Trustworthy Wireless Industrial Sensor Networks - Interconnecting Smart Objects with the Internet Workshop position paper

Authors: Markus Wehner, Thomas Bartzsch, Dirk Burggraf, Sven Zeisberg (University of Applied Sciences Dresden, {wehner, bartzsch, burggraf, zeisberg}@htw-dresden.de), Alexis Olivereau, Oualha Nouha (Commissariat à l'Energie Atomique France, alexis.olivereau@cea.fr; nouha.oualha@cea.fr)

1. Introduction

Over the past years, the deployment of sensor networks in industrial environments has attracted much attention in several business domains. An increasing number of applications have been developed, ranging from defense, public security, energy management, traffic control to health care. Sensor networks are particularly interesting due to their ability to control and monitor physical environments. However, it appears that many security concerns, raised by business applications, have not been properly and efficiently addressed, particularly as far as multi-owner or mobile networks are concerned. This document presents the position of the recently started "TWISNet: Trustworthy Wireless Industrial Sensor Networks" project that aims to support and secure the integration of sensor networks into large scale industrial environments.

The objective in TWISNet is to develop a platform supporting the integration of sensor networks in an efficient, secure and reliable way, considering the strong technical constraints of sensor networks. For that purpose a number of use cases in the area of nuclear plant facility management, supply and demand energy management, industrial process monitoring and control, and multi-owner environmental monitoring are identified.
In scope of the workshop, the relevant use cases are described which address the major concerns of remote management of wireless sensor networks (WSNs), deployment concepts of wireless sensor nodes in industrial environments, data confidentiality and reliability in multi-owner networks, user's privacy, secure authentication mechanisms and inter-technology communication protocols. All those security requirements must be fulfilled considering resource constraints on the nodes by means of efficient (e.g. battery, CPU, memory) security and trust mechanisms.

2. Uses cases

2.1. Sensors networks for supply and demand optimization

Supply and demand energy management appears to be the one of the first large scale (thousands to millions of nodes) sensor network deployment. To improve the management of the existing resources, the consumers and electrical suppliers both need better information on the electrical consumption even down to individual devices and a means of automatically controlling these devices to schedule power consumption in low energy demand periods. The potential economic benefits of such systems far out-weigh the costs of the sensor networks themselves.

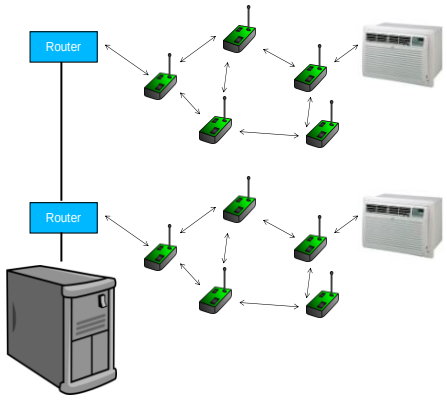

Figure 1: Architecture for WSN supply and demand operation

However, in Europe the confidentiality of the consumer information is ensured by national regulators. A key challenge of this scenario is the consumers' privacy preservation, which also raises an additional issue: processing confidential information. Monitoring applications need to be

able to make decisions derived from confidential information, for example, any abnormal energy consumption.

Assuming that remote management of customer equipment is possible, this equipment is prone to remote attacks, in particular to DoS (Denial of Service) attacks. Therefore, authentication of the provenance of commands to customer equipment is another strong requirement.

The electrical industry strives to obtain equipment lifetimes of 30 years. Customer devices lifetimes are meant to approach this threshold. However, due to the rapid evolution of the ICT industry in recent years this is not feasible and it presents major issues not only for the reliability of equipment but also for the long term security of the system. If a customer owns a ten-year old device, the external computing industry will have progressed and attacks that were not envisaged at that time when the systems were initially designed will become available. Therefore another key challenge of this scenario is the remote management of the authentication key and security model of the customer devices.

2.2. Multi-owner sensor networks

This scenario uses wireless sensors from multiple different services to form a single network, where a network for each service is not viable due to the geographical coverage of the wireless nodes. Typically, this might be for environmental monitoring for pollution control, but equally for control of natural resources such as the water quantity, quality, etc. in a dam or even wide spread industrial processes such as electrical distribution.

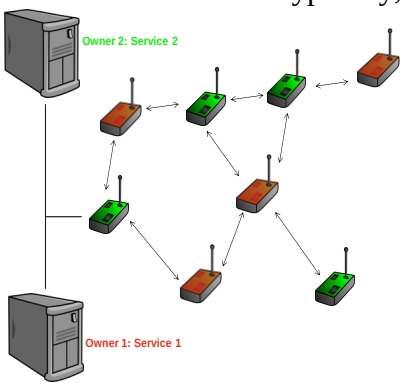

Figure 2: Architecture of multi-owner networks

The multiple services that would make up such a network are not generally owned by the same organisations and so the authentication to the shared network is a key challenge for this scenario. Once authenticated, the users must still consider that the wireless sensor network is a shared resource and treat the security requirements of this network accordingly. Another key challenge is devising appropriate means of securing the services of the multiple owners data from each other.

The rights of the various services to access the resources of the network are also needed to be managed. Nodes from one service will route the packets of another with no direct benefit to service of the node routing the packet, but with consequences on its battery life. A third key challenge in this scenario is therefore the resource management, so as to ensure fair distribution of resources between the services.

3. Technical Approach

The use cases presented in the previous section highlighted several key challenges for sensor networks for secure and trusted data processing. These can be categorized as follows: (1) remote credentials provisioning, (2) fast (re-)authentication, (3) privacy, (4) inter-operator connection sharing, (5) service availability & trustworthiness and (6) adaptive security. The technical solutions that are being developed to address these identified security challenges are organized into six corresponding security services and key challenges as follows:

- Automatic Configuration and Reconfiguration

Envisioned devices are likely to be widely spread and possibly in locations that are difficult to access. Furthermore, they are expected to be deployed in very large numbers. Therefore, manual administration should be reduced to a minimum. Instead, TWISNet will provide an interface allowing for secure and remote administration, so that mobile devices can be

easily updated. Especially, this interface will allow for the refreshment of expired/compromised cryptographic material (e.g. encryption keys) or authentication parameters. The interface may rely for that on an enhanced version of the μTESLA broadcast authentication protocol that for instance addresses denial of service attacks.

- Identity Management, Authentication and Access Control

In TWISNet, additional keys, called cluster keys, can be used for authentication. It allows a mobile sensor node to pre-authenticate with multiple nodes at the same time. When the sensor node moves, it can rely on such key to establish key paths with new neighbouring nodes. The proposed authentication mechanism in TWISNet should not reveal the real identities of sensor nodes to an eavesdropper. Application-level virtual identities can be used instead.

- Shared Information and Resources

Location privacy where mathematical algorithms do not match the reality of the sensor world and privacy protection of context-related information are considered. To alleviate these problems, we propose dynamic provisioning of virtual identities specifically adapted to wireless sensor networks. In certain situations, true anonymity can be attained. Otherwise, pseudonymity is used in conjunction with WSN, such that intermittently-connected devices can obtain pseudonyms on time. Finally, software-assisted privacy modules are designed to prevent the user from inadvertently disclosing sensitive information.

- Availability for Communications, Information and Services

Trustworthy architectures have to be designed to guarantee certain levels of service quality in the presence of hardware and software damage. Therefore, a service quality assessment system is used to monitor the availability and the security of the network. When network components are accidentally or maliciously damaged, the system pinpoints unsecure nodes and the network availability is updated. Based on the monitoring process, a secure and trusted system ensuring failure anticipation, prevention and detection is designed

- Adaptive Security

TWISNet enhances fixed security architectures by providing support for dynamicity and context dependency in all the security services it designs.

- Secure and Trusted Mediation Layer

Erroneous sensor data can have far reaching consequences. In the case of WSN where the nodes are easily accessible, ensuring the trustworthiness of the sensors data might even be impossible as an attacker might have physical access to the WSN. TWISNet follows the approach of investigating trustworthiness assessment of processed sensor data rather than ensure that the sensor data is implicitly trustworthy. Foreseen challenges beyond the state of the art include algorithms for the detection of misbehaving node or malicious data from sensor nodes, trust and reputation systems and development of a trust model from the capture of the data on the sensor to its use in a business process.

4. Conclusions and Outlook

These solutions will be further enhanced by implementing their algorithms and protocols on a sensor network prototype, tested in actual industrial conditions. Integrating commercial off-the-shelf or pre-standard devices, this platform will serve as a mediation layer between the sensor network and industrial applications. With a security architecture addressing the major business application security requirements (e.g. user's privacy, data confidentiality, reliability), its usefulness will be validated based on the identified use cases. Finally, the scientific and technical outcome of TWISNet will be its contribution to standards, such as IETF 6lowpan.

TWISNet is partially funded by EU FP7 Research and Development programme.