Communication Security in Wireless Sensor Networks

Rui Miguel Pinheiro Pires
rui.pires@ist.utl.pt

Instituto Superior Técnico, Lisboa, Portugal

November 2015

Abstract
With the increasing usage of wireless sensor networks, it is necessary to ensure the basic security properties for the data communication, particularly in applications where the communication exchanged is sensitive. This work analyses the particular problem of communication security for a system that has several wireless sensor networks, and presents a solution for it. The proposed solution is implemented and its operation analyzed.

Keywords: Wireless Sensor Network, Security

1. Introduction

Thanks to the recent technological advances, the manufacture of small sensors with reduced power consumption and wireless communication capabilities has become possible and economically viable. The combination of the characteristics of these devices, such as: their small size, low cost and wireless communication capability, gives the wireless sensor networks a large area of application possibilities. As identified in [1], such networks can be used in a large variety of applications, like geographical monitoring, performing, for example, the tracking of an animal's location.

The proliferation of wireless sensor networks makes security a priority research field in order to ensure the reliability and proper operation of the applications supported by them. The devices usually used in wireless sensor networks have limited resources [2], normally in terms of processing, memory and energy capabilities. These limitations make the use of some traditional security techniques impossible.

The special characteristics that wireless sensor networks present, such as mobility and the limited capabilities of the devices normally used, are challenges that must be overcome to ensure the desired security properties.

This work studies the problem of security in wireless sensor networks. Analyzing the major attacks that these networks are susceptible to, and studying the main proposed protocols to ensure their safety. In addition to this study, this work analyses in particular the problem of security for a network of this kind, and presents a solution for it.

This solution protects the basic security properties for the communication of the system, authentication, confidentiality and integrity, and tests the use of asymmetric key cryptography for the authentication and key distribution process. This solution is implemented and its operation is analysed.

2. Background

Throughout this chapter we expose the related work on security aspects of wireless sensor networks and mesh networks.

2.1. Security in wireless sensor networks

2.1.1 Wireless sensor networks

A wireless sensor network (WSN) consists in a set of sensors, spatially distributed to monitor physical or environmental conditions.

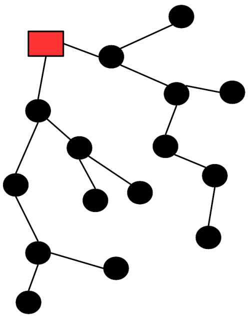

Figure 1: Example of a wireless sensor network.

As illustrated in figure 1 this kind of networks uses small sensors with wireless communication capabilities that form autonomous mesh networks to route data to a gateway, the node responsible for making the connection between the sensors and some external infrastructure, such as the Internet.

The combination of characteristics of these devices, such as their small size, low cost and wireless communication capability, gives specifically to wireless sensor networks a large area of application possibilities.

As identified in [1], wireless sensor networks may be used in a large variety of scenarios. They can be applied in applications as geographical monitoring, habitat monitoring, for example performing the tracking of animals, or for intelligent parking systems, among others.

These sensors measure the ambient environmental conditions surrounding them, send periodically updates to monitor the environment and in case of change of particular state, may create alarm messages that are sent to a central unit to alert the system supervisor.

As mentioned in [2] the devices normally used in sensor networks have limited resources, usually are resource limited with respect to their energy, memory, computational, and communication capabilities.

Table 1 presents the memory capacity for several typical types of sensors.

Name	RAM Memory	ROM Memory
MICAz	4 kB	128 kB+ 512kB
Imote	64K SRAM	512K Flash
TelosB	10 K SRAM	48 KB/1024 KB

Table 1: Memory capacities for several typical sensors used in WSN.

Wireless sensor networks are sometimes also referred as mesh networks because they share some similarities. The main similarity is the fact that in both models the communication is multi-hop, i.e, using nodes that have the ability to forward messages. However, as identified in [3] the major difference between these two types of networks is the fact that in wireless sensor networks there is no flow communication between two network nodes that are not neighbours. In contrast, mesh networks are characterized by the possibility of communication between all the elements of a network.

2.1.2 Threats and trust models

The communication medium in WSN is wireless, it is assumed that the transmission medium is insecure, and an attacker can listen the communication and introduce or repeat messages.

Like the entity that owns the network, an attacker can still distribute new sensors with abilities matching the legitimate ones. Given the usual lack of physical security, it is normal to assume that an attacker can capture the nodes of the network, and read or write their memory [4].

There is a great difference between two types of attackers, they may be internal or external. The external threat consists of attacks by elements outside the network. On the other hand, the internal attacks are carried out by legitimate nodes that have been compromised, or by external elements that through information theft (such as obtaining the cryptographic keys that secure the communications), can participate in the network as legitimate nodes.

As mentioned above the vast majority of wireless sensor networks have at least one node that enables the connection to other networks - the gateway. Compromising one gateway, can render the entire network unusable, hence, it is normal to assume that this is a reliable node [3], i.e, that they behave correctly and as expected.

The desirable security properties for protecting the communication in wireless sensor networks are identical to those required in computer networks:

- Authenticity. Property that allows a node to trust the identity of another node with whom he communicates. A received message is authentic if it was really originated and sent by the identity announced. When this property is not guaranteed an adversary can impersonate any node in the network, creating false messages.

- Integrity. This property ensures that data is delivered to the destination as it was originally sent by the source. The invalid alteration of a message may be caused by communication failures that cause errors, or carried out maliciously by an attacker who changes the content of a message.

- Confidentiality. It is a basic requirement in any communication system, it ensures that data is only accessed and viewed by members authorized to do so. Confidentiality is usually achieved using encryption.

- Availability. Availability is the property that ensures survivability and proper operation of network services, even in the existence of several attacks.

2.1.3 Main attacks

In this subsection we present the main attacks that wireless sensor networks are subject to.

Attack to information in transit. An attacker who has adequate means may collect the data that circulates on the network. If the data it is not properly protected an attacker knowing the existing communication model can, for example, introduce false messages trying to impersonate another node, change their content, repeat messages sent in the past, or just make them useless.

Sybil attack. It is common that in wireless sensor networks, several sensors are necessary to work together to perform a certain task, for example: the aggregation of several signals detected by various sensor nodes to determinate the state of the environment.

In such situations an attacker node can try to impersonate multiple nodes, in order to change the final result of the aggregation of the several detected signals.

This type of attack where a node tries the embodiment of multiple nodes simultaneously is known as a Sybil attack [5], and it is not just specific to WSN.

Selective forwarding/Black-hole. Multi-hop networks assume that the intermediate nodes participating in the network will send all the messages they receive, which is an assumption that does not always hold true.

A selective forwarding attack consists in a malicious node that does not perform such function for some of the traffic that it receives, as an attacker selectively prevents the forwarding of a set of the messages.

An attacker node can also block all traffic it receives, performing a so called black-hole attack.

If such attack is performed, after a while, the neighbours will easily suspect of the attacker and will try to route traffic by other nodes. On the other hand, performing a selective forwarding attack the malicious node raises less suspicions, since the number of lost packets can be assumed to be a cause of nodes failing, transmission errors or losses due to network overload.

Sinkhole attack. The goal of a sinkhole attack is to attract the whole network traffic of a given area to the attacker node.

This attack usually corresponds to an internal node of the network, for example a compromised node, make himself appear particularly attractive for routing messages to the gateway.

This attack can be carried out by falsifying the messages of the routing protocol, for example, simulating that the attacker node is within walking distance of the gateway.

Achieving this type of attack becomes more effective with the subsequent implementation of a selective forwarding or black-hole attack.

Wormhole attack. A Wormhole attack [3] consists in an attacker node receiving a message in a given area network and repeat the same message in another distant zone. This type of attack usually involves two malicious distant nodes, who share an external network connection between them.

For example, as illustrated in figure 2, an attacker node A when receive a message from the gateway routes the messages to another malicious node B, using an external link. When node B gets the messages it repeats them to his neighbours.

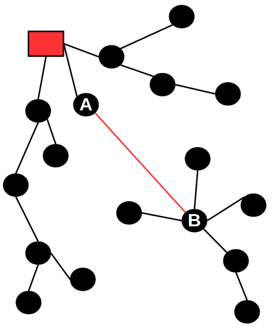

Figure 2: Wormhole attack.

This culminates in a kind of denial-of-service attack, as the neighbouring nodes of node B will assume that they are just at one-hop distance of the gateway. The neighbours of node B will try to send messages directly to the gateway, but these will be lost given that they are out of the gateway's range.

This technique also allows for other types of attacks. If the Node B route the messages to the gateway, its neighbours will believe that they are even closer to the gateway. This way node B will have much of the network communication in their possession. This leads to a perfect situation to carry out an information in transit or a selective forwarding attack.

Jamming. At the physical layer it is possible to attack the system's availability running a jamming attack. This attack consists in an attacker that just transmits noise to prevent communication between the elements of the network.

This attack can be accomplished abruptly, creating constant interferences that prevent full communication of neighbours nodes within range, or selectively transmitting noise only when a specific node is transmitting.

Denial of service. The concept of denial of service defines a set of attacks that attempt to prevent the network ability to provide access to a particular service.

This type of attack can occur at different protocol layers in WSN.

At the physical layer it can occur running a jamming attack, in the medium access layer can be achieved by infringing the rules of the medium access, for example sending messages only in order to generate collisions with messages sent by other node.

At the network layer can be achieved by performing a black-hole attack in such a way that prevents part of the network to communicate with the gateway.

2.2. Protecting WSN
In this section are presented the main security mechanisms proposed to ensure the security of the communication in wireless sensor networks.

2.2.1 Communication security

This subsection identifies protocols that ensure the basic security properties at the communication level.

Several protocols are proposed to solve this problem in WSN: SNEP, MiniSEC and TinySec are three examples.

The identified protocols ensure the security of communications exchanged between two elements, including their authenticity, integrity, confidentiality and protection against replay attacks.

These protocols do not address the problem of key management, being assumed the existence of a pre-shared symmetric key between nodes.

The identified protocols use identical ideas:

- All three use a message authentication code MAC, to guarantee authenticity and integrity of each message sent.
- The MAC used has only 4 bytes.
- Concerning encryption, these mechanisms mainly use the CBC (cipher block chaining) mode of operation.
- Semantic security is achieved using a shared counter between the source and receiver used as an Initialization Vector (IV) in CBC mode.

2.2.2 Broadcast Message Authentication

A mode of communication commonly used in wireless sensor networks, as generally in wireless networks, is send messages in broadcast. The use of broadcast is usually done in order to spread certain messages over the network, in particular in WSN for the dissemination of routing messages.

In this case, in order to ensure authentication of each message sent is not reasonable to use symmetric encryption alone.

To solve this problem were presented two protocols uTesla, ARMS.

This two protocols use the same base idea, achieve asymmetry with delayed key disclosure based on one-way function key chains.

2.2.3 Key management

Given the limitations of the devices commonly used in wireless sensor networks, the use of symmetric key encryption is dominant in this kind of networks. The distribution of those keys is normally held by pre-distributing them on the sensors or through the proactive establishment, i.e., after their deployment in the network.

A pre-distribution process consists in installing the keys before the deployment of each node in the network, which will allow subsequent secure communication between them.

In contrast, proactive distribution is based on dynamic generation of keys after the deployment phase and before data can be exchanged.

These are some of the proposed ways to perform the proactive establishment of symmetric keys between two elements in WSN:

LEAP+. Localized encryption and authentication protocol [6]. In LEAP+ it is assumed that sensors are static and can be compromised, but only after a given time t posteriorly to their deployment in the environment.

Initially, each node knows the master key of the system and is able to authenticate itself against its neighbours and establish the symmetric keys used for protection of the further communications. After time t each new node delete the master key from memory.

The major disadvantage of LEAP+ is the fact that it is assumed that the network nodes are static, which limits the applications where it can be used.

Probabilistic key distribution. The probabilistic key distribution mechanisms try to guarantee a specific probability for symmetry key establishment for each two nodes of the system.

A large pool of keys is generated for all the system, and only a randomly selected k number of keys are offered for each node.

If two nodes have one or more keys matching, a secure link is established after a symmetric key is establish.

Asymmetric cryptography. One of the techniques most commonly used to provide support to the key management of symmetric keys in computer networks, is asymmetric cryptography.

However, in wireless sensor networks it is assumed that asymmetric cryptography cannot be used efficiently, which is justified by the hardware limitations of the devices normally used in such networks, and the high resources costs associated with the techniques commonly used by these methods.

In recent years with the improving capabilities of the devices used for WSN, a number of studies have been presented that show that this assumption may be outdated.

In [7] is shown that the public key cryptography is computationally feasible in 8-bit processors, although tests show that energy costs are high, and only suggest its use for key distribution. Results are also confirmed by later studies [8] and [9].

In [10] is carried out a comparative analysis between two asymmetric encryption techniques RSA and Elliptic curve cryptography (ECC). The results as suggested previously in [6] and [9] show that the ECC technique performs better in terms of computational cost. But the great advantage of this technique is the small size of the keys used when compared to the same security levels with an RSA key. For example, to get the same security level of a RSA key of 1024-bit, ECC only use a key of 160 bits [10].

The tests performed in [10] shown that the cost of a handshake between two nodes, with mutual authentication and symmetric key establishment between them, using ECC with key size of 160, when compared to the total cost of transmitting 64kB it represents only about 2% of the total energy consumed.

Pairing-based cryptography Pairing-based cryptography is a young area in cryptography, this technique allows that two elements who know the identifiers of each other, calculate a shared symmetric key between them in an authenticated way. This method is also based on elliptic curves.

Although this technique is not yet widely used, it is a recent technique that seems to fit perfectly in wireless sensor network. It offers a shared key establishment between two elements in an authenticated way, with low computational costs and energy.

In [11] an implementation of a Pairing Based Cryptography scheme is presented.

The theoretical results show that this technique allows the creation of shared key establishment with a shorter runtime when compared with other techniques such as elliptic curve DiffieHellman (ECDH), but also that the required ROM resources are doubled.

3. Solution

3.1. Problem

This project aims to resolve the computer security issues associated with a monitoring system. The project is being developed by Sensefinity, a technology start-up based in Lisbon.

The problem is to ensure the various security aspects of communications between a set of multiple devices that form mesh networks, which communicate with a central entity that can be found geographically distant. This entity is contactable via the Internet or via the mobile network.

Each of these mesh network may be comprised by dozens of nodes and with one or more gateway nodes. The gateway nodes act as the exit point of the network and are not energy limited.

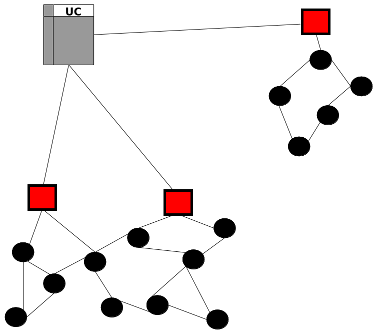

Figure 3: Architecture of the system

The system has the architecture illustrated in figure 3. Set of various mesh networks, each network consisting of several mobile nodes (black circles) and one or more gateway nodes (red squares). As already mentioned, the gateway nodes enable the communication between the network elements and the central unit (UC).

The network nodes consist of small size devices with limited computational and energy capabilities, associated to a large object with mobility capabilities. This objects remain static lot of the time, but may change its position on the network or move between the various networks that belong to the system.

The aim of the system is to perform the monitoring of the geographical location and the condition of the objects to which the devices are associated. To do this, each device periodically sends a message with their location information. Moreover, when certain events are detected the nodes must send alarm messages to the central unit.

The devices used in the system shown in Fig.4, have the following characteristics:

- Processor *Texas Instruments* MSP430 (16*bits*), 12 Mhz.
- 128 kBytes of ROM memory.
- 16 kBytes of RAM memory.
- 10 communication range.

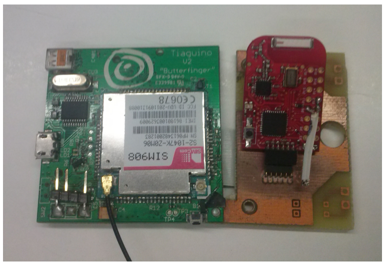

Figure 4: Devices of the system

The main threat in the environment considered in this work is that the network elements are particularly vulnerable to attackers physically close to the network. This way attackers may easily listen or interfere with the communication.

It is a requirement ensure the confidentiality, integrity and authenticity of the existing data exchanged between the network elements. To this end, due to the mobility ability of the nodes, the implementation of a proactive authentication and key establishment mechanism is required.

For this purpose, the implementation of an authentication mechanism of the nodes in the system is necessary, so that only the legitimate node will be able to send valid messages to the central unit.

Finally, it is expected, and it is essential that the proposed solution is efficient so that the expected lifetime for the network nodes will not be reduced too much with its implementation.

3.2. Solution description

In order to ensure the authenticity of each node, an authentication protocol is carried out using a library that offers the basic operations for digital certificates based on elliptic curves cryptography.

The use of asymmetric encryption is often considered inappropriate for sensor networks. However, in the environment considered in this work, this kind of technique can be used.

In this case, although nodes can change their position within each network or cross other networks, the communication flow is always the same, the messages will be sent to the central unit. So only one authentication protocol will be necessary to establish a shared session key between each node and the central unit. This key will be used to ensure the safety of the messages subsequently sent by each node to the central unit.

The choice between the various possible techniques for asymmetric cryptography fell on the elliptic curves cryptography. This choice is justified by the studies considered earlier in this document, as it is proven to be the one with the best results in terms of energy consumption and on the required computing and memory capabilities.

A new entity was added to the initial system: the certification authority (CA) - a trusted entity responsible for generating the key pairs for each node and sign their certificates.

When each node is installed in the system it has:

- Public and private key pair
- The public key of the CA.
- A certificate signed by the CA, attesting to the truthfulness of the public key of the node.

In order to ensure the security of the routing protocol messages, it was defined that they will be secured using a group key. This group key should be shared by all nodes in the same network properly authenticated.

3.3. Network authentication

When a node connects for the first time, it must perform an authentication protocol and establish a shared session key between him and the central unit in order to ensure the safety of future communication between them.

Since the same network may comprise several gateway nodes and each node may move between different networks, to avoid different authentication processes on different gateway nodes, the authentication process will be validated by the central unit (UC).

The establishment of a symmetric key between node and gateway is performed using the protocol ECDH (Elliptic curve Diffie-Hellman), shown in figure 5.

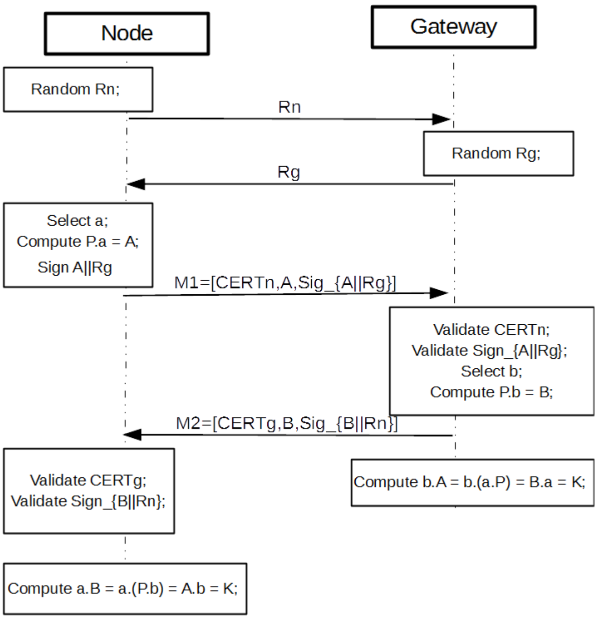

Figure 5: Authentication protocol

In figure 5, the parameters a, A and P for the node and parameters b, B and P for gateway are elements of the basic ECDH protocol.

To protect this process several measures were taken:

To ensure the authentication of the messages exchanged, they are signed with the private key of the source element and sent together with the corresponding certificate.

When a node receives messages M1 and M2, it checks the validity of the certificate received using the trusted public key of the CA and then verifies that the message was signed by the correspondent private key.

To prevent replay attacks of these messages it was added a prior stage, where the elements only exchange random numbers between them. In the later stage each element expects that messages M1 and M2 will be signed using this random number, ensuring that messages correspond to the previous requests.

This way, an attacker can only repeat authentication messages for the same two elements when the random number requests are repeated.

3.4. Secure Communication

Using the established session key, each node sends messages in a secure way to the central unit. In this system's case, the nodes send periodically the geographical location information of each object.

For these messages the following properties are guaranteed: confidentiality, integrity, authenticity, and replay protection of messages.

In order to ensure the confidentiality of communication is based on an encryption scheme that uses AES on the CBC mode of operation.

To ensure authenticity and integrity of communication, for each message is computed a MAC using the CMAC technique.

Protection against the repetition of messages is achieved with the use of a sequence number, present in the header of each message and used also on the MAC calculation.

3.5. Routing messages

For the routing messages it was decided to protect their authenticity and integrity. To achieve this, a MAC is associated to each routing message.

This MAC is also computed using the CMAC technique, using the network key shared by all nodes of the same network.

This key is obtained by each node at the end of the authentication protocol, for correct processes.

3.6. Alarm messages

For the alarm messages, it was decided that in addition to ensuring the security properties already referred, it would additionally be necessary to get a message acknowledgement (ACK) from the central unit, confirming the receipt of the message.

For this purpose, the central unit when it receives each alarm message, it has to send back a message to the source node acknowledging the receipt of the alert. If the original source node doesn't receive the reply message within a certain period of time, it will repeat the sending of the alert.

This way it is ensured that even in case of error occurrence, or if any node is blocking or corrupting the traffic, the lost messages will be sent again and we have the guarantee that at the end of the process, the alarm message arrives at least once to the central unit.

3.7. Multipath

In addition to the preventive measures for protection of the messages, some resilience techniques were also used so that the system has the ability to withstand internal attacks to the network.

This type of attack can be, for example, a compromised node that performs attacks such as selective routing or black-hole or localized jamming attacks.

To resist these attacks, when a node routes traffic to the gateway, it doesn't always use the same path. Thus, the traffic will go through multiple paths avoiding possible attackers. Another benefit of this is a better distribution of the traffic over the network given that the routing function is not always made by the same nodes.

4. Results

The tests performed over the solution try to answer two key questions: ”What is the impact caused by the solution on each node” and ”is this solution acceptable based on its impact? ”. To do this, the tests try to analyse the impact of the solution mainly in three aspects, memory used, runtime added and the battery consumption.

4.1. Elliptic curve cryptography

The resources consumption was compared over the different sizes of the asymmetric keys available by the library used (128 bits, 160 bits and 192 bits).

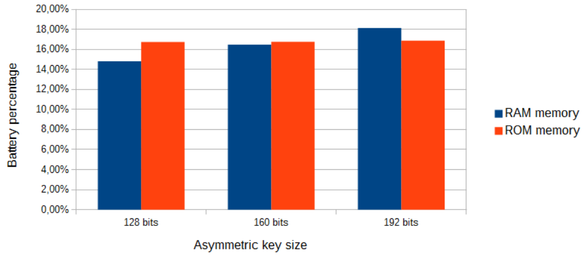

Figure 6: Variation, in percentage, of the memory used for the three asymmetric keys sizes available.

As observed in the figure 6 the variation of memory used for the different sizes of asymmetric keys tested, has more relevance in the required RAM memory.

Overall, these results show that the use of this technique consumes a very significant percentage of the total available memory in each node, whether in terms of RAM and ROM memory.

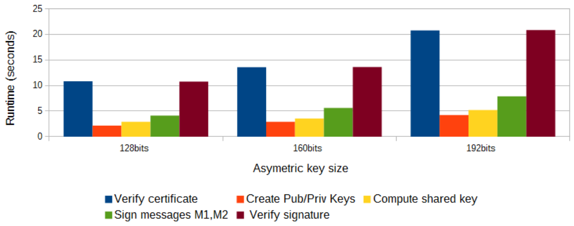

Figure 7: Variation of the average execution time for each of the different ECC operations required in the authentication protocol, again analysed for the different sizes of asymmetric keys.

In contrast to the results for the required memory, in the run-time results of each operation it is easy to note the relevance of the size of the asymmetric keys used, as seen in figure 7.

The results show that the difference between the average time of each operation is substantially doubled when we compare the use of asymmetric keys of 128 bits over 192 bit keys.

4.2. Communication security

In this section we analyse the impact of the operations required to protect the communication.

In terms of memory required to perform such operations, the tests show that the RAM is irrelevant (about 50 bytes), while the required ROM is about 3kb, (about 3% of the total ROM memory available). These values are considered to be acceptable.

For the run-time tests the results show that for the maximum size of the content of the application messages the execution times of each operation are the following:

- Encryption and MAC calculation: 43 ms
- Decryption and MAC validation: 79 ms

In this system, only the encryption and MAC calculation are done by the nodes and the decryption and MAC validation are done by the gateway.

Similar results were obtained for the MAC computation used for protecting the routing messages. Again these results were considered acceptable and feasible.

4.3. Global analyses

Analyse only the impact of each ECC operation it is not enough therefore were conducted also tests to the authentication protocol. For this point were made tests for the runtime and battery consumption required by the process.

The average values obtained from the execution of the authentication protocol between two elements was 70 seconds.

In general terms, 70 seconds is not a significant value since this process is only performed when a node first enters the system and is not required to be repeated on its expected lifetime.

For this test it was also possible to estimate the battery consumption. The results obtained show that a total execution of 500 runs of this process, decrease the battery in about 10%.

These results reinforce the need for gateway not be limited in terms of energy, since they will have to carry out this process at least once for each node of the network.

In contrast the results also show that for the remaining nodes the execution of this process a small number of times does not significantly wear their battery.

About the added bandwidth by the implemented solution, the imposed impact is the following:

- Each authentication protocol needs the exchange of approximately 500 bytes, divided in several messages.
- For each data message sent to the gateway, is added an average of 8 bytes, 4 to the MAC associated with each one, and more 4 bytes in average for padding.
- For each routing protocol message a 4 bytes MAC is added.

Compared with the previous sizes of each message type, data messages have an average increase of 42 %, while the routing messages have an increase of 57 %.

5. Conclusions

This work aimed at ensuring the security of the existing communication in several wireless sensor networks that belong to a system that monitors the geographical location of mobile objects.

The proposed and implemented solution ensures security properties such as authenticity, integrity and confidentiality for point-to-point communication, between each node and the gateway.

On the other hand, it is also ensured the correct functioning of the routing protocol used, being guaranteed the authenticity and integrity of the exchanged messages.

The authentication and key distribution processes are made based on the use of elliptic curve cryptography.

So this work is also a test for the possibility of using this technique in wireless sensor networks with characteristics similar to the ones presented in this system.

The tests showed that the use of asymmetric cryptography, in particular using the technique based on elliptic curves, is possible when used in a limited way. As it is the case in the presented solution, where this technique is used only for the authentication and key distribution processes.

With future improvements for the capabilities of the devices used in wireless sensor networks, it is expected that the elliptic curve cryptography will be used more commonly for these processes.

As exemplified by Bluetooth low energy, a technology widely used in wireless sensor networks and for the so called Internet of things, which in its latest version (4.2), it also uses the ECDH method for establishing a session key between two elements.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal. "Wireless sensor network survey.". In *Computer networks*, 2012.

[2] Gungor, Vehbi C and Hancke, Gerhard P. " Industrial wireless sensor networks: Challenges, design principles, and technical approaches.". In *Industrial Electronics, IEEE Transactions*,2009

[3] Karlof, Chris and Wagner, David " Secure routing in wireless sensor networks: Attacks and countermeasures.". In *Ad hoc networks*,2003

[4] Hartung, Carl and Balasalle, James and Han, Richard " Node compromise in sensor networks: The need for secure systems.". In *Department of Computer Science University of Colorado at Boulder*,2005

[5] Newsome, James and Shi, Elaine and Song, Dawn and Perrig, Adrian " The sybil attack in sensor networks: analysis & defenses.". In *Proceedings of the 3rd international symposium on Information processing in sensor networks*,2004

[6] Zhu, Sencun and Setia, Sanjeev and Jajodia, Sushil " LEAP+: Efficient security mechanisms for large-scale distributed sensor networks". In *ACM Transactions on Sensor Networks (TOSN)*,2006

[7] Gura, Nils and Patel, Arun and Wander, Arvinderpal and Eberle, Hans and Shantz, Sheueling Chang " Comparing elliptic curve cryptography and RSA on 8-bit CPUs". In *Cryptographic Hardware and Embedded Systems-CHES*,2004

[8] Gaubatz, Gunnar and Kaps, Jens-Peter and Sunar, Berk " Public key cryptography in sensor networksrevisited". In *Security in Ad-hoc and Sensor Networks*,2005

[9] Malan, David J and Welsh, Matt and Smith, Michael D " A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography". In *Sensor and Ad Hoc Communications and Networks*,2004

[10] Wander, Arvinderpal S and Gura, Nils and Eberle, Hans and Gupta, Vipul and Shantz, Sheueling Chang " Energy analysis of public-key cryptography for wireless sensor networks". In *Pervasive Computing and Communications*,2005

[11] Oliveira, Leonardo B " TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks.". In *Computer Communications*,2011