Reconfiguration in Wireless Sensor Networks

Helen C. Leligou\textsuperscript{1}, Luis Redondo\textsuperscript{2}, Theodore Zahariadis\textsuperscript{1}, Daniel Rodriguez Retamosa \textsuperscript{2}, Panagiotis Karkazis\textsuperscript{3}, Ioannis Papaefstathiou\textsuperscript{3}, Stamatis Voliotis\textsuperscript{1}

\textsuperscript{1} Technological Educational Institute of Chalkis, Chalkida, Greece, \textsuperscript{2} Metodos Y Tecnologia, Madrid, Spain \textsuperscript{3} Telecommunication Systems Institute, Technical University of Chania, Chania, Greece

Abstract

Wireless Sensor Networks are becoming more and more popular and offer a wide set of solutions invading our life. As the research community is working towards integrating them in the so-called “Internet of Things”, the capability to reconfigure them provides an unprecedented flexibility allowing for the flexible use of all available resources of different types. However, the desired reconfiguration features differ from use case to use case while the architecture of the device is also a restrictive factor. Full or partial reconfiguration, partial reprogramming, different reconfiguration frequencies and reprogramming of different functional components of the devices are among the available options. Since reconfiguration/reprogramming offers important benefits increasing however the complexity of the implemented logic and the network load, the design of reconfiguration applications is not a trivial task. This paper presents use cases where the reconfiguration features can be exploited, and discusses the functional blocks that can be reconfigured. We analyse as example applications the urban surveillance case based on a set of different sensors, and we identify communication modules and parameters that can be reconfigured/reprogrammed and investigate the reconfiguration frequency desired. Special emphasis is placed on the security modules and their attributes such as the key-length of the encryption algorithm.

Key Words: Reconfigurable Components, Wireless Sensor Networks, WSNs applications

1. Introduction

Wireless Sensor Networks (WSNs) are expected to have widespread application in the coming decades, ranging from monitoring and control (in industrial environments) to emergency response to habitat and environmental monitoring. WSNs have been identified as one of the most important technologies for the 21st century \cite{1} and according to current market projections, more than half a billion nodes will be shipped for wireless sensor applications in 2012. These networks must be capable of adapting to changing environments and requirements. A WSN application may need to alter its behaviour to manage limited resources more efficiently, recover from broken network links, or change its functional behaviour in response to commands issued by an operator or even implied by the environment itself.

Focusing on the resource constraints of WSNs, since sensor nodes are typically run on batteries, one of the most important factors in determining the success of a certain distributed sensor network (if not the most important one) is how well it manages energy. Hence, by allowing WSNs to adapt their energy consumption in real time based upon the rapidly changing environmental conditions results in the elongation of the network lifetime. This can be achieved by realizing Real-Time Dynamic hardware reconfigurability.

Moreover, given the limited processing and memory resources of a sensor node, and assuming that such a node is running specific security and video compression algorithms, a different combination of these algorithms may better fit the desired application. Another reason for building reconfiguration/ reprogramming functionality in a WSN is the related cost: reprogramming of nodes on-the-fly could be necessary when dealing with more than 30 nodes while the cost will be very high if a person has to go to field and program each node at a time.

The rest of the paper is organised as follows: in section 2 indicative use cases where the remote reconfiguration capabilities are useful are described, while in section 3, a more detailed view of the functional blocks that can be reconfigured is provided. Conclusions are drawn in section 4.

2. WSN applications and reconfiguration needs

In an attempt to investigate the reconfiguration and reprogramming needs of current WSN applications, we have analysed a wide set of them including:

- urban operations (movement indoors and between buildings, rapid dissemination to combatants, shooter localization)
- surveillance (e.g. Border Monitoring, Littoral operations, construction detection)
- environmental Monitoring (e.g. River Overflow and Forest Fire)
- building monitoring (monitoring cracks in bridges/buildings, historical buildings, harbor structures, dams and levees
- liquid pipeline monitoring (gas, oil, water) and tunnel monitoring
- smart home, smart farming and irrigation (monitoring of the social behavior of animals in farms and natural habitats, farm waste monitoring
- asset management
- health monitoring of humans and critical plants

Due to space restrictions, we present in the sequence (as an indicative example) the case of urban operations.

Deploying a network of sensors for monitoring and controlling urban operations is a common practice. For example, cameras in museums, supermarkets, or buildings are installed for surveillance purposes. Sensor technology has greatly advanced in terms of size, power consumption, processing capabilities, and low cost, thus fostering deployments of self-organizing wireless sensor networks over large geographical areas to support a large variety of so-called sensing applications ranging from emergency and surveillance to tourist guidance and entertainment. However, urban mobile sensor networks are challenging programming environments due to the dynamism of mobile devices, the resource constraints of battery-powered devices, the software and hardware heterogeneity, and the large number of concurrent applications that they need to support. These requirements hinder the direct adoption of traditional distributed computing platforms developed for static resource-rich networks.

Using cameras and sensors to detect indoor movement as well as movements between buildings requires the clear definition of the objective and faces. Several technical issues are raised, among which the cameras management, density, camera coverage and positioning, as well as the technical characteristics and operation of the control room. The main components of an automatic video surveillance system include [2] video cameras connected to a video processing unit, to extract high-level information for any identified alert situation; this processing unit could be connected throughout a network to a control and visualization center that manages, for example, alerts; another important component is a video database and retrieval tool where selected video segments, video objects, and related contents can be stored and inquired. Video objects show in general (a) low-level features such as color, texture, and motion, (b) high-level features such as dynamics (i.e., movement, activities, action, or events) and semantic information (behavior), and (c) syntax.

A survey on camera-based systems used for surveillance reasons in different urban sites (including city center, hospital, shopping malls, etc.) [3] has proven that a surveillance scheme must be properly managed and this requires technical expertise while lack of interest and lack of knowledge on the part of project managers may compromise the ability of schemes to meet their objectives. The density of cameras, the level of camera coverage, the type of camera used and the way that it was mounted influences the efficiency of a system in live monitoring.

In this case, the capability of reconfiguring the camera network and possibly integrating it with other sensor types allows first, for switching off part of the devices to economise energy and prolong the network lifetime, second, for reconfiguring the video processing algorithm in order to adjust the video quality, resolution and coverage and the aggregated data volume as well as for adaptation of the security levels. The integration of the camera system with other sensors allows for changing the configuration based on dynamically changing environmental parameters. For example, when temperature increases above a certain threshold, possibly revealing the start-up of a fire, higher accuracy of the captured video is desired to detect possible causes and control the situation onwards.

It is widely agreed that urban military operations demand reliable and fast information exchange in battlefield so that the commanders lead their troops safely and successfully to their mission goal. Soldiers need “smart” mapping tools to tell them not only their position but real time information on what is around a corner, behind walls, what are the enemies troops movements, which are the most safe extraction routes, where is the nearest medical support unit, which of the near open fields or buildings roofs are suitable for helicopter landing as well as reliable data links to each other. Also, commanders in headquarters need accurate knowledge of “what is happening” in entire city in order to evaluate the situation, make the right decisions and give the appropriate orders to combatants.

Visual and audio data are two key sources of information. Acoustic tracking of mobile targets using tiny sensing devices is very attractive, as massive deployment of wireless sensors in large area can provide more accurate and timely information about the geographical location of the targets. The basic idea of acoustic tracking is to detect the location of a target by analyzing the specific cues such as delay and amplitude received by multiple sensors. This effort can be supported from a low cost Wireless Sensor Network (WSN) for outdoor deployment. WSNs could deploy over urban battlefield collecting all the data via high bandwidth communication to Locals and Central processing units in which data flows convert to useful intelligence and display battlefield information to headquarters and also to local commanders. One of the biggest threats in urban battlefield is enemy’s shooters who are taking cover for long time periods in buildings, roofs etc and they are observing the behavior of the people in front of them. Their intention is to identify the target and then prepare to fire at him.

Real-time tracking with WSN is extremely challenging since it requires high system robustness, real time decision making, high frequency sampling, multi-modality of sensing, complex signal processing and data fusion, distributed coordination and wide area coverage.
In such an environment the ability to reconfigure / adjust the sampling frequency of the city sensors (to increase the accuracy) and of the tiny sensors carried by the men in the battlefield (decrease the sampling frequency when not needed to save energy) can highly affect the efficiency of the overall operation. Also, a really crucial aspect of the communication in such a WSN is security. An adversary could easily perform eavesdropping of classified information, Denial-of-service attacks by means of jamming and/or confusing the networking protocols or supply misleading information, e.g. enemy movements in the East where in fact they are in the West. Thus the security levels of the WSN security protocols should be reconfigurable.

Other applications where reconfiguration and reprogramming over the air is highly needed is in environmental and border monitoring. Wireless networks used to monitor river levels face the difficulty that rivers extend along several hundreds kilometers. In order to cope with such long flow the network is based on a simple 2 levels hierarchical model. In normal operation, the involved sensors periodically report, every few hours to the remote control unit meteorological data, water level and speed. On request, they can send pictures of the river that are useful to verify that the sensors have not moved and are working properly. In emergency operation, when strong rain occurs and the central unit is alerted, all sensor data are transmitted more frequently and slow but high resolution video is also transmitted for a better analysis of the river status. Forest fires are among the disasters causing threats to both the humankind and the ecosystems throughout the world.

The probability of forest fires is steadily increasing due to the climate change and human activities. Since sensor nodes may be strategically, randomly, and densely deployed in a forest, WSN can provide valuable information in order to perform passive and active firefighting actions. Such information like the exact origin of the fire could be very valuable to the end users in organization of the firefight means -by local and central point of view- before the fire is spread and goes uncontrollable. Wireless networks for the prevention of forest fire are based on 3/4-level hierarchical model. That is due to the large area to be covered and to the need to make efficient use of the fire fighting means and personnel. It is evident that all the unmanned units would greatly benefit from every reduction of power consumption and size of the equipments.

A country’s geographic border line usually spans hundreds or thousands of kilometers, involving terrain with alternating and often “difficult” characteristics. Various systems are already available and have been installed for such applications, offering numerous features such as event triggering, threat classification and target tracking upon detection as well as secure remote access and data encryption. However, the SMART architecture can greatly enhance the functionality of such infrastructures by offering the capability to dynamically adjust their functionality according to the environment requirements.

Many countries have large coastline that needs to be supervised e.g. Greek coastline extends to a total length of about 15,000Km. SMART platform could be incorporated in a coastline monitoring system and, due to its capabilities for rapid reconfiguration, provide additional functionality whenever required. Such a coastline monitoring system can be based on a two-tier architecture. This will incorporate a set of monitoring stations (MONS) mounted on top of towers allowing the observation of large coastline areas. Depending on the terrain characteristics, WiMAX or satellite networking will provide connectivity of all monitoring stations with a central station (CSS) that will be able to receive data from all monitoring stations and process them further.

Nowadays, aged civil infrastructures and buildings have a huge maintenance necessity. This causes the investment of large amounts of money, which cannot be avoided in order to prevent cracks that cause accidents, structures collapse and, in short, the premature end of the structure life span. This structural monitoring will help in increasing the grade of safety and security of constructions.

Structural Health Monitoring (SHM) of buildings - civil infrastructures- is, maybe, one of the most in-demand real-world applications of wireless sensor networks, which justifies the Research community effort. By using the emergent technology of WSN (Wireless Sensor Networks) we can address these issues involving safety, maintenance and prevention of structural properties of civil infrastructures. Some examples of structures where applying this technology could be satisfactory are buildings, bridges, dams, waterways, roads, etc, because they suffer severe environmental conditions and overloading scenarios that may result in a long-term structural deterioration.

Habitat monitoring is the surveillance of a natural environment or the animals living inside this. Based on wireless sensor networks it allows to instrument natural space for long-term and preserving data collection. The onboard compute power and storage capability of single nodes enables data preprocessing and selection utilizing complex filters and trigger function directly at on-site. Cooperating nodes are able to perform even more complex tasks like statistical sampling and data aggregation or system health and status monitoring. The possibility of reprogramming a node in field enables operating adoption over time.

Habitat monitoring is the surveillance of a natural environment or the animals living inside this. Based on wireless sensor networks it allows to instrument natural space for long-term and preserving data collection. The onboard compute power and storage capability of single nodes enables data preprocessing and selection utilizing complex filters and trigger function directly at on-site. Visual habitat monitoring is the most common technique. SMART sensor nodes offer impressive video capabilities for monitoring and tracking with ultra low
power consumption thus providing long lifetime. Deployed sensors can stay in the field for a very long time and record visual information with high-end video quality mitigating the time-space problem. On board computation power allows data preprocessing and filtering resulting in a reduced amount of data for transmission. Finally highly efficient encryption and compression algorithms are implemented in SMART enabling secured data transmission from the sensor node to the gateways and base station.

3. Reconfigurable modules

Although full reconfiguration of nodes can in general be supported, analyzing the above applications we found out that there is a need for a more concrete and flexible way of adapting the current behaviour of a node in order to avoid bringing it to a resetting state. The real-time reconfiguration in response to changes in the operational conditions either autonomously or remotely targets specific modules. The main adaptive system modules capable of being reconfigured are:

3.1. Data communication modules

Changing the communications parameters of the sensors can bring advantages. For instance, nodes may auto-configure routing mechanisms based on radio link availability and congestion indicators, or regulate transmission power based on remaining battery measurements and received signal strength (RSSI) from their neighbours. The former situation could occur if a high video resolution has been selected or a large load of data is to be transmitted towards a central device. The latter may occur if an estimation of the autonomy of the node falls subsequently under predefined battery thresholds or inter-node distances increase in the WSN as a result of a re-deployment operation. Likewise, the amount of transferred data and transmission rate (frequency) may be enlarged or reduced according to the actual needs advised by the sensing mechanism, e.g. high likelihood of attacks or higher bandwidth resources required by priority applications in the WSN.

3.2. Data encryption and authentication modules

It is highly desired that a sensor node offers a number of security properties for reconfiguration with the aim of achieving adaptive levels of data confidentiality and integrity and efficient power resources management. It could offer for example:

- Only data encryption
- Data authentication and data encryption
- Data authentication, data encryption and reply protection

Various mechanisms for encryption, cipher-based authentication and genuine source node validation can be supported. The security/performance trade-off deserves special attention when performing cryptographic computations. Certain parameters in any cryptographic algorithm determines their computational cost and associated power load [4] [5]:

- **Key length**
  
  The size of keys used by specific algorithms (either symmetric or asymmetric) is always associated to the actual implementation considered. The amount of data employed by encryption/decryption procedures has direct impact in the level of security provided to data transmission. The effect of key size on consumption is much more pronounced in asymmetric algorithms which are much more computationally demanding. Nevertheless, the key length within symmetric algorithms also affects the performance and power consumption. This is also the case for authentication methods, which speed and computation load is influenced by signature size [6].

- **Block cipher operational mode**
  
  In occasions, the length of outgoing messages may be larger than the maximum block size considered by the cipher block. To provide support for messages length, several modes of operation may be used in conjunction with any symmetric key block cipher algorithm and be selected in run-time: the Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR) modes [7].

- **Number of cipher rounds**
  
  Encryption or decryption procedures perform iterative mathematical computations that increase the level of security, in exchange for a power consumption increase. The number of attacks needed to break the algorithm increases with increasing ciphering repetitions or rounds. This parameter is thus considered for reconfiguration purposes.

  The WSN can operate in a low-secure, low-power mode until the detection mechanism realizes that a certain security threat appears; then a group of nodes can be reconfigured so as to support a much better encryption protocol, and, whenever the threat the threat is considered to have disappeared the nodes will switch back to the low-power mode. Additionally, nodes could use a certain communication protocol for a low-noise environment. Whether the noise increases over a specific threshold, it can increase the security aspects of both the transmitted data and the sensor node itself when it senses any kind of a security attack.

3.3. Data authentication modules

Sources of information and data received must be verified to achieve a fully secure communication in the WSN perform the communication process over a secure channel. As for encryption/decryption mechanisms, authentication techniques require different signature sizes which redound to faster and lighter computations for shorter signatures. If this feature is made available
for sensor nodes, reconfiguration could imply switching between various implemented methods in run-time or simply relaxing security requirements by turning off authentication.

3.4. Data and video compression modules

According to the actual scenario needs, and in isolated cases, a higher/lower data and video compression rates might be needed, always at the cost of higher/lower processing power for the nodes. Nevertheless, low-complexity encoding will be applied and the reconfigurable device could be requested to switch between various paradigms in order to balance the compression/communication trade-off. On the one hand, a good approach for video sensors is performing a high degree of compression to reduce the number of bit transmissions/receptions. On the other hand, the use of an intensive compression technique will result in a considerable increase in the number of local computations at a sensor [8]. Commonly, both operations are the main source of energy drain for a network node with video capabilities.

4. Conclusions

Each application has specific reconfiguration/reprogramming requirements and it may adapt differently to a changing environment as well as it may require a different frequency of reconfiguration of its functional modules. The main parameters of the reconfiguration procedure that differs among use cases are the estimated period of reconfiguration, the associated degree of reconfiguration (partial or full, and which functional blocks) and the reconfiguration delay. The period of reconfiguration or frequency of updates over a certain module is related to the level of safety and energy saving required in the scenario. For example, high frequency is expected when real-time adaptation to fast changing environments is needed, while medium frequency is expected for periodic reprogramming. Finally, when reconfiguration is driven by an alarm or a specific event, the frequency is low although the tolerated reconfiguration delay is constrained in this case. Apart from the reconfiguration frequency, the degree of reconfiguration also differs from application to application. Thus, in certain cases only parameter adjustment suffice while in other cases the algorithms executed on the sensor nodes need to be reprogrammed.

5. Acknowledgement

This work was supported in part by the ARTEMIS JU under the ARTEMIS-2008-100032 SMART (Secure, Mobile Visual Sensor Networks Architecture) project.

6. References