. On the other hand, in hierarchical configurations the network can be divided into clusters, or group of nodes, where all the organizational decisions, like data aggregation, are made by a single entity called "cluster head". Notice that it is also possible to have a mixture of the two previous configurations in the same network, for example to avoid situations where the "spinal cord" of the network - the cluster heads - fails to work and the information must be routed to the base station.

3.1 Hardware Platforms

At present there are many types of sensor nodes in the market, mainly because a sensor network must be highly specialized to work in a certain application context, and its sensor nodes must be highly optimized for this very purpose. However, sensor applications nowadays are not used in production environments, being restricted to research purposes. As a result, there is still some room for improvement in this market, as companies continue to develop new and better prototypes.

The main components of a sensor node are its microprocessor, its communication chip, its integrated sensors, and limited mass storage. It is also possible to have support for external components, such as GPS chips or external flash cards, or a better security support, like radio chips with hardware implementations of cryptography mechanisms such as AES. It would seem a simple task to improve the characteristics of any these components, creating better sensor nodes with more capabilities. However, the hardware designers must achieve a balance between the resources of the nodes, the energy they spend while functioning, the overall cost of the node, and the expected functionality of the node inside a certain context and application. Therefore, most hardware platforms are specialized on providing certain functionality to the network at a reasonable cost.

For example, for hierarchical networks in critical environments, the nodes belonging to a cluster just need to sense their environment and securely send its information to a cluster head. There are many types of nodes that can do this type of job, and we can highlight two of them due to their lower costs: TMoteSky (Moteiv Inc. (2007)) powered by an MSP430F1611 microprocessor (16 bit, 8 Mhz, 10KB RAM, 48KB memory) and a Chipcon CC2420 radio chip (operating on the 2.4Ghz band), and MSB (Scatterweb GmbH (2007)) powered by a MSP430F1612 microprocessor (16 bit, 8 Mhz, 5KB RAM, 55KB memory) and a Chipcon CC1020 Radio Chip (operating on the 433/868 MHz bands).

Once the hardware of the nodes belonging to a cluster are selected, it is time to choose the node that can be the cluster head. Such node can be slightly more powerful than the other nodes since it is supposed to do more kinds of computations, although the previously presented nodes (TMoteSky by Moteiv Corp. and MSB by ScatterWeb GmbH) have enough resources for this purpose. Other nodes like the MicaZ/Mica2 family (powered by an 8 bit Atmel 128L with 8 Mhz, 4KB RAM, 128KB memory) (Crossbow Inc. (2007)), or the zPart/pPart family (powered by a 8 bit PIC18F6720 microprocessor with 20 Mhz, 4KB RAM, 128KB memory) (Particle Computer GmbH (2007)) can be also effective. In case the cluster head has to be an extremely powerful node, the SunSpot (Sun Microsystems Inc. (2007)) provides better capabilities (an ARM920T core with 180 Mhz, 512KB RAM, 4MB memory) at a slightly higher cost.

On the other hand, if a sensor network follows a distributed configuration, it is necessary that all the nodes have enough resources for sensing their environment and securely processing the data at a moderate price. Nodes like TMoteSky and MSB that are able to sense simple features of the physical environment such as light can be up to the task. In sections of the network where the nodes have to be equipped with a bigger array of sensors, it is possible to use nodes such as the pPart/zPart family or the Mica2/MicaZ family. Lastly, notice that not all nodes work in the same radio band (2.4Ghz band for the CC2420 radio chip or 433/868 MHz bands for the CC1000/C1020 radio chip), thus the network designer must choose what type of nodes is going to use based on the bandwidth requirements of its applications.

3.2 Applications

The number of scenarios where sensor networks can be used is specially broad. Generally speaking, WSNs can be used in applications where sensors are unobtrusively embedded into systems, consequently involving

operations like monitoring, tracking, detecting, collecting or reporting. Such applications can range from simple systems like measuring the environmental situation of a household to critical applications like monitoring the health of workers and the robustness of the infrastructures of a coal mine.

One of the biggest applications of sensor networks is in agricultural scenarios, and more concretely, in the wine production industry (Beckwith et.al. (2004)), where sensor nodes can detect physical events such as broken sprinklers, heat accumulation, and signs of a future frost. Sensor Networks are not limited to simply monitor a controlled environment, though: they can monitor natural phenomenons such as volcanoes (Werner-Allen et.al. (2006)), the state of a glacier (Martinez et.al. (2006)), or the coastal effects of a windfarm (Wokoma et.al. (2005)).

Another well-known application of sensor networks is in militar scenarios. Since sensor nodes can be easily deployed in either controlled or uncontrolled environments, they can be able to detect, locate and track targets over long periods of time. For example, a number of sensor nodes can locate a certain target and alert the pursuer of the actual location of that evader (Sharp et.al. (2005)). In another example (He et.al. (2006)), the nodes can be deployed along a long perimeter which would represent a typical choke or passageway, where they can cooperatively detect, track, and identify different targets of interest while activating more powerful sensors such as cameras.

It is also possible to use sensor networks in Healthcare, for helping assisted-living and independent-living residents by continuously and unobtrusively monitoring health-related factors such as their heart-rate, heart-rhythm, temperature, and others. It is also possible to monitor the status of a patient in other environments, such as an hospital or an ambulance (Harvard Univ. (2006)). Sensor networks can also be used in other Ambient Intelligence Scenarios, such as smart offices (Minder et.al. (2005)). In these smart offices, it is possible to record the movement and meeting patterns of employees, and also answer queries related to the employees (such as their location) and related to the rooms (such as their temperature).

4 Role of Sensor Networks in CIIP

Both the scientific community and the governments around the world have recognized the importance of Wireless Sensor Networks as an integral part of the protection of Critical (Information) Infrastructures. The U.S. De-

partment for Homeland Security stated, in the 2004 National Plan for Research and Development in Support for CIP (U.S. Goverment (2005)), that one of the strategic goals was *"to provide a National Common Operating Picture (COP)"* for Critical Infrastructures, where the core of the systems would be an intelligent, self-monitoring, and self-healing sensor network.

On the other hand, the Australian government, through the Research Network for a Secure Australia (RNSA), launched a major R&D initiative called the Cooperative Research Center for Security (CRC-SAFE) that aims to develop research and commercialization opportunities for CIP in Australia. One of the research programs of that initiative, Electronic Systems Security, is examining and developing solutions to security problems that arise in systems that are utilized in the critical infrastructure environment, including Wireless Sensor Networks (Bopping (2006)).

There are also plenty of research efforts and prototypes in the academia dedicated to use sensor networks as an integral part of both Critical Infrastructure Protection and Critical Information Infrastructure Protection. Related to Infrastructure Monitoring, Intel (Intel (2006)) conducted an experiment to monitor the health of its semiconductor fabrication equipment in one of its plants in Oregon, specifically by sensing the vibration signature of the water purification equipment and providing it as an input for early warning systems. The Research Council of U.K. (EPSRC) has also started funding two projects, Underground M3 and Smart Infrastructure (Soga (2006)), related to develop a low-cost smart sensing environment for monitoring ageing public infrastructure, such as water supplies and sewer systems, tunnels, and bridges.

A wireless sensor network can be also used for detecting and reacting against problems in safety-critical infrastructures, such as oil rigs and water-treatment plants. An example is the DISCOVERY (Distributed Intelligence, Sensing and Coordination in Variable Environments) project (CSIRO (2006)), that aims to create fully autonomous underwater sensor networks that are able to protect these critical infrastructures by tracking oil spills to their sources and establishing absorption perimeters. About water quality monitoring, the University of California, Los Angeles, is involved in two projects (Ramanathan et. al. (2006)) related to groundwater quality: a system to understand the prevalence of arsenic in Bangladesh groundwater, and a system to monitor nitrate propagation through soils and ground water in California.

Since a sensor network can be easily set up in the same places where the existent sensors of a previously deployed CII system are located, it

is also possible to automatically create an information network which allows the system administrators to discover and take measures against any anomalies in the actual sensing system. This is one of the aims of the SMEPP project (SMEPP (2006)), where sensors will be able to help in measuring physical events such as the ambient noise or the radiation levels. Another application derived from the previous one is to use these networks as a self-powered redundant communication and diagnosis system, able to route both internal information about a malfunctioning control system and information about its physical environment to any living system.

4.1 Applicability

As seen before, sensor networks play a fundamental role in the protection of critical infrastructures. Thanks to their ability to work under severe conditions, They can provide a robust and self-reactive network that is able to continuously monitor any kind of physical event of an infrastructure, such as vibration, humidity, radiation, or others. Also, in case the infrastructure starts to fail, the sensor network can provide the exact location and extent of the problem, helping to solve the situation in a short period of time.

The role of sensor networks, however, does not end in the protection of critical infrastructures. They are useful in the protection of critical information infrastructures, as well. This technology facilitates the existence of an redundant and resilient control system, allowing the different components of the network to remain operative, even in crisis situations. In other words, it does provide the foundation of an intelligent distributed control system, both monitoring and supervising parts of the system even in situations where there is no central management available.

The data provided by the network that monitors both the infrastructure and the systems that control the infrastructure can also be used for providing an accurate diagnosis of a certain context, detecting the events previous to a dangerous situation by feeding systems such as Early Warning Systems. Not only that, but it is also possible to use the events generated by the EWS as an input for Dynamic Reconfiguration Systems (DRS), which are capable of re-configuring the different components of the CII in an automatic way. Surely, the redundant and resilient information provided by the sensor networks will help a system to react accurately against serious stresses or disruptions.

Moreover, due to its computational and wireless capabilities, a Sensor Network can be easily set up in a physical context where it is needed,

being extremely useful for controlling and diagnosing any previously existent equipment. For example, in case a control system is faced with a serious disruption that renders the operation of its subsystems unusable, a sensor network can be deployed "on the spot" for providing reliable and robust information about the physical infrastructure or the status of any component. Such sensor network can also be used for diagnosis purposes, comparing the actual values returned by a fully functional control system with the values acquired in real time by the network.

5 Research Issues on Sensor Networks

5.1 Sensor Network Development and Security

Since sensor networks is a young technology, there are many research problems that need to be solved, such as models and tools for designing better WSN architectures, standard protocols adapted to work robustly on certain scenarios, and so on. At present, the "de facto" standard Operative System for sensor nodes is an open source OS called TinyOS, which provides limited support for network and protocol simulations. The preferred programming language for developing applications in this environment is a component-based C-dialect called nesC, but it is also possible to use other languages in other OS, such as C for the MSB nodes and Java for the SunSpot nodes.

Another concern in the development of sensor network applications is the lack of a standardized set of core protocols, which could be used for providing the services of the network in a certain context and application. These core protocols are routing, data aggregation, and time synchronization, and the service they provide are the ability to route a packet from a node to another node, to summarize many sensor readings into one single piece of data, and to synchronize the clocks of the network, respectively. The specific problem in this area is not the lack of protocols developed by the research community, but the lack of a set of tested solutions that could work robustly in a production environment.

However, the biggest issue that a sensor network in a production environment has to face is security. Sensor nodes are highly constrained in terms of computational capabilities, memory, and battery power. In addition, the nodes can be physically accessible by anyone because they must be located near the physical source of the events, but they usually are not tamper-resistant due to cost issues. Moreover, the communication channel is public and any device can access to the information exchange. As a result, any malicious adversary can manipulate the sensor nodes, the

environment, or the communication channel on its own benefit. It is then necessary to provide the sensor network with basic security mechanisms and protocols that will assure a minimal protection to the services and the information flow.

On the hardware layer, nodes neither have tamper protection nor are enclosed on a tamper-resistant package. Fortunately, the time and effort of subverting a node is not trivial (Becher et.al. (2006)). Even more, there exists certain mechanisms that allows a better protection of the node. For example, it is possible to use *data and code obfuscation* schemes that are able to generate different and harder-to-break versions of the sensor software for each node (Alarifi, Du (2006)). Moreover, although a node cannot protect itself, it is possible for others to check its state using a procedure called *code attestation* (Park, Shin (2005)).

Regarding the communication flow, the nodes must be provided with the basic security primitives that would authenticate the peers involved in the information exchange while protecting the confidentiality and integrity of the channel. Those primitives are *symmetric key encryption* schemes (SKE), *message authentication codes* (MAC), and *public key cryptography* (PKC). It has been a challenge to implement those security primitives, specially PKC, in the existent sensor nodes, but the state of the art in these areas is quite advanced. There are software-based SKE, like TinySec (Karlof et.al. (2004)), that can provide block ciphers such as Skipjack or RC5 in CBC mode with a minor overhead - less than 10%. MAC computations usually takes advantage of the existing SKE primitives, so they do not pose a problem. And it has been possible to implement PKC on sensor nodes (Liu, Ning (2006)) by using elliptic curve cryptography (ECC).

A problem associated with the existence of the security primitives is the need of having a key management system (KMS). The security primitives need certain security credentials, i.e. pairwise secret keys, in order to work, and the KMS is in charge of creating and providing these keys, hence constructing a secure key infrastructure. There have been multiple KMS suggested by the research community that allows two neighbouring nodes to share a secret key. Fortunately, it is possible to deduce which KMS is more suitable for a certain context (Alcaraz, Roman (2006)), by analyzing if the properties offered by a certain KMS matches with the requirements of the scenario where the nodes are going to be deployed.

The security of a sensor network is not assured by just protecting the communication channel between two nodes. The core protocols of the network must be secure enough to withstand both errors coming

from faulty nodes and attacks initiated by malicious elements outside and inside the network. There are multiple attacks that can be performed against these core protocols (Karlof, Wagner (2003)) (Sang et.al. (2006)) (Manzo et.al. (2005)). The field of time synchronization is fairly advanced, existing many protocols able to provide that service in a secure way. Unfortunately, this is not the case with routing and aggregation. On the other hand, this area of research is advancing at a steady pace.

There are other security issues that need to be addressed, such as secure management of mobile nodes and base stations, robust and secure location methods for the nodes, data privacy, trust management, delegation of privileges, intrusion detection systems, and many others. While it would seem that there is a long way until it is possible to make a completely secure sensor network deployment, the foundations of a secure system (such as security primitives, key infrastructures, and basic protocol mechanisms) are almost done. In addition, the research community working in this field is very active, thus it is expected to have new and exciting results in the future.

5.2 Sensor Network Interoperability

It has been shown that sensor networks are useful elements in the global picture of protecting a critical information infrastructure, since they can provide the foundation of a robust and self-reactive intelligent distributed control system, be used for controlling and diagnosing any previously existent equipment, or used as an event feeder for Early Warning Systems or Dynamic Reconfiguration Systems (DRS). It is an open question, then, how to integrate these sensor networks with CII in order to provide all these protection services. This problem is actually being addressed by the CRISIS (CRitical Information Infrastructures Security based on Internetworking Sensors) project (Lopez et. al. (2006)).

At a low level, it should be necessary to define and design the software components located in the sensor nodes needed to provide basic mechanisms for the creation of security services. These software components should allow the deployment of the control infrastructure, the efficient access to the information acquired by the sensors system and adjacent subsystems, and the secure access and control of the behavior of the network. On the other hand, at high level it should be obligatory to specify mechanisms for providing an appropriate interoperability of the elemental mechanisms, establishing the foundation of the sensor network as a Service-Oriented Architecture (SOA). This requires the correct specification of the associated middleware and the creation of security policies

and interfaces for the interchange of information. Finally, it is important to design mechanisms for facilitating the interoperability among the different services, external or internal to the network.

Regarding the Security services, the SOA should provide Advanced Authentication Services for the authentication of each of the elements of the network, Authorization Services for controlling how resources are used, and Delegation Services for assuring the scalability of the authentication process. These three services and the existence of a trust management model allow the definition of essential composite services such as Information Sharing, Aggregation, and Privacy. Once these composite services are included into the framework, it can be possible to provide a secure control system with monitoring and maintenance services, such as Early Warning Systems, Dynamic Reconfiguration Systems, Auditing procedures and forensic techniques.

Lastly, the framework would be incomplete without the testing and evaluation of the CII. Therefore, it should be necessary to develop a simulation tool that can verify the security of the interconnections between systems in the CII. Using this tool, it is possible to create a Decision Support System (DSS). Such system can recognize the stability of the CII under a certain context, its ability to adapt to this context, and the onset of irreversible trends. This Simulation-based DSS has to be based on the properties of individual nodes, the overall system and its context (for instance, an electricity system consumes less during the night than during the morning), and the faults and intrusions to which the system is susceptible.

6 Conclusions

In order to protect the well-being of a nation and its citizens, it is essential to guarantee the security of Critical Infrastructures and its information infrastructures. One of the multiple technologies that are specially suitable for this purpose is the Wireless Sensor Networks. Thanks to their intelligent distributed control capabilities, alongside with their capacity to work under severe conditions, such networks are an excellent tool for detecting and reacting against problems in safety-critical information infrastructures. Both the scientific community and the governments around the world have recognized the importance of Wireless Sensor Networks for this very purpose, spanning multiple research efforts and prototypes.

However, a sensor network does have its research issues of its own. There are few models and tools for designing WSN architectures, and

most protocols are reported to work in research testbeds but are untested in production environments. The state of the art on security in sensor networks is quite advanced, but it is also limited to research projects and prototypes. There have been no serious attempts to measure the actual security of a sensor network in a critical environment. Moreover, it is not clear how these sensor networks can be integrated with critical information infrastructures in order to provide all its protection services, although there are some research projects that pursue this precise goal.

Because of all these problems and research issues, one may argue that it would be a better solution for CII scenarios to use another technology for the same purposes, rather than WSN. However, there is no better technology available at this moment. Even more, experts agree on the high benefits that this new technology can provide to the many different facets of Information and Communications Technology. Therefore, many believe that it is only a matter of starting developing security solutions for sensor networks, in the same way as years ago the scientific community started developing security solutions currently under use for typical networks. As a result, it is essential to achieve successful deployments of secure sensor networks for the protection of CII.

Bibliography

Adar E., Wuchner A. *Risk Management for Critical Infrastructure Protection Challenges, Best Practices & Tools*, First Intern. Workshop on Critical Infrastructure Protection, pp 90-100, November 2005.

Akyildiz I.F., Su W., Sankarasubramaniam Y., Cayirci E. *Wireless sensor networks: a survey.* Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 38, no. 4, pp. 393-422, March 2002.

Alarifi A., Du W. *Diversifying Sensor Nodes to Improve Resilience Against Node Compromise.* In Proceedings of The 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2006), Alexandria, USA, October 2006.

Alcaraz C., Roman R. *Applying Key Infrastructures for Sensor Networks in CIP/CIIP Scenarios.* Proceedings of the 1st International Workshop on Critical Information Infrastructures Security (CRITIS 2006), Samos (Greece), August-September 2006.

Becher A., Benenson Z., Dornseif M. *Tampering with motes: Real-world physical attacks on wireless sensor networks.* Proceedings of the 3rd International Conference on Security in Pervasive Computing (SPC 2006), York, UK, April 2006.

Beckwith R., Teibel D., Bowen P. *Report from the field: Results from an agricultural wireless sensor network.* In Proceedings of the 1st IEEE Workshop on Embedded Networked Sensors (EmNetS-I 2004), Tampa, USA, November 2004.

Bologna S., Di Costanzo G., Luiijf E., Setola R.*An Overview of R&D activities in Europe on Critical Information Infrastructure Protection (CIIP).* In Proceedings of the 1st International Workshop on Critical Information Infrastructures Security (CRITIS 2006), Samos (Greece), August-September 2006.

D. Bopping. *CIIP in Australia.* 1st CI2RCO Critical Information Infrastructure Protection conference. Rome, March 2006.

Carlier L., Dhaleine L., Genestier P., Lac C., Savina B. *Emergency and Rescue: Methodology and Tool for Alert Activation and Crisis Management*, Informatik2003, Lecture Notes in Informatics, 2003.

Crossbow Technology, Inc. Wireless Measurement Systems. http://www.xbow.com

Distributed Intelligence, Sensing and Coordination in Variable Environments. CSIRO.
http://www.ict.csiro.au/page.php?cid=97

D'Antonio S., Oliviero F., Setola R. *High-speed Intrusion Detection in Support of Critical Infrastructure Protection*. In Proceedings of the 1st International Workshop on Critical Information Infrastructures Security (CRITIS 2006), Samos (Greece), August-September 2006.

Commission of the European Communities. *Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the Fight Against Terrorism*, COM (2004) 702 final, Brussels, 20 October 2004.

Hammerli B.M. *CIIP Task Description and a Proposal for a Substitute of National C(I)IP Policies*, 1st International Workshop on Critical Infrastructure Protection, pp 51-61, 2005.

Harvard University. *The CodeBlue Project*. http://www.eecs.harvard.edu/ mdw/proj/codeblue

He T., Krishnamurthy S., Luo L., Yan T., Gu L., Stoleru R., Zhou G., Cao Q., Vicaire P., Stankovic J.A., Abdelzaher T.F., Hui J., Krogh B. *VigilNet: An integrated sensor network system for energy-efficient surveillance*. ACM Transactions on Sensor Networks, Vol. 2, n. 1, pp 1 - 38, February 2006.

Sensor Nets / RFID. Intel Corporation. http://www.intel.com/research/exploratory/wireless_sensors.htm

Karlof C., Wagner D. *Secure routing in wireless sensor networks: attacks and countermeasures*. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, pp. 293-315, September 2003.

Karlof C., Sastry N., Wagner D. *TinySec: a link layer security architecture for wireless sensor networks*. Second Intern. Conf. on Embedded Networked Sensor Systems, pp 162-175, 2004.

Liu A., Ning P. *TinyECC: Elliptic Curve Cryptography for Sensor Networks (Version 0.2)*. http://discovery.csc.ncsu.edu/software/TinyECC/, September 2006.

Lopez J., Montenegro J.A., Roman R. *Securing Critical Information Infrastructures*. In Proceedings of the 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SecPerU 2006), Lyon (France), June 2006.

Manzo M., Roosta T., Sastry S. *Time Synchronization Attacks in Sensor Networks*. Proceedings of The 3th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 2005), Alexandria, USA, November 2005.

Martinez K., Padhy P., Elsaify A., Zou G., Riddoch A., Hart J.K., H.L.R. Ong. *Deploying a Sensor Network in an Extreme Environment.* In Proceedings of Sensor Networks, Ubiquitous and Trustworthy Computing (SUTC 2006), pp. 186-193, June 2006, Taiwan.

Minder D., Marrón P.J., Lachenmann A., Rothermel K.. *Experimental construction of a meeting model for smart office environments.* In Proceedings of the First Workshop on Real-World Wireless Sensor Networks (REALWSN 2005), Stockholm, Sweden, June 2005.

Moteiv Corporation. http://www.moteiv.com

Park T., Shin K.G. *Soft Tamper-Proofing via Program Integrity Verification in Wireless Sensor Networks.* IEEE Transactions on Mobile Computing, pp. 297-309, vol. 4, no. 3, May-June 2005.

Particle Computer GmbH. http://www.particle-computer.de

Ramanathan N., Balzano L., Estrin D., Hansen M., Harmon T., Jay J., Kaiser W.J., Sukhatme G. *Designing Wireless Sensor Networks as a Shared Resource for Sustainable Development.* In Proceedings of the International Conference on Information and Communication Technologies and Development (ICTD 2006), Berkeley, USA, May 2006.

Rinaldi S.M. *Modeling and Simulating Critical Infrastructures and Their Interdependences.* 37th Hawaiian International Conference on system Sciences, 2004.

Sahinoglu M. *Security Meter: A Practical Decision-Tree Model to Quantify Risk*, IEEE Security & Privacy, vol. 3, n.3, pp.18-24, 2005.

Sang Y., Shen H., Inoguchi Y., Tan Y., Xiong N. *Secure Data Aggregation in Wireless Sensor Networks: A Survey.* Proceedings of the 7th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT 2006), Taipei, Taiwan, December 2006.

Scatterweb GmbH. http://www.scatterweb.com

Schmitz W. *Modelling and Simulation for Analysis of Critical Infrastructures*, First GI Workshop on CIP, within Annual Meeting Informatik, 2003.

Sharp C., Schaffert S., Woo A., Sastry N., Karlof C., Sastry S., Culler D. *Design and Implementation of a Sensor Network System for Vehicle Tracking and Autonomous Interception.* In Proceedings of the 2nd European Workshop on Wireless Sensor Networks (EWSN 2005), pp 93-107, Istanbul, Turkey, January 2005.

SMEPP "Secure Middleware for Embedded Peer-to-Peer Systems" (FP6-2005-IST-5). http://www.smepp.org

Kenichi Soga. *Underground M3, Smart Infrastructure.* http://www2.eng.cam.ac.uk/ ks/soga.html

University of Southern California. *Networked Aquatic Microbial Observing System (NAMOS).* http://www-robotics.usc.edu/ namos/

Sun Microsystems Inc. http://www.sunspotworld.com

2004 US National Plan for Research and Development in Support for CIP. April 8, 2005. Retrieved from http://www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf

Verssimo P., Neves N.F., Correia M. *CRUTIAL: The Blueprint of a Reference Critical Information Infrastructure Architecture.* In Proceedings of the 1st International Workshop on Critical Information Infrastructures Security (CRITIS 2006), Samos (Greece), August-September 2006.

Werner-Allen G., Lorincz K., Ruiz M., Marcillo O., Johnson J., Lees J., Welsh M. *Deploying a Wireless Sensor Network on an Active Volcano.* In IEEE Internet Computing, Special Issue on Data-Driven Applications in Sensor Networks, March/April 2006.

Wokoma I., Shum L., Sacks L., Marshall I.W. *A Biologically-Inspired Clustering Algorithm Dependent on Spatial Data on Sensor Networks.* In Proceedings of the 2nd Annual European Workshop on Wireless Sensor Networks (EWSN 2005), Istanbul, Turkey, January-February 2005.

Wolthusen S. *Modeling Critical Infrastructure Requirements.* 5th IEEE SMC Information Assurance Workshop, 2004.