Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol

David Martins, Hervé Guyennet

Attacks with Steganography in PHY and MAC Layers of 802.15.4 Protocol

David Martins and Hervé Guyennet
Computer Science Department
University of Franche-Comté, France
Email: {dmartins,hguyennet}@lifc.univ-fcomte.fr

***Abstract*—Wireless sensor networks are threatened by numerous attacks. Therefore, security is now becoming an important new path of research and attempts to counter these attacks. However, even if research finds solutions to counter known attacks, we show in this article that there is a threat in wireless sensor networks by using the 802.15.4 protocol. It is possible to hide data in PHY and MAC layers with steganographic techniques. In this article, we explain what steganography is, how we can use it in the layers of 802.15.4 protocol, how an attacker can do an attack and what we can do to detect this kind of threat.**

***Index Terms*—wireless sensor networks, steganography, security, 802.15.4 protocol, MAC layer**

I. Introduction

Steganography is an old technique that has existed since antiquity. Herodotus, a Greek historian who lived in the 5th century B.C., relates how the Greeks sent and received warnings of enemy movements using a message underneath the wax of a writing tablet. Other examples were the use of secret ink to hide information on a white paper or the use of micro-dot by intelligence agencies in World War 2.

The word steganography comes etymologically from the Greek words *Stegano*, meaning *I cover*, and *Graphô*, meaning *I write*, and is literally *cover what I write* - or more simply, hide data. If cryptography is to encrypt and render a data unreadable, steganography is the way to hide the existence of this data.

In this paper, we show that it is possible to use steganographic techniques to hide the existence of data in the 802.15.4 protocol. This protocol is a protocol widely used in wireless sensor networks. This protocol specifies the PHY and MAC layers of communication, because it provides an energy-efficient solution for communication between wireless sensors. Zigbee [1], the most used protocol in wireless sensor networks, uses this 802.15.4 protocol for the communication layer. We explain in this article that this threat exists and uses 802.15.4 protocol fields to hide data in the network and create a steganographic channel. By using steganographic methods, this data becomes undetectable in the wireless sensor network if there is not a steganographic detection policy.

In Section 2 of this paper, we present previous work on steganography and specifically in communication protocols. In Section 3, we show the possibility of hiding data in wireless sensor networks by using a PHY layer field of the 802.15.4 protocol. In Section 4, we describe different possibilities for hiding data in MAC layer fields of the 802.15.4 protocol. In Section 5, we analyse risks and limits of this kind of attack. In Section 6, we discuss about solutions for protecting wireless sensor network against steganography attacks in layers of the 802.15.4 protocol. Finally, we conclude in Section 6.

II. Related work

The aim of steganography consists of embedding data (text, movie, picture, etc...) called the secret message, in another media or support [2]. The support where the data is hidden is named the cover object. Once the secret message is embedded in the cover message, the result is called a stego object. For example, we can hide a picture in another picture, and in this latter picture, we cannot see that the first picture is hidden inside.

When we speak about steganography, we refer to the analogy of Alice and Bob [3]. Alice and Bob are in jail and are monitored by a warden, Wendy. If Alice wants to send a message to Bob, this message must go through Wendy. If Wendy sees that the message contains an important message (for example the hour of an escape), Wendy will never give the message to Bob. Therefore, Alice should find a way to hide information in the message without Wendy seeing it. For example, Alice will hide a message in another

message. If we read every other letter, we can read the hidden message; but if Wendy reads this message, she will not see the hidden message. In steganography, this example shows that the steganographic method must be kept secret (if Wendy knows the steganographic technique, she can read the message) and all participants who want to communicate should know this method to hide and to read the data. This example of Alice and Bob can be implemented in wireless sensor networks: where Alice and Bob would be two sensors, and Wendy would be another sensor or a device that listens to network communications.

A lot of steganographic techniques exist [3], but the most important goal of actual research work in steganography is to hide pictures in an other picture. These techniques have given birth to watermarking [4], which consists of watermarking a picture to add data. For example, watermarking can be used to add the name of a patient or private information to a medical picture (scanner, radiography, MRI).

Several steganographic techniques aim to use specificities of communication protocols to hide data and use communication layer fields as the cover object. This use of steganographic data in communication layer fields provides the creation of a hidden channel in the network. Only devices that know in which fields the data is hidden can read data or write data. They can invisibly exchange data in the network if the network does not know the steganographic technique.

[5], [6] and [7] show different possibilities for hiding data by using specificities of protocol to create a hidden channel (steganographic channel). The most used techniques consist of using the reserved field of the protocol. Thus, [5] uses the reserved field in the TCP packet header of the TCP/IP protocol, as we can see in Figure 1, and gives the possibility to hide six bits per exchanged packet in this example.

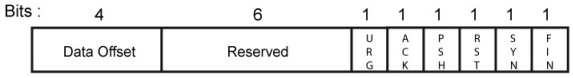

Fig. 1. Reserved bytes in TCP Packet Header

This technique can also be used to create a hidden channel in a wireless local area network as explained in [8]. This example is closer to what we can do in wireless sensor networks if we try to apply this method in the 802.15.4 protocol.

In wireless sensor networks, the use of steganography has been first mentioned in [9], with the conclusion that it would be difficult to apply it in wireless sensor network, because steganography is more applied with picture or video. However [10] and [11] show possibilities using noise in the physical layer of the 802.15.4 protocol to hide data and create a steganographic channel. If these examples are known possibilities for using the 802.15.4 protocol to hide data, and show that steganography is a new way of research in wireless sensor network, to the best of our knowledge [12], we do not know of an example of steganography using communication of MAC layer fields in the 802.15.4 protocol.

III. Hiding data in PHY IEEE 802.15.4

In this section, we show the possibility of hiding data in the PHY layer of the 802.15.4 protocol.

The general structure of a PHY frame can be seen in Figure 2. This structure can be found in [13].

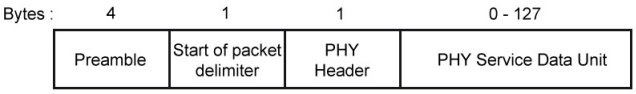

Fig. 2. PHY frame structure

The PHY Header field provides the length of the PHY Service Data Unit field. This field is encoded on one byte, but only seven bits on this byte are used - the eighth is reserved. Because this eighth bit is reserved and never used, it is possible to use it to hide data. A stego message should be sent one bit by packet and the receiver should read every bit of all sent packets to recover the secret message.

If this possibility requires a large number of packets to be sent, we can combine it with other hidden bits in the MAC layer to decrease the number of packets required to exchange a stego message.

IV. Hiding data in MAC IEEE 802.15.4

In this section, we show the possibility of hiding data in the MAC layer of the 802.15.4 protocol.

Frames in the MAC layer of the 802.15.4 protocol are different and depend on the kind of packet sent. The MAC layer uses 4 different kinds of frames:

1) - *Data frame*
2) - *Beacon frame*
3) - *Acknowledgment frame*
4) - *MAC command frame*

We will discuss ways to hide data in these different kinds of frames.

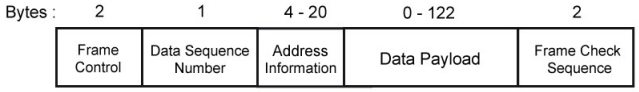

Fig. 3. MAC data frame structure

A. Data frame

The general structure of a MAC data frame can be seen in Figure 3. This structure can be found in [13].

In this frame, the Frame Control field, Data Sequence Number field, and Address Information field provide possibilities to hide information.

1) Frame control field: The Frame Control field is represented by Figure 4.

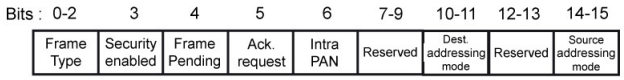

Fig. 4. Frame control field structure

We can see that the 7-9th bits and the 12-13th bits are reserved and can be used to hide a stego object. Here, we can encode three and two bits, respectively, in these fields.

2) Sequence Number field: The Sequence Number field contains the numbering of each packet on 8 bits, used in particular with packet acknowledgements to specify which packet has been acknowledged. The value of this number corresponds to the PIB macDSN variable. This variable is initialized randomly, then incremented after each received packet.
If we choose this initialized number of the PIB variable, we can hide a stego object (or a part of the stego object) inside. We can hide up to one byte of data in this field.

3) Address Info field: The Address Info field is represented in Figure 5. Its size varies between four and 20 bytes.

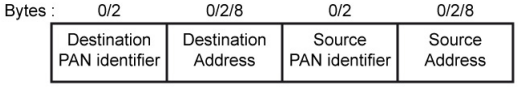

Fig. 5. Address Info field structure

The Source Address field is interesting, because we can choose to have a short (16 bits) or an extended source address (64 bits). It is possible to hide data in this field, for example, if we specify a nonexistent source address. With this nonexistent address, we can hide a stego object with a size up to 64 bits. This steganographic technique can be particularly undetectable if the network does not know the exact number of nodes present in the network, especially in a big network where nodes can be added over time.

B. Beacon frame

The general structure of a MAC Beacon frame can be seen in Figure 6.

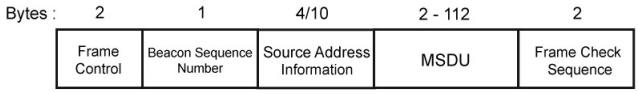

Fig. 6. Beacon frame structure

We find the same possibilities for hiding information as in the Data Frame, in the Frame Control and in the Source Address Information field. However, in the Beacon Frame, the source address information is limited to 10 bytes; yet the Beacon Sequence Number field give us another way to use the cover object.
The Beacon Sequence Number field contains the sequence number of the Beacon node. This number is given by the macBSN variable. This variable is ordinarily initialized randomly. As in the Sequence Number field of the MAC data frame, we can voluntarily choose the value of this number and then hide up to one byte of data.

C. Acknowledgement frame

The general structure of an Acknowledgement frame can be seen in figure 7.

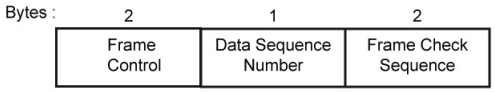

Fig. 7. Acknowledgement frame structure

We find the same possibilities for hiding data in the Frame Control field and Data Sequence Number field. Both are identical to fields of the MAC data frame.

D. Command frame

The general structure of a command frame can be seen in figure 8.

Here, we can see that the Frame Control, Data Sequence Number and Address Information fields provide the same possibilities of hiding data in the command frame as in the MAC data frame.

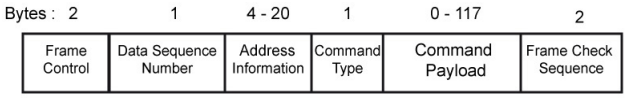

Fig. 8. Command frame structure

V. Analysis of the threat

In this section, we present what kind of attack can be made by hiding data in the 802.15.4 protocol and what we can do to detect and counter these attacks.

A. Threats

In the previous section, we presented a list of possibilities for hiding data in different fields of the communication frame of the 802.15.4 protocol. Obviously, there are other possibilities for hiding data in the 802.15.4, but we have chosen to present the most significant parts. These different possibilities show how it is simple for an attacker to hide an important number of data in a communication in a wireless sensor network.
If we take the example of a sent MAC data frame, an attacker could hide in the different fields that we have seen previously :

1) *3 + 2 = 5 bits for the frame control field*
2) *8 bits for the data sequence number field*
3) *64 bits for the address info field*

...making a total of 77 hidden bits. This number of bits is enough to exchange one or more stego messages.
The attacker can very easily create an undetectable hidden channel in a wireless sensor network, if there is not a mechanism to detect it. With this hidden channel, the attacker can execute new attacks in the network.
For example, we can imagine a threat model where an attacker uses a hidden channel to prepare a denial-of-service attack. This preparation can be found in the representation of Figure 9.

In this representation, the A, B, C and D black nodes are malicious or compromise nodes controlled by the attacker. White nodes are normal nodes of a wireless sensor network. The A node is an interface between the attacker device and other malicious nodes. With the steganographic channel made by using specific fields of the 802.15.4 protocol, the A, B, C and D nodes can communicate without alerting the other nodes of the network (if there is not a policy of steganographic channel detection), even if the network uses a trust reputation policy and uses a watchdog mechanism [14]. In this attack scenario, the attacker

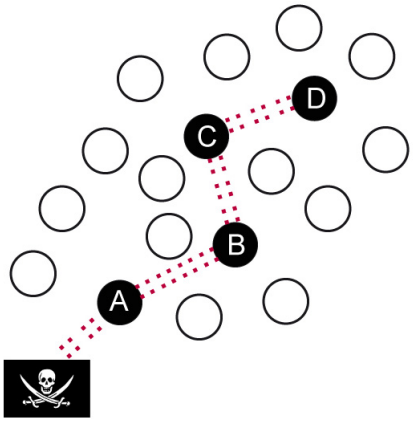

Fig. 9. Representation of a hidden/steganographic channel in a wireless sensor network

will send an hour of onset to A to know when a denial-of-service attack should begin. After that, A will send a stego message containing the hour, minutes and seconds through the hidden channel to synchronize the attack.
This attack hour can be easily contained in 13 bits of the Frame Control field and the Data Sequence Number field of a MAC data frame. Then, A will invisibly send this stego message to B, which will send it to C, and then D. All nodes will be synchronized and could launch an attack at the time wished by the attacker.
This example is just one possibility of using steganography in the 802.15.4 protocol. The steganographic channel can also be used for monitoring the network and informing an attacker of what the wireless sensor network detects or senses.
Nevertheless, we present an obvious way to hide data in the communication fields of the 802.15.4. We can imagine that an attacker can complicate the use of steganography by combining different fields, dividing a stego object into many packets, encrypting this data, using just one bit of a field to launch an attack, exchanging Morse communication or choosing a significant size of the data payload. We cannot make an exhaustive list of possibilities to create a steganographic channel, because steganographic possibilities are only limited by the attacker's imagination.

B. Limits

Steganographic channel can not be detected without a specific detection policy. But if this policy exists and the network monitores some fields of PHY and MAC layers, the steganographic channel could be easily detected. Then an attacker have to find other

possibilities in the PHY or MAC layers to hide the data, but with a number of possibilities that decreases, the size of data exchanged increases the number of packet exchanged.

The Figure 10 shows the number of packets needed for

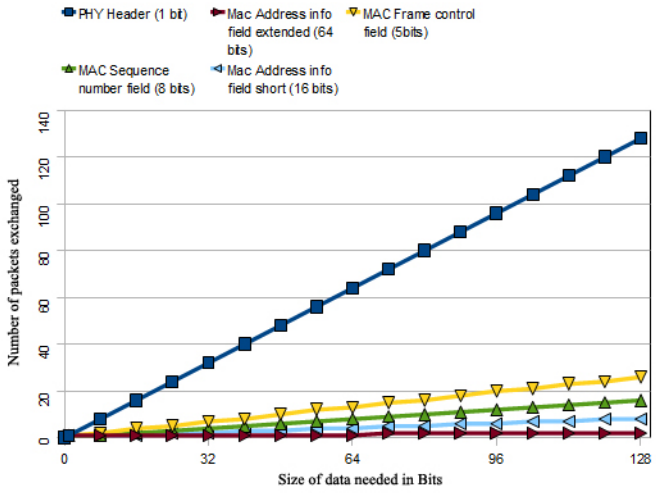

Fig. 10. Number of Data frame packets exchanged for a data size needed with use of different fields of PHY and MAC layers of the 802.15.4 Protocol

sending a size of data with the different possibilities that we have discussed. We can obviously see that without a detection policy, an attacker can exchange a size of data without increase considerably the number of packet exchanged. However with a detection policy, if an attacker has fewer possibilities of bits for hiding data, the number of exchanged packets will increase and the network could monitore an abnormal activity and presumes the existence of a steganographic channel. Another problem for an attacker can be that, with a large number of packets exchanged, the lifetime of malicious nodes will decrease.

VI. Prevent steganographic attacks

As we saw before, there are many possibilities for creating a steganographic channel for an attacker. Thus, we cannot find a single solution to prevent the use of a hidden channel, but as explained before, we can limit the possibilities of cover objects and increase then the number of packets exchanged by an attacker. The activity generated by the steganographic channel will avoid to detect it.

To prevent possibilities of steganographic attacks, we propose a set of rules for detection policy in wireless sensor networks which use the 802.15.4 protocol:

- Set the reserved bits : set to 0 the 8th reserved bit of the PHY header of the PHY layer, the 7th, 8th, 9th, 12th and 13th reserved bits of the frame control field of the MAC layer.
- Set the DSN and BSN fields : the DSN and the BSN fields of MAC layer have to be set to a departure value and no more a random value.
- Set size of the data payload field : the size of data payload of the MAC layer have to be set if it is able. If it is not, we have to choose a limit number of possible sizes of the field.
- Limit the number of sensor address : the source address field have to be short (16 bits), if the number of nodes of the network is small. If the number of sensor cannot be known when the network is created, the routing protocol have to provide the number of nodes of the network. We can then know if the source info address field of the Mac layer contains an address which are bigger than the number of nodes.

This set of rules to become efficient has to be coupled with use of watchdog mechanisms. Each communication between two sensors will be overheard by a third sensor, which monitore data exchanged and if PHY and MAC layer respect the set of rules or not. However the use of watchdog has an energy cost for a wireless sensor network, because each communication needs 3 sensors (a sender, a receiver, a watchdog), and it is known [15] that overhearing or sending data energy costs are nearly the same, the energy consumption for sending data will be multiplied by 1.5 times. To reduce this coefficient we still have to find others solutions where watchdog overheard not all communications but this is another problematic of research.

Our set of rules does not prevent against all possibilities of steganographic channel creation, but it limits the possibilities for hiding data and we assume that with our policy detection, the number of packets exchanged for created a steganographic channel with PHY and MAC layer of 802.15.4 protocol will increase. This augmentation of data exchanged can be monitore by the watchdog and it can presume the existence of a steganographic channel if an average number of packets exchanged can be previously set or with the use of steganalysis detection [3].

Finally if we respect the set of rules and the use of watchdogs, an attacker can always find another ways to create steganographic attacks but he would have some difficulty to find new cover objects without increase the number of packets exchanged.

VII. Conclusion

In this paper, we presented a new threat with the use of steganography in the 802.15.4 protocol, and particularly if an attacker uses steganographic methods to hide data or create a hidden channel. We show that hidden data possibilities and the creation of new kind of attacks are numerous. We proposed a set of rules and the use of watchdog to limit possibilities of steganographic attacks. However, steganography is a new research path in wireless sensor networks and we mean that some other possibilities of cover objects for steganographic attacks can be found. In our future works, we want to search for other solutions to detect hidden data using steganalysis and also find energy-efficient solutions based on steganography in order to reinforce wireless sensor network security.

References

[1] Alliance Z. In http://www.zigbee.org.

[2] Anderson R, Petitcolas F. On the limits of steganography. *IEEE Journal of Selected Areas in Communications* 1998; **16**:474–481.

[3] Katzenbeisser S, Petitcolas FA ((eds.)). *Information Hiding Techniques for Steganography and Digital Watermarking*. Artech House, Inc.: Norwood, MA, USA, 2000.

[4] Cox I, Miller ML, Bloom JA. *Digital watermarking*. Morgan Kaufmann Publishers Inc.: San Francisco, CA, USA, 2002.

[5] Handel TG, Sandford MT II. Hiding data in the osi network model. *Proceedings of the First International Workshop on Information Hiding*, Springer-Verlag: London, UK, 1996; 23–38.

[6] Trabelsi Z, El Sayed H, Frikha L, Rabie T. A novel covert channel based on the ip header record route option. *Int. J. Adv. Media Commun.* 2007; **1**(4):328–350, doi:http://dx.doi.org/10.1504/IJAMC.2007.014811.

[7] Murdoch SJ, Lewis S. Embedding covert channels into tcp/ip. *Information Hiding: 7th International Workshop, volume 3727 of LNCS*, 2005; 247–261. URL http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.66.1389.

[8] Szczypiorski K. A performance analysis of hiccups - a steganographic system for wlan. *CoRR* 2009; **abs/0906.4217**.

[9] Pathan ASK, Lee HW, Hong CS. Security in wireless sensor networks: Issues and challenges. *CoRR* 2007; **abs/0712.4169**.

[10] Mehta AM LS, K P. Steganography in 802.15.4 wireless communication. *Advanced Networks and Telecommunication Systems, 2008. ANTS '08. 2nd International Symposium on*, Mumbai, 2008; 1–3.

[11] Kho T. Steganography in the 802.15.4 physical layer. *Technical Report* 2007.

[12] Zhou Y, Fang Y, Zhang Y. Securing wireless sensor networks: A survey. *IEEE Communications Surveys and Tutorials* 2008; **10**(1-4):6–28.

[13] Ieee 802.15.4. 2003. part 15.4: Wireless medium access control and physical layer specifications for low rate wireless personal area networks. *Technical Report*, ANSI/IEEE Standard 802.15.4 Sept.

[14] 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.

[15] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Computer Networks* 2002; **38**:393–422.