Wireless Sensor Network Attacks and Security Mechanisms - A short survey

David Martins, Hervé Guyennet

SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks **00**: 1–11 (2009)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.0000

Attacks and security mechanisms in wireless sensor networks : a survey

David MARTINS*, Hervé GUYENNET*
LIFC, University of Franche-Comté, France

Summary

Wireless sensor networks are specific ad-hoc networks. They are characterized by their limited computing power and energy constraints. This paper proposes a survey on security in this kind of network. We show what are the specificities and vulnerabilities of wireless sensor networks. We present a list of attacks, which can be found in these particular networks and different solutions made by the scientific community to secure them. Finally we take the opportunity to present two of the most representative secure protocols, SPINS and TinySEC. Copyright © 2009 John Wiley & Sons, Ltd.

KEY WORDS: wireless sensor network, security, vulnerability, secure protocol

1. Introduction

The facilities of sensors deployment and the reduction of costs have increased the use of wireless sensor networks. Today we find this kind of network in the industrial monitoring, the record of environmental data [1] [2], the home automation [3], the fire detection [4], the medical [5] or even in the military. Most of these applications are deployed to monitor an area and to have a reaction when they record a critical factor. Data doesn't need to be confidential in areas such as home automation or the capture of environmental events. But confidentiality of data can be essential in other applications, such as for medical diagnostic of a patient in an hospital or for the security of a territory in the military. An example of these critical applications exists in the CodeBlue project [5], where sensors collect information from a patient in a hospital. Other examples also exist in military applications such as monitoring a zone of war, registration of health status or position of troops. In these two examples, the confidentiality of the information is essential, from a legal point of view in the first case, and a security point of view in the second. This security is obviously endangered by the medium used, radio waves, but also by specific vulnerabilities of wireless sensor networks.

The solutions used in conventional ad hoc networks, can not be applied in wireless sensor networks, because the sensors are limited by their battery and computing power. Specifically, cryptographic solutions currently used such as asymmetric key solutions are too complicated to be calculated by processors of current sensors. In addition, all security protocols must limit the number of messages necessary for its proper functioning, because communication between sensors is the main source of energy consumption in wireless sensor networks.

These constraints [6] require us to rethink effective current solutions in terms of speed of calculation and energy consumption, in order to secure wireless sensor

*Correspondence to: LIFC, University of Franche-Comté, 16 route de gray - 25030 BESANCON Cedex - FRANCE
Tel : +33 (0)3 81 66 64 55 - Fax : +33 (0)3 81 66 64 50 Email : dmartins@lifc.univ-fcomte.fr ; hguyennet@lifc.univ-fcomte.fr

networks without consuming their energies.

In this paper we present the specificities of wireless sensor networks and their vulnerabilities that we list. Then we explain the most common solutions proposed by the scientific community and existing secure protocols. This paper is organized as follows : section 2, we describe specificities of wireless sensor networks, focusing on their vulnerabilities and their architecture. In section 3, we list the attacks that threaten wireless sensor networks. In section 4, we present existing solutions to counter these attacks and the mechanisms which are used. In section 5, we introduce two secure protocols : SPINS [7] and TinySEC [8]. Finally in Section 6, we conclude on future advances.

2. Architecture of wireless sensor networks

Wireless sensor networks are specific ad-hoc networks [9] with a larger number of nodes, a limited energy and a lower computing power. We are going to introduce these particularities in this part.

2.1. Topology

Figure 1 shows the topology which prevails in wireless sensor networks : a set of nodes (each node is a sensor), which are raised on an heterogeneous zone, on objects or moving individuals. All these nodes communicate with each other. Each node can communicate with other nodes which are located in its coverage area.

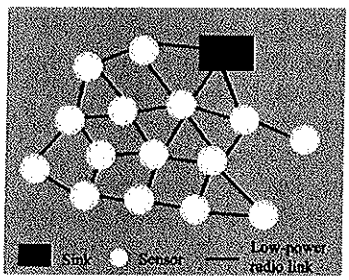

FIG. 1. *Topology of a wireless sensor network*

Generally, wireless sensor networks are connected to one or several sinks. These sinks have mission to collect information circulating on the network, and store them or send them directly via an Internet or a GSM connection. There can be for example a laptop or a sensor with a greater power. They monitor the network and make a link between user and network.

2.2. Routing

To limit the number of communications, because they consume energy, wireless sensor networks need protocols with effective routes [10]. A solution is to use clustering, which divides networks in many clusters. In each cluster, a cluster-head is elected and this cluster-head collects data from the other nodes of the cluster. It transmits this data to the other clusters and inversely. The election of the cluster-head is made by choosing, for example, the node with the most important energy. The objective is to extend the life of the network.

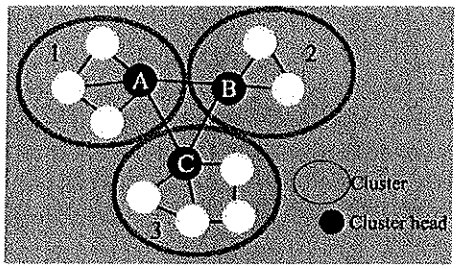

FIG. 2. *Clusterisation's example*

Figure 2 shows an example of clustering network, where nodes A, B, C were elected respectively cluster-head of clusters 1, 2 and 3. We have to take care of other problems to limit the number of communications, such as problems of implosion and overlap [11]. Figure 3 shows the problem of implosion, where node A sends data to its neighbours B and C. Without an effective protocol, both send the same data to their neighbour D. The energy used will be double and we will have a redundancy of this data. We can also have a problem of collision, if the two nodes send data at the same time.

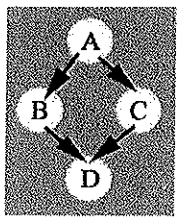

FIG. 3. *Implosion's problem*

The overlap problem is shown figure 4, where two nodes, A and B, monitor respectively two areas, 1 and 2, and share the same area 3. If they detect the same information in the same time in area 3, without

an effective protocol, they will send the same data at the same time to their neighbour C. We have a redundancy of the data, a double consumption and maybe a problem of collision.

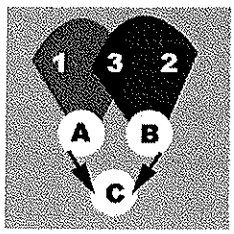

FIG. 4. *Overlap's problem*

These two problems show us the need of protocols with effective routings, and with a negotiation between nodes before they send data.

2.3. Fault tolerance

In wireless sensor networks, one or several sensors can be deficient. Sensors are sensitive to an alteration of state, like climatic phenomena (humidity, temperature, electromagnetism) or because their battery are low. The network have to be able to detect this kind of error and correct it. It can modify the routing table to find an another route to send data. Sensors should be able to detect deficient sensors, which send wrong data.

2.4. Scalability

The number of sensors used for application could be some to thousands. The number could be more in some networks. This scalability is one of a main asset of wireless sensor networks, because they can monitor a large area. Protocols have to be efficient whatever the number of sensors.

2.5. Limited energy

Most of sensors use a battery. But this battery is actually limited (from some days to some years). Wireless sensor networks are often used to monitor an area. Sensors are deployed to never be recovered or modified. Moreover, it will be difficult in a network with thousands sensors, to find a sensor, which has a deficient battery and to change it. To limit their consumption, sensors have a period of sleep. Communications and calculations use more energy. That is why we have to limit communications and calculations to economize energy.

2.6. Low power

Despite the current progress in the fabrication of most powerful sensors, sensors have a low power of calculation (for example 16 MHz of frequency and 128Ko of memory for MicaZ). This low computing power does not allow to use complex algorithm for sensor networks, like complex cryptography. Moreover, most of applications using wireless sensor networks need a large number of sensors. That is why, it is important these sensors are cheap, but cheap sensors have a lower computing power. The weakness of computing power also increases the latency of the network. If a sensor have to do many calculations, its responsiveness will significantly deteriorate.

2.7. Medium

The medium used is radio waves. We find generally three technologies in wireless sensor networks :

- Wi-Fi : it provides the most important bandwidth, but its energy cost is too important for sensors that do not require big communications.
- Bluetooth : it is used in wireless sensor networks, but for specific applications, because it limits the number of nodes.
- Zigbee : It is the medium of communication, which is the most suited to wireless sensor networks, with a low-cost communication, it allows a very large number of nodes in the network (60 000 nodes).

3. Vulnerability

The specificities of wireless sensor networks (low power, limited energy, etc) expose them to many threats. If some of these threats could be found in all ad-hoc networks, others are specific to wireless sensor networks. For most of them, they attack the limited energy sensors.

An attacker could try to capture some data in the network to listen the network, if these data is sent with no encryption. In such a case, we call a passive attack, an attack that doesn't modify the data. We call an active attack, an attack that modify or delete some data. Following of this section, we make a list of the most current attacks in wireless sensor networks.

3.1. Eavesdropping

This passive attack consists to listen the network to intercept information on the network. This attack is easy to make, if data are not encrypted. Since this

DOI: 10.1002/sec

attack doesn't modify the data, it is difficult to detect it.

3.2. Message's injection

The attacker will send many messages on the network. The aim may be to send false information or simply to saturate the network.

3.3. Flooding

An attacker will use one or many malicious nodes or something else with a powerful signal, to send regularly some messages in the network, to flood it. This is an active attack such as deny of service, to consume the energy of nodes in the network [12].

3.4. Node compromise (Destruction or theft)

Theft or the destruction of one or many nodes is the simplest physical attack in wireless sensor networks. Sensors are deployed in an area, which can not always be monitored. One physical person can steal one or many nodes, or can destroy them. The network can not work if a node, that link two nodes, is destroyed or stolen. Moreover, if a node is stolen, an attacker can capture some data in this node, like cryptographic data. He can also reprogram the sensor, which can become a malicious node in the network and will spy the network, like explained in [13], [14] and [15].

3.5. HELLO Flooding

Many discovery protocols in ad-hoc network use the sending of Hello message to discover neighboring nodes and to automatically create a sensor network. With an attack of Hello Flooding, an attacker can use a device with large enough transmission power could compromise every node of the network that this device is its neighbor.

In [16], we find an example of this attack, showing picture 5, of a malicious node with a powerful connection, which sends HELLO messages to nodes of the network. The neighbouring nodes V believe that the malicious node is a neighbour and will send data to it, but because they are far away, they send packets into oblivion.

3.6. Radio jamming

An attacker sends some radio waves at the same frequency that it used by wireless sensor networks [12]. The nodes can not communicate if the transport medium is flooded by radio interferences.

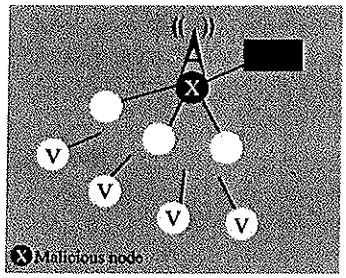

FIG. 5. *HELLO Flooding attack*

3.7. Black Hole Attack

The black hole attack consists at first to insert a malicious node in the network [16]. This malicious node, in several ways, will change routing tables, to force a maximum of neighboring nodes to send data to it. After that, like a real black hole in space, all recovered data will never be sent back by the malicious node. The picture 6 shows a malicious node X, which has created a black hole attack. It has changed the routing table of clusters 1, 2, 3 and 4, which send their data to it. In this case, the black hole created by the malicious node X, will never send data, and the communication between the four clusters becomes impossible.

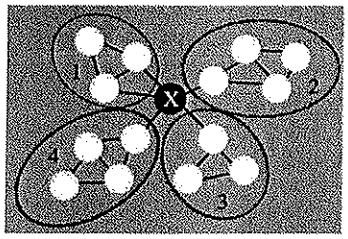

FIG. 6. *An example of black hole attack in a clustering network*

3.8. Selective Forwarding (Grey hole attack)

This is a variant of the black hole attack [16]. Like in the black hole attack, an attacker will insert a malicious node in the network and this node will change the routing to capture data around it. Unlike the black hole, the attack of selective forwarding relays information. For example, the malicious node will relay all information concerning the routing and it will not relay data, which is critical. That is why, this kind of attack is more difficult to detect than the black hole attack. If the malicious node works normally, it can not easily be detected.

3.9. Wormhole attack

This attack needs to insert in the network at least two malicious nodes [17]. These nodes are connected by a powerful connection such as a wired liaison or a powerful wireless signal.

This attack wrongs the other nodes of the network on the distance between the two bad nodes, and proposes a route quicker. Generally the routing protocols search the route with the shortest number of hops. In a wormhole attack, the two malicious provide to achieve a distant position with an unique hop. This possibility will wrong other nodes on the real distances that separate the two malicious nodes. The nodes will choose this shortest route for send their data, and they will send their information to the malicious nodes. The wormhole attack is showed in the figure 7. Two malicious nodes X1 and X2, connected by a powerful connection, make a wormhole. The nodes A and B will choose the shortest route provided by the wormhole for send their data. Data will be captured by the malicious nodes and the attacker.

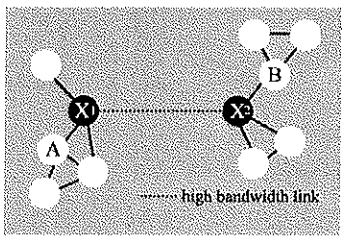

FIG. 7. *A wormhole attack*

3.10. Sinkhole attack

A malicious node will attack directly the data, which circulate near the sink, because the sink is the point, which catch the maximum of data on the entire network [16]. To do this attack, the malicious node will offer the quickest route to reach the sink, using a powerful connection, as shown in figure 8.

Nodes, which are near the malicious node, will send data for the sink to it. All information, which is sent from these nodes to the sink, may be captured by the attacker.

An attacker can make an attack even more powerful. The attacker can use wormhole attacks associated with a sinkhole attack. The aim is to use these wormholes to cover all the nodes in the network, as shown in figure 9. The malicious nodes X1, X2, X3 are connected with powerful connections and make wormholes. X3

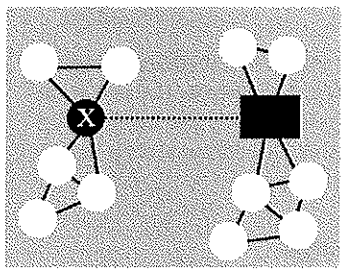

FIG. 8. *A sink hole attack*

is connected to the sink with a powerful connection to make a sinkhole attack. This is known as a sphere of influence exerted by the attacker on the network, because it is then able to recover all the information circulating in the wireless sensor network.

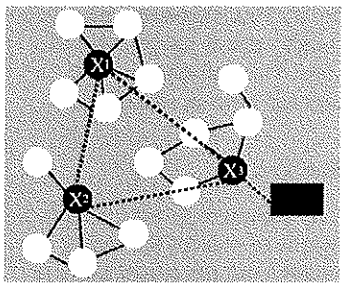

FIG. 9. *An example of sinkhole attack using wormhole attacks*

3.11. Specific sensor attack

This kind of attack depends on the kind of sensor. An attacker will modify by physical means the response of a sensor. For example, it can light a flame in front of a thermal sensor or light a lamp in front of a brightness sensor. The aim is to deceive sensor, and then send or record false information on the network, or simply to react quite a long time a node or a network, so that they consume their energy.

3.12. Sybil attack

A Sybil attack [18] is a malicious sensor which is masquerading as multiples sensors. It will modify the routing table, which will be wrong. A malicious node, which is masquerading as multiple nodes, can have an important advantage for a cluster head election. With a higher number of votes, it may compromise its neighboring nodes to become a cluster head.

3.13. Infinite loops

An attacker can use two or more malicious nodes to send infinitely packets on the network. Because these messages will be endlessly sent by the network like a ping-pong game, sensors will consume their energy and the network will saturate.

3.14. Message alteration

A malicious node will catch a message and change it. It will add wrong data (about the receiver, the sender or information itself) or delete some packets. The message will be illegible.

3.15. Slowdown

An attacker can use some malicious nodes to slowdown the network. It can use a selective forwarding attack to do it. This slowdown may be crucial if the network sends critical information like fire detection or intrusion. This information will be slowed so that the attacker can have an advantage.

3.16. Sleep deprivation torture

An attacker sends many messages or asks calculations to a sensor. The aim is to prevent the sensor to sleep to consume his energy until the sensor become out of order. This active attack prevents a sensor to sleep in different ways [19]. If the sensor can not sleep, it will consume very quickly its battery to be out of service.

4. Security Mechanisms

To counter these attacks, that threaten wireless sensor networks, several researches are trying to find appropriate solutions. These solutions have to take into account the specificities of wireless sensor networks. We have to therefore find simple solutions that allow securing the network while consuming as little energy as possible and that these solutions are adapted to a low computing power.

Among these solutions, there are mechanisms such as the data partitioning, using key management, intruder detection by location or even trust management.

4.1. Data Partitioning

[20] and [21] give a solution to prevent the capture of information in wireless sensor networks by the data partitioning. The aim is to divide the information into several parts.

If a sensor tries to send information, it will cut the data into several packets of fixed size. Each packet will be sent on a different route. Packets will pass in different nodes. Packets will eventually be received by the sink, which could then bring them together to reproduce information. All these parts will be received by the sink, which will assemble data to have the information. If someones want to read the information, he needs to have all the parts. The problem of this solution is that it consumes more energy, because data come from more sensors. An attacker have to catch all packets of a message if it want to know the information. In order to do it, it has to be able to listen the entire network. It is more complicated for an attacker to have the information, but this solution increases the energy's consumption (with a risk of overloading treatment), because it needs to use a number of nodes more important to communicate.

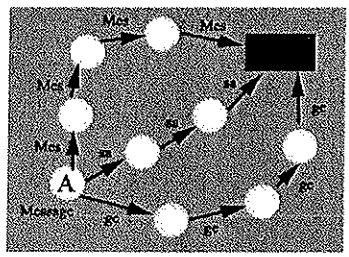

FIG. 10. *An example of partitioning data*

An example of this solution is represented by the figure 10, where a sensor A divides a message into 3 packets which are going to follow 3 different routes.

4.2. Key management

As we have explained before, it is not possible in wireless sensor networks to use complex encryption methods like use of assymetric keys. The low computing power of sensor processor does not allow it, and when it permits, the computing time is too long and incompatible with a responsive network. The table 1 is an example of time execution made by [22].

However, it is possible to use simple key management with symmetric keys as shown in [23].

Four types of cryptography are used :

- Global key : one key is shared by the entire network. To send a message, information is encrypted with this key. Once the message is

Sensor node	RSA-1024 Performance	ECC-160 Performance
MICA2DOT	22.00 s	1.60 s
MICA2/MICAz	12.00 s	0.87 s
TelosB	5.70 s	0.5 s

TAB. I. Time needed by the sensor nodes to perform SSL/TLS handshake

received, it can be decrypted with the same key. This solution is an energy-efficient solution of cryptography . The information is encrypted once by the sender and decrypted only once by the receiver. However, it's the solution with a limited security. If an attacker could find the key, he is able to hear the entire network which communicates with this unique key. To know this key also allows the possibility to insert a malicious node in the network.

- Pair wise key node : Each node has a different key to communicate with a neighboring node which shares this key. So if one node has "n" neighbours, it will have "n" key stored to communicate with its neighbours. In this solution, a node that will send a message have to encrypt the message with key neighbour who will receive the information. The neighboring node will decrypt information to re-encrypt with the key corresponding to the following receiver. This solution increases considerably the security of the network, because if an attacker discovers a key, this key is just able to communicate with two nodes, and limits the power of this attack. The attacker have to find all pair wise key to listen the entire network. However, this technique is not energy-efficient especially in time of calculation, since each pair of nodes which transmits information must encrypt and decrypt a message. The lifetime of the network and its rate is going to be reduced.

- Pair wise key group : Each group or cluster has a key to communicate between nodes in the cluster. Cluster-heads use a single key for all cluster-heads to communicate or use a pair wise key to communicate between two cluster-heads. This solution is an hybrid solution to the first two techniques of encryption and offers a compromise between security and energy efficiency.
  It may limit the number of encryption in communications. However it increases the work of clusters heads, which have to decrypt and encrypt the information. To be effective, we have to ensure that cluster-heads change regularly in order not to consume all the energy of the cluster head.

- Individual key : In this solution, each node has its own key to encrypt data. This key is only known by the sink. As a consequence, a message sent by this node goes around hidden on the network until it reaches the sink.
  This solution is one of the better way to limit the consumption of the network. Nevertheless, this solution secures only communication between a node and the sink.

4.3. Generation

One solution proposed by [24] is to use a key generation. Each period or generation, the sink sends a new key to the whole network. This key is used as a certificate to each node, to prove it belongs to the network. If an unidentified node tries to come into the wireless sensor network and if it does not have this key generation, the network will refuse its integration.

Another benefit of this technique is that it limits substitution attacks of a sensor and the reprogramming of the sensor to be reused in the network. If this node is removed at the moment 0 with the key generation K(0), by the time the attacker reprograms to bring it back into the network, it will have elapsed time "x". When the sensor will be back in the network, key of the new generation will be then K(x). The malicious node will ask its neighboring nodes to return in the network with the key K(0) and not K(x) because he was unable to receive this new key. As K (0) ! = K (x), neighboring nodes will not accept its request and the malicious node won't join the network.

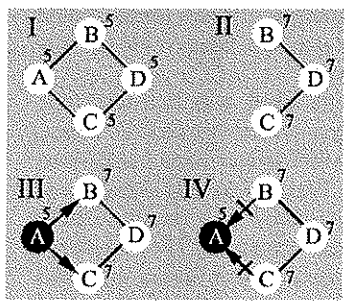

FIG. 11. *Detection of a malicious node with key generation*

An example is given in figure 11, where four sensors A, B, C, D are part of a sensor network which communicate with a symmetric pair wise key node. In Phase I, sensors have a key generation 5. In Phase II, the A node is removed by an attacker, and during its absence on the network, the sink forward a new generation key 7. In Phase III, the sensor A which has been reprogrammed and reinserted into the network makes an insertion request into the network to sensor B and sensor C. In Phase IV nodes B and C reject the request of A, because comparing their key generation, they found that they are different.

This technique is energy-efficient and easy to deploy. However it directed only closed networks, which can not accept new nodes. Moreover, there is the problem of a node, which can not receive a key to progress time.

4.4. Localization

A mechanism used to detect malicious nodes and especially wormhole attacks, is to use a technique for locating geographically a node, as proposed by [25] and [26]. For this solution, the wireless sensor network have to be equipped with specific sensors called beacon, which are sensors that knowing their geographical position. They use for example a GPS equipment.

With the localization, if a sensor requests to join the network, beacons will receive this request and be able to estimate its location with their listening area. Beacons will make a grid of their respective listening area, and each beacon node, which received the request for entry in the network, will vote for an area of the grid that is able to hear. The area which receives the greatest number of votes will be supposed to be the area where is the new sensor.

Figure 12 shows an example of election between 4 beacon sensors A, B, C and D. They make a grid of their area listening. They vote for each zone of the grid. They can estimate the position of the sensor which they are able to estimate. The new sensor should be found in the area with the most votes, in this example area with 3 votes.

In case of a wormhole attack with two malicious nodes, they will be geo-located by beacon nodes, which are going to be to able to determine the distance between the two nodes. They can see if this distance is higher than the normal distance for a communication in one hop, and then detect the attack. The problem of this solution is that it needs beacon sensor equipped with GPS device (and it is more expensive) or pre-calibrated on the ground.

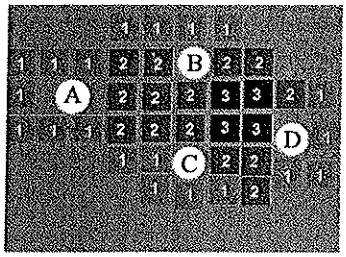

FIG. 12. *Localization with beacons*

4.5. Trust management

One solution proposed by [27], [28], [29], [30], [31] and [32] is to use the mechanisms of trust and reputation that can be found in peer to peer networks [33], community networks or even market websites like Ebay .

In this kind of network as in wireless sensor networks, it is hard, because of the large number of nodes, to know what node can be a malicious node. To detect and protect the integrity of the network, each node of the network will monitor its neighboring nodes and their actions over time. Depending on actions taken by its neighboring nodes, a node will increase a level of trust of these nodes, based on its reputation. When a node does not carry out a request, its level of trust will fall. If this node always sends correctly data, its level of trust will increase.

With the help of these levels of trust, a node will then choose the most secure route for sending data. Instead of going through the fastest route (number of hops or geographical distance), the node will choose to send its data via nodes with the highest level of trust (the safest route).

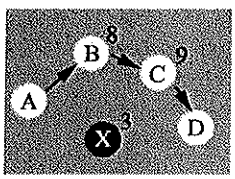

FIG. 13. *Routing with trust management*

This mechanism is represented figure 13, where a node A has to send data to a node D. Instead of going through the shortest route which passes through X, which is a node with a level of trust of 3 (level is between 0 and 10, 10 is the highest level of trust), that is potentially a malicious node, the node A will send information via nodes B and C that they have

a level of trust of 8 and 9 and which propose the safest route. With this solution, it also uses a technique called watchdog [34]. In the mechanism of watchdog, each communication between two nodes A and B is heard by an intermediate node C, located in the area of communication. The node can oversee if this communication has been carried out, as shown in Figure 14.

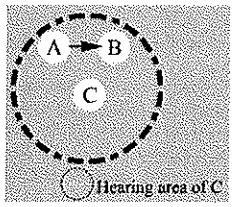

FIG. 14. *An example of watchdog*

These techniques make it possible to eliminate nodes that are potentially dangerous, and protect data to go through these nodes. Solutions based on the trust management are energy-efficient, and can not use cryptography in a network, which doesn't need a high security. But for networks that require maximum security, they are not always adapted. Thus a malicious node that just record data on the network and, would behave in the normal way, is hardly detectable.

5. Security protocols

Among the security protocols, SPINS [7] and TinySEC [8] are currently the most widely used. This iw why, we choose to describe the security mechanisms used by these two protocols in this section.

5.1. SPINS

SPINS (Security Protocols for Sensor Networks) is a protocol based on two blocks of security : SNEP and μTESLA [35].

SNEP uses two security mechanisms. The first is to encrypt to ensure the confidentiality of data and the second is to use a code authenticity of messages MAC (Message Authentication Code) to ensure authentication and data integrity between two entities.

With SNEP, for each first exchange of data between two nodes, the sender node adds a string of random bits in the beginning of the message, also called the initial vector (IV). Then it encrypts the message with a DES-CBC function. This technique prevents an attacker, who is listening to the network and who knows the encryption key, from understanding the message, even if it has got an equivalent of the message cleared and encrypted. The two nodes then share a counter allowing them to use cipher blocks in counter mode (CTR). They stop using initial vector. For each block exchanged, the counter is incremented. An attacker can decrypt the information if he can see exactly the same message several times encrypted. Using a random initial vector and a counter prevent this possibility. A single message will be followed unencrypted either by a string of bits or by a counter always different. μTESLA allows the use of broadcast authenticated. It is a version suited to wireless sensor networks of protocol TESLA [36]. μTESLA uses a symmetrical authentication linked to an asymmetrical method where the symmetrical keys are disclosed over time. To enable this authentication, it is necessary that the sink and the different nodes be loosely synchronized. The sink adds a MAC key in the packets to send, which remains secret at this moment. A node receiving this packet can verify that the MAC key has not been disclosed through its synchronized clock yet. If it has not been disclosed, it can be deduced that only the sink knows the MAC key and an attacker was unable to alter the message during its transit. It can then store the packet in its buffer until the next disclosure of the key. When the key is released, it will decrypt the message and verify its authenticity.

5.2. TinySEC

TinySEC is a security package integrated in operating system TinyOS [37].

The aim of this link layer is to detect unauthorized packets while they are injected for the first time into the network, to prevent their spread in the network that would generated by communications, to a loss of energy. TinySEC establishes authentication mechanisms (with the use of MAC key), encryption of information and protection against duplication of information.

To allow greater freedom of action, TinySEC offers two different security options :

- TinySEC-Auth : the security provided only authentication data. The data are not encrypted, but are sent with a MAC key to ensure the authenticity of the sender.
- TinySEC-AE : the security concerns authentication and data encryption. The data are encrypted and sent with a MAC key generated from the data encrypted.

For authentication and encryption TinySEC uses a building cipher block channels with CBC-MAC to create and verify the key MAC. This method is particularly suitable for sensor networks because it does not require a large memory. However CBC-MAC is not a secure solution for packets with various sizes because it can be easily circumvented.

6. Conclusion

Recent technological advances in wireless sensor networks have allowed widespread use of this kind of network. But information is still vulnerable to many attacks, which are often specific to ad-hoc networks, or even exclusive to wireless sensor networks.

Some solutions are proposed by the scientific community to counter these attacks. But these solutions have not yet a maximum security. The low computing power of sensors and especially their limited energy are obstacles to the deployment of advanced techniques, and we are still searching for solutions, which can accomodate security, would meld life-time and a good latency of sensors. We have to remember that they are not an only secure solution in wireless sensor networks. The level of security in wireless sensors networks depends on the application that we have to deploy.

Références

1. Kim S, Pakzad S, Culler DE, Demmel J, Fenves G, Glaser S, Turon M. Wireless sensor networks for structural health monitoring. *SenSys*, Campbell AT, Bonnet P, Heidemann JS (eds.), ACM, 2006 ; 427–428.
2. Welsh M. Deploying a sensor network on an active volcano. *USENIX Annual Technical Conference, General Track*, USENIX, 2006.
3. Baker CR, Armijo K, Belka S, Benhabib M, Bhargava V, Burkhart N, Minassians AD, Dervisoglu G, Gutnik L, Haick MB, *et al.*. Wireless sensor networks for home health care. *AINA Workshops (2)*, IEEE Computer Society, 2007 ; 832–837.
4. Thierry AS, Francois SJ, de Gentili Emmanuelle, Bernadette C. Using wireless sensor network for wildfire detection. a discrete event approach of environmental monitoring tool. *Environment Identities and Mediterranean Area, 2006. ISEIMA '06. First international Symposium on*, 2006.
5. Malan D, Fulford-Jones T, Welsh M, Moulton S. Codeblue : An ad hoc sensor network infrastructure for emergency medical care. *International Workshop on Wearable and Implantable Body Sensor Networks*, 2004.
6. Carman DW, Krus PS, Matt BJ. Constraints and approaches for distributed sensor network security. *Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD*, 2000.
7. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. Spins : Security protocols for sensor networks. *Wireless Networks* 2002 ; **8**(5) :521–534.
8. Karlof C, Sastry N, Wagner D. Tinysec : a link layer security architecture for wireless sensor networks. *SenSys*, Stankovic JA, Arora A, Govindan R (eds.), ACM, 2004 ; 162–175.
9. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks : a survey. *Comput. Netw.* 2002 ; **38**(4) :393–422, doi :http://dx.doi.org/10.1016/S1389-1286(01)00302-4.
10. Al-Karaki JN, Kamal AE. Routing techniques in wireless sensor networks : a survey. *IEEE Wireless Comm.*, vol. 11, 2004 ; 6–28.
11. Heinzelman WR, Kulik J, Balakrishnan H. Adaptive protocols for information dissemination in wireless sensor networks. *MOBICOM*, 1999 ; 174–185.
12. Wood A, Stankovic J. Denial of services in sensor networks. *IEEE Computer* October 2002 ; .
13. Parno B, Perrig A, Gligor VD. Distributed detection of node replication attacks in sensor networks. *IEEE Symposium on Security and Privacy*, IEEE Computer Society, 2005 ; 49–63.
14. Wang X, Gu W, Schosek K, Chellappan S, Xuan D. Sensor network configuration under physical attacks. *ICCNMC, Lecture Notes in Computer Science*, vol. 3619, Lu X, Zhao W (eds.), Springer, 2005 ; 23–32.
15. Hartung C, Balasalle J, Han R. Node compromise in sensor networks : The need for secure systems. *Technical Report CU-CS-988- 04, Department of Computer Science, University of Colorado at Boulder*, 2004 ; .
16. Karlof C, Wagner D. Secure routing in wireless sensor networks : attacks and countermeasures. *Ad Hoc Networks* 2003 ; **1**(2-3) :293–315.
17. Hu YC, Perrig A, Johnson DB. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications* 2006 ; **24**(2) :370–380.
18. Newsome J, Shi E, Song D, Perrig A. The sybil attack in sensor networks : analysis & defenses. *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*, 2004 ; 259–268, doi :10.1109/IPSN.2004.1307346.
19. Stajano F, Anderson RJ. The resurrecting duckling : Security issues for ad-hoc wireless networks. *Security Protocols Workshop, Lecture Notes in Computer Science*, vol. 1796, Christianson B, Crispo B, Malcolm JA, Roe M (eds.), Springer, 1999 ; 172–194.
20. Thomas Claveirole MA Marcelo Dias De Amorim, Viniotis Y. Résistance contre les attaques par capture dans les réseaux de capteurs. *JDIR*, 2007.
21. Deng J, Han R, Mishra S. Countermeasures against traffic analysis attacks in wireless sensor networks. *SECURECOMM '05 : Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, IEEE Computer Society : Washington, DC, USA, 2005 ; 113–126, doi :http://dx.doi.org/10.1109/SECURECOMM.2005.16.
22. Piotrowski K, Langendoerfer P, Peter S. How public key cryptography influences wireless sensor node lifetime. *SASN '06 : Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, ACM : New York, NY, USA, 2006 ; 169–176, doi :http://doi.acm.org/10.1145/1180345.1180366.
23. Zhu S, Setia S, Jajodia S. Leap - efficient security mechanisms for large-scale distributed sensor networks. *SenSys*, Akyildiz IF, Estrin D, Culler DE, Srivastava MB (eds.), ACM, 2003 ; 308–309.
24. Bekara C, Laurent-Maknavicius M. A new resilient key management protocol for wireless sensor networks. *WISTP, Lecture Notes in Computer Science*, vol. 4462, Sauveron D, Markantonakis C, Bilas A, Quisquater JJ (eds.), Springer, 2007 ; 14–26.
25. Gruteser M, Schelle G, Jain A, Han R, Grunwald D. Privacy-aware location sensor networks. *HotOS*, Jones MB (ed.),

USENIX, 2003 ; 163–168.
26. Liu D, Ning P, Du W. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. *ICDCS*, IEEE Computer Society, 2005 ; 609–619.
27. Yan Z, Zhang P, Virtanen T. Trust evaluation based security solution in ad hoc networks. *NordSec 2003, Proceedings of the Seventh Nordic Workshop on Secure IT Systems*, 2003.
28. Zhu H, Bao F, Deng RH, Kim K. Computing of trust in wireless networks. *Proceedings of 60th IEEE Vehicular Technology Conference, Los Angles, California*, 2004.
29. Niki P, V CG. Cluster-based reputation and trust for wireless sensor networks. *Consumer Communications and Networking Conference, 2007. CCNC 2007. 4th IEEE*, 2007 ; 604–608.
30. Ren K, Li T, Wan Z, Bao F, Deng RH, Kim K. Highly reliable trust establishment scheme in ad hoc networks. *Computer Networks* 2004 ; **45**(6) :687–699.
31. Ganeriwal S, Srivastava MB. Reputation-based framework for high integrity sensor networks. *SASN*, Setia S, Swarup V (eds.), ACM, 2004 ; 66–77.
32. Oleshchuk V, Zadorozhny V. Trust-aware query processing in data intensive sensor networks. *SENSORCOMM '07 : Proceedings of the 2007 International Conference on Sensor Technologies and Applications*, IEEE Computer Society : Washington, DC, USA, 2007 ; 176–180, doi :http://dx.doi.org/10.1109/SENSORCOMM.2007.100.
33. Liang Z, Shi W. Pet : A personalized trust model with reputation and risk evaluation for p2p resource sharing. *HICSS*, IEEE Computer Society, 2005.
34. Roman R LJ Jianying Zhou. Applying intrusion detection systems to wireless sensor networks. *Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE*, 2006 ; 640–644.
35. Liu D, Ning P. Multilevel μtesla : Broadcast authentication for distributed sensor networks. *Trans. on Embedded Computing Sys.* 2004 ; **3**(4) :800–836, doi :http://doi.acm.org/10.1145/1027794.1027800.
36. Perrig A, Canetti R, Tygar D, Song D. The tesla broadcast authentication protocol 2002.
37. http ://www.tinyos.net/ 2008 ; .

DOI: 10.1002/sec