# Message Denial and Alteration on IEEE 802.15.4 Low-Power Radio Networks

Colin P. O'Flynn
NewAE, Canada. coflynn@newae.com

***Abstract*— The severely constrained resources present in many IEEE 802.15.4 wireless nodes limits the available security protocols which these nodes can run. Selecting protection for the resource-constrained devices requires understanding the attacks which can be performed.**

**This paper presents several simple attacks which allow a reader of any background to understand the vulnerability of IEEE 802.15.4 networks. Denial of Service (DoS), Passive Listening, and Man In The Middle (MITM) attacks are demonstrated running from a simple and low-cost platform. Considerations for real-life deployments of the attacks covers issues such as defeating channel hopping or attacking at a distance. The ease of performing the attacks demonstrates why security is critical on all networks.**

**Protection against the attacks through both academic and industry-developed standards is briefly discussed.**

***Keywords*-constrained devices, denial of service, low-power networks, security, man in the middle**

## I. Introduction

THE IEEE 802.15.4 wireless standard is aimed at low-power and low-cost devices. The expected proliferation of such devices would see 'smart objects' throughout our entire world, powered by wireless standards such as IEEE 802.15.4 [1]. Various commercial entities are planning on or already using the IEEE 802.15.4 standard as a base for their networks. ZigBee for example has specifications targeted towards markets as diverse as home automation, consumer electronics, medical, smart energy, and industrial [2].

These low-power networks often have complicated security requirements. A single network may have nodes ranging from light switches to meters responsible for billing and payments [3]. It is important to understand the types of attacks present on these networks to evaluate whether the selected security method is sufficient.

Considerations for security aspects of the IEEE 802.15.4 standard are presented in [4], and general attacks which may be used in low-power networks are presented in [5]. Work in [6] concentrated on jamming and defences; this paper demonstrates how clever use of jamming can be part of more sophisticated attacks.

This paper will provide a brief overview of the IEEE 802.15.4 standard before moving into the hardware used for demonstration, including results of attacking working networks. Some extensions of the demonstrated attacks will show how sophisticated attacks could occur in a network, and finally some notes on defences against these attacks.

## II. Background on IEEE 802.15.4

IEEE 802.15.4 is designed to provide low data rate, low-power networking. Typical ranges could be between 10 to 200 metres, although certain modes can provide ranges in excess of a kilometre. IEEE 802.15.4 can be run on a variety of frequency bands and with various modulations and data rates. The most common is running on the 2.4 GHz band, with 250 kilobit/second data rate.

Fig. 1 shows what a data frame on this system would look like; the Physical (PHY) payload is limited to 127 bytes and includes two check bytes. There is a choice of 16 channels on the 2.4 GHz band, numbered 11 through to 26 [1].

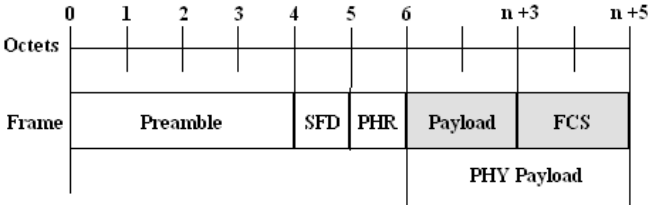


Fig. 1. A typical IEEE 802.15.4 frame, as would occur on a 2.4 GHz network. Using the standard data rate each octet would be 32 µS long. The SFD is the Start of Frame Delimiter, which breaks the preamble. The PHY Header (PHR) consists of a single byte with the length of the frame. The Frame Check Sequence (FCS) is a 16-bit CRC.

## III. Attack Hardware

A wide variety of vendors provide IEEE 802.15.4 transceiver chips. The hardware in this paper used an Atmel AT86RF231 RF transceiver combined with an Atmel microcontroller on each node [7]. Two such nodes were wired together as in Fig. 2, which allows one node to always function in a monitor mode while the other is transmitting.

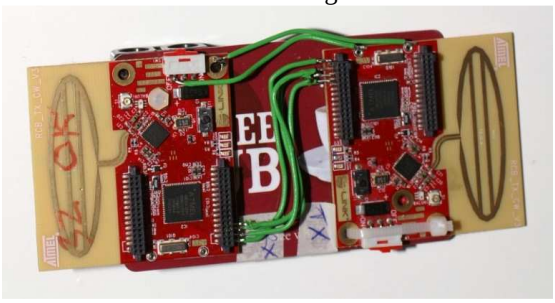

Fig. 2. The physical jamming hardware used has two radios present. One radio is always in the receive state, and the other always ready to transmit. This dual-radio configuration is faster at transmitting a colliding signal than using a single radio and switching between receive and transmit states.

## IV. Denial of Service attacks

There are three basic types of denial of service (DoS) attacks demonstrated. The first is a wide-band jamming of all channels in the RF environment. A more selective jamming method results in just IEEE 802.15.4 traffic being jammed. After that a demonstration of how an individual message could be disrupted, which may be part of a more complex attack, or just performing a DoS against a specific node.

### *A. Wide-Band Denial and Pulse Denial*

The easiest method of jamming traffic is to simply block the entire RF spectrum. This results in a total loss of the affected spectrum to all users. A generic RF generator could be used for this, but an even cheaper option is to use the 802.15.4 transceiver chips. In [6] this is described as 'pulse jamming', since the jammer sends pulses of transmit power. A more thorough treatment of pulse jamming is presented in [8]. A test of over 1500 packets sent while single-channel pulse jamming was present showed it to be 100% effective while the jamming node was located close to the receiving node. As discussed in section V.A an attacker could achieve similar results at a further distance.

This is extended to wide-band pulse jamming by channel-hopping to every 802.15.4 channel and transmitting a quick burst of data before going to the next channel, as demonstrated in Fig. 3. The pulse jamming demonstrated here had a very short pulse length of only 24 µS, which is shorter than the time it takes to transmit a single byte. This was accomplished by issuing the start transmission command, followed by immediately an abort command. It can be seen that it takes 1600 µS to complete a single sweep of all 16 channels. In 1600 µS the network could transfer 50 octets; thus any message longer than 50 octets will be corrupted. Using multiple radio devices could form a denser jamming network, as each radio would only hop between a smaller number of channels.

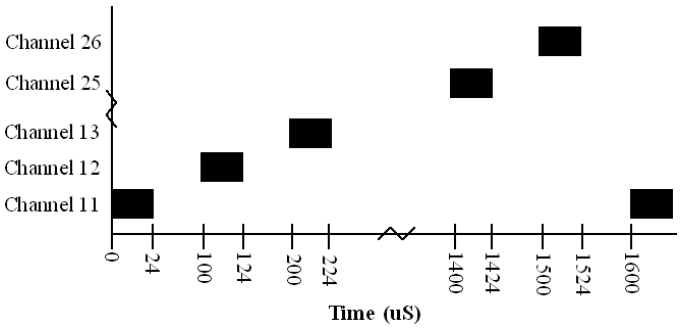


Fig. 3. Jamming all channels by channel-hopping. Measurements showed transmit lasted for 24 µS on each channel, and the radio takes 76 µS to change channels.

A more interesting use of the wide-band approach is actually shaping a network to run on a desired channel. The IEEE 802.15.4 standard provides a method of doing an energy detect (ED) scan, which is designed to allow a node to select a channel to operate on which is free from interference. Using the approach in Fig. 3 one can simply jump over a certain channel to leave it free. Fig. 4 demonstrates how this would appear to another node in the area. A comparison of the true background noise (black bars) is shown compared to the artificially created background noise by selective jamming (grey bars).

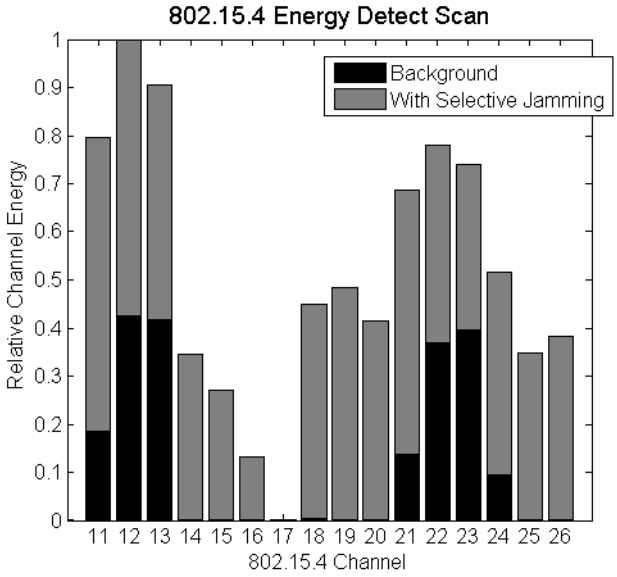


Fig. 4. Comparisons of energy detect scan results on IEEE 802.15.4 channels. The black bars show the result of background noise, mainly due to 802.11 networks which share the frequency band. The grey bars show the additional noise added by the attacking hardware to force the target to prefer channel 17.

The disadvantage of wide-band jamming is that it is very easy to detect. It is illegal to operate a radio transmitter with intent to jam airwaves in all countries, and tracking down a continuously operating transmitter is relatively easy. This provides excellent deterrents against using such measures.

### *B. IEEE 802.15.4 Specific Interruption Denial*

An extension of the previous example would be to transmit interfering messages only when IEEE 802.15.4 messages are detected. This would minimise interference to other users, such as WiFi traffic on the 2.4 GHz band. As well, since the interfering energy is only present when other IEEE 802.15.4 traffic is present, the interfering transmitter would be masked by the legitimate users. Detection of the interfering transmitter would be difficult as it is never spontaneously present. This jamming mode is described as an interrupt mode in [6].

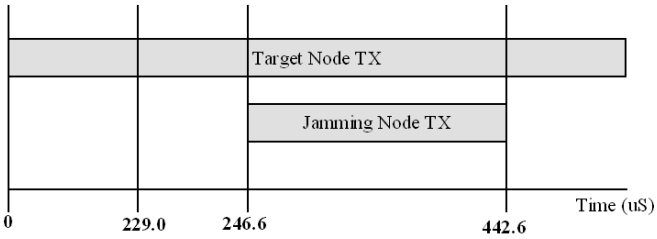


Fig. 5. Measurements taken from physical jamming hardware showing how quickly it can respond. The target node's transmission is detected at 229 µS, and it takes 17.6 µS after that before the jamming node's RF output is active. The jamming node transmits for 196 µS, disrupting at least six octets.

The hardware used is again as in Fig. 2. When 802.15.4 traffic is detected, the monitoring node tells the transmitting node to send a burst of data. Fig. 5 shows the timing between these two events. The time between the target node's transmit power being present and the jamming node beginning to transmit is about 250 µS, which corresponds to about eight octets. This should result in the 2nd or 3rd byte of the PHY payload being corrupted. Note that the jamming energy does not extend beyond the target node transmission in this case, again complicating attempts to detect the jamming device.

The results are shown in Table 1. It successfully jams each of the 802.15.4 messages by disrupting the third and higher byte.

TABLE I. IEEE 802.15.4 BEACON REQUEST JAMMING

| Frame (Hexadecimal) | FCS OK | Jamming Enabled |
|---|---|---|
| 03 08 94 ff ff ff ff 07 86 7e | Yes | No |
| 03 08 a4 ff ff ff ff 07 56 b9 | Yes | No |
| 03 08 b4 ff ff ff ff 07 e6 fb | Yes | No |
| 03 08 **da ff fb 89 fb 09** 44 fe | No | Yes |
| 03 08 **89 fa fa df f9 ca** 45 3b | No | Yes |
| 03 08 **5f ef ff df 50 09** f5 79 | No | Yes |

The last two bytes in the frame are the FCS. The third byte is the sequence number, and in the first three messages is seen as incrementing in each message (94, A4, B4, etc). The four bytes in the middle in each frame should be ff ff ff ff as in the first three messages, but are jammed in the last three messages. Incorrect bytes are shown in **bold underline**.

### C. Node-Specific and Message-Specific Denial

The previous example would attempt to jam a message as soon as possible. For pure disruption this would be effective, but more interesting and useful applications wish to deny specific messages. This is accomplished by reading the first several bytes of the 802.15.4 Medium Access Control (MAC) header, which includes information such as the frame type and addressing information. It is possible to receive these bytes in the attacking node, and decide on the action to take, such as only jamming data being sent to a certain address.

A further extension of this is the ability to receive data in the attacking node while denying that data to a target node. Consider again the frame from Fig. 1; it is only necessary to corrupt the FCS for a node to discard the data packet. Since the length of the message is transmitted in the PHR, an attacking node can predict exactly when the FCS will be transmitted over the air. At this exact time another node can transmit to jam the FCS.

The results of such an experiment are shown in Fig. 6 and Fig. 7. Note in Fig. 7 how the actual data is valid, and only the FCS has been corrupted. The attacking node could even corrupt only one byte of the FCS if it wanted to at least confirm that part of the FCS matches to prevent a node from purposely transmitting incorrect data as a countermeasure.

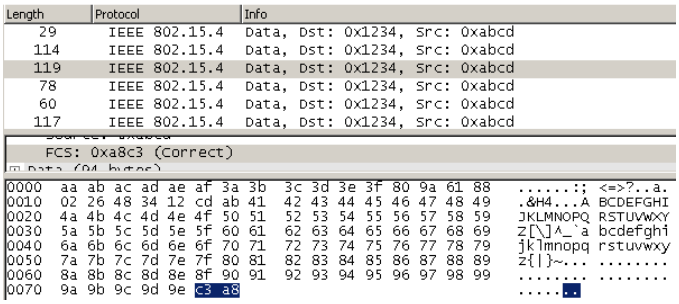


Fig. 6. A selection of various message sizes transmitted without interference. Note in the sniffer capture the FCS line is marked as 'correct'.

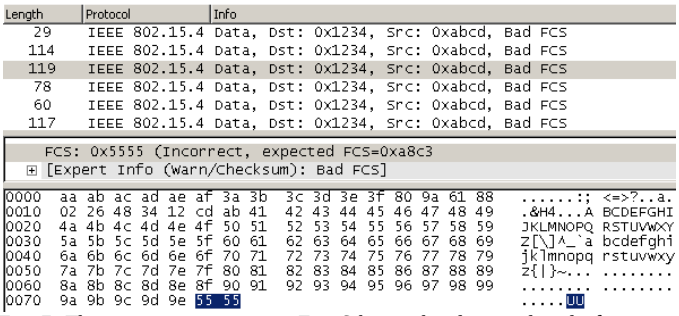


Fig. 7. The same messages as in Fig. 6 but with selective denial of service. Note just the FCS (highlighted) is corrupted. The 'Bad FCS' message is displayed in the sniffer for each of the packets.

## V. ADDITIONAL CONSIDERATIONS

### A. Imbalance of Resources

The example development boards used for both the victim and attacker node here are the same device. In real deployments this is not likely to be the case; the attacker may have significant advantages over the target nodes. This could be in terms of antenna strength, power output, or receive sensitivity.

The 2.4 GHz band which many IEEE 802.15.4 devices run in also covers the same band used by WiFi. As such any devices such as power amplifiers or high-gain antennas that can be easily purchased or made for WiFi networks are usable on IEEE 802.15.4 networks.

The attacker may also feel free to ignore governmental requirements on transmit power. This would be extremely useful when jamming a node which is physically more distant, since the attacker's power will be too weak at reception. A study from [9] shows that to achieve reliable jamming requires the interferer's power to be up to 6 dB greater than the desired signal, but some level of jamming can be achieved with the interference signal at a level of -3 dB compared to the desired signal. Table 2 provides some examples of loss in dB for different distances at 2.4 GHz based on the free-space formula [10]. The typical 802.15.4 transmit power from a small node is around 3 dBm [7], whereas commercially available 2.4 GHz amplifiers are typically in the 20–44 dBm output range [11]. The effective output power could be increased through a directional antenna, which could expect about a 10 dB gain.

Consider the example of Fig. 8 where an attacker is separated by 25 m to each node, and the two nodes are separated by 10 m. The received power from each node will be around -37 dBm at 10 m, assuming 3 dBm transmit power and

an antenna with no gain. To achieve jamming at a 25 m range would require at least 37 dBm transmit power from the attacker, which would provide the required 6 dB advantage at reception over the desired signal. This level of transmit power is achievable with available amplifiers and antenna configuration [11], making the 'attack at distance' scenario possible.

TABLE 2
DISTANCE VS. POWER LOSS AT 2.4 GHZ

| Distance (M) | Loss (dB) |
|---|---|
| 10 | 40 |
| 25 | 68 |
| 50 | 74 |
| 100 | 80 |

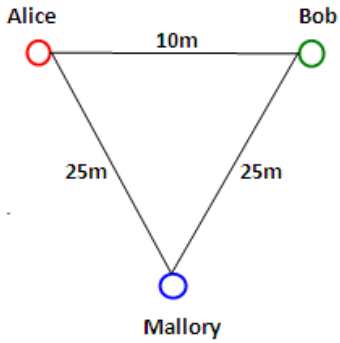


Fig. 8. An example of a network under attack, where the two nodes are separated by 10 m and an attacking node is 25 m away.

### B. *IEEE 802.15.4 Security*

The IEEE 802.15.4 standard provides the ability to add several security models. This can take the form of authentication through adding a Message Integrity Code (MIC), or encrypting the data payload itself.

The encryption covers only the MAC payload, and not the MAC headers. As mentioned the DoS attacks can be tailored to specific nodes by reading the MAC headers and only blocking those messages. Since the MAC headers are not encrypted using IEEE 802.15.4 security provides no protection against this.

IEEE 802.15.4 acknowledgements are never secured, and thus cannot be relied on to guarantee a node actually received a message [4].

## VI. ATTACK SCENARIOS

Sections IV and V are combined here to provide some example attacks beyond simple DoS attacks. An interception attack and bootstrapping attack will be covered.

### A. *Interception Attacks*

An IEEE 802.15.4 exchange could consist of Alice sending a message to Bob, and waiting for the IEEE 802.15.4 Acknowledge (ACK). After receiving the ACK Alice assumes Bob received her message, and then Alice waits for Bob's response.

Using the methods outlined in section IV.C an attacker, Mallory, could interrupt the transmission of the message from Alice to Bob. She could then spoof an ACK to appear as if Bob did receive the message correctly. The end result is that Mallory has received the message intended for Bob; Alice *thinks* Bob received the message, and Bob has received no message.

If Mallory was to then send a modified message it would begin to establish a Man In The Middle (MITM) attack [12]. This is shown in Fig. 9 with both an attacker absent and present.

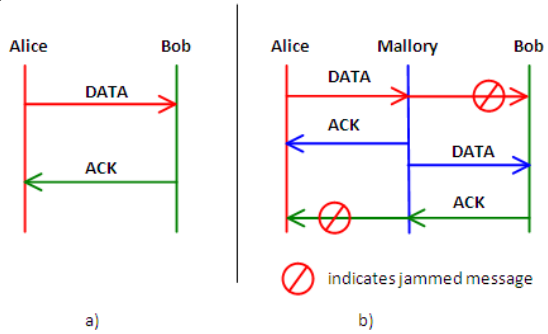


Fig. 9. a) Indicates the correct sequence of messages being exchanged without an attacker present. b) Indicates the message sequence with an attacker in the middle. To both Alice & Bob the sequence looks the same as extra messages have been jammed.

### B. *Bootstrapping Attacks*

During initial network setup (bootstrapping) some method of configuring two nodes to securely join up is required. On very resource-constrained nodes this could simply be two push-buttons on each node, which when pressed puts the nodes in a special join mode. This system relies on an attacker not being present during this initial configuration, which may be 'secure enough' for simple applications such as remote controls. The ZigBee RF4CE standard uses such a system for device bootstrapping [13].

The DoS attacks presented in section IV could be used to force a particular device off the network. Eventually the user would need to perform the bootstrapping again, except the attacker is now present during this operation, and can either simply listen in to the join process or perform a MITM as detailed above. To the user the device now appears to be working, while in reality they have assisted an attacker in intercepting important bootstrapping traffic.

For this reason it is important to consider that while an attacker may not be present initially, they could create the required conditions to force bootstrapping to occur at a time when the attacker is present. Further information about bootstrapping is presented in [14].

## VII. DEFENCES AND NETWORK DESIGN

This project's primary aim was to demonstrate how easily a number of attacks can be performed on these networks and to demonstrate the minimum requirements for a secure network. These are not 'new' attacks, but attacks which can be performed with much greater ease than previously thought. A few examples of counter-measures for the attacks are presented, but these are far from exhaustive and simply

demonstrate what additional sort of effort is required to avoid the attacks.

In [6] a coverage of DoS attacks is given, and also the DEEJAM protocol is presented which combines several defences against the DoS attacks. It demonstrates how the PHY-level Start of Frame Delimiter (SFD) can be changed or made into a pseudo-random sequence so the attacking node cannot synchronise to the radio sequence. In addition channel-hopping at the PHY level is shown to make it difficult for the attacker to follow or jam the message. However, typical commercial installations require the use of approved standards, thus upcoming networks are very likely to use IEEE 802.15.4-2006, and not 'unofficial' protocols such as DEEJAM. This means higher layers must be aware of the limitations of the lower layers, such as not trusting the IEEE 802.15.4 acknowledgments [4].

For networks which require higher security, the upcoming IEEE 802.15.4e amendment could be useful. It adds secured acknowledgements and channel-hopping as an IEEE standard [15]. This could be combined with higher-layer cryptographic protocols when a secure network is required.

As mentioned in section V.A, an attacker may also have considerable resources available. For example if channel-hopping is implemented, an attacker could operate attacking nodes on every available channel.

Preventing the MITM and interception attacks requires adding authenticity to the network. For ad hoc networks this might be impossible, since the nodes have not had any previous contact. In such situations another solution is to provide an out of band channel which an attacker does not have access to and is physically protected from MITM attacks. The wireless nodes could be required to physically touch together for bootstrapping to exchange keys or signatures [14].

## VIII. Conclusion

Performing Denial of Service attacks on IEEE 802.15.4 networks can be accomplished easily with minimum hardware. These attacks could be dumb and block access to certain areas, or sophisticated and block certain messages as part of a larger attack; e.g. Man In The Middle. The wide availability of IEEE 802.15.4 development kits and hardware means performing these attacks is trivial. Designing a network with inadequate or missing security is unacceptable, as it leaves nodes open to misuse.

Section V.A highlights how attacks could be performed at a distance, however further research is necessary to measure the effects of variances in resources between the attacking and target node in different environments.

The simple attacks presented in this paper demonstrate it is possible to block or alter messages over the wireless environment. Further research in this field can use these building blocks for more complex attacks; for example targeting the specific security suites used in IEEE 802.15.4 or other standards.

## Appendix

This paper makes several references to IEEE 802.15.4. Unless otherwise specified this paper always references 802.15.4-2006, the latest revision of the main specification. Changes between the 2003 and 2006 revisions would not affect this paper, but some of the referenced papers may use names of e.g. security suites in the 2003 version which have changed slightly in the 2006 version.

## References


[1] Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). IEEE Std 802.15.4-2006. IEEE. ISBN 0-7381-4997-7. Available: http://standards.ieee.org/getieee802

[2] ZigBee-2007 r17 Specification. ZigBee Alliance Inc. 2007. Available: http://www.zigbee.org/Products/DownloadZigBeeTechnicalDocuments.aspx

[3] Romer, K.; Mattern, F., "The design space of wireless sensor networks," *Wireless Communications, IEEE*, vol.11, no.6, pp. 54–61, Dec. 2004.

[4] Wagner, D; Sastry, N., "Security considerations for IEEE 802.15.4 networks," *In WiSE '04: Proceedings of the 2004 ACM Workshop on Wireless Security*. pp.32-42. 2004.

[5] Redwan, H.; Ki-Hyung Kim., "Survey of security requirements, attacks and network integration in wireless mesh networks," *New Technologies, Mobility and Security, 2008. NTMS '08.*, pp.1–5, 5–7 Nov. 2008 doi:10.1109/NTMS.2008.ECP.94

[6] Wood, A.D.; Stankovic, J.A.; Gang Zhou, "DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp.60–69, 18-21 June 2007 doi: 10.1109/SAHCN.2007.4292818

[7] AT86RF231 Datasheet. Atmel Corporation. September 2009.

[8] Iskander, C.-D., "Performance analysis of IEEE 802.15.4 noncoherent receivers at 2.4 GHz under pulse jamming," *Radio and Wireless Symposium, 2006 IEEE* , pp. 327–330, 17–19 Jan. 2006 doi: 10.1109/RWS.2006.1615161

[9] Subbu, K.P.; Howitt, I., "Empirical study of IEEE 802.15.4 mutual interference issues," *SoutheastCon, 2007. Proceedings. IEEE*, pp.191–195, 22–25 March 2007 doi: 10.1109/SECON.2007.342883

[10] Thompson, R.; Tipper, D.; Krishnamurthy, A.; Kabara, J., *The Physical Layer of Communication Systems*. Artech House, 2006. pp. 652–653

[11] L-Com. "Wireless LAN Amplifiers 2.4 GHz Amplifiers". 2010. Available: http://www.l-com.com/familylist.aspx?id=2040

[12] Schneier, B., *Applied Cryptography 2nd ed.*, Wiley, 1996, pp. 48–49.

[13] ZigBee RF4CE Specification Version 1.00. ZigBee Alliance Inc. 2009. Available: http://zigbee.org/Markets/ZigBeeRF4CE/download.aspx

[14] O'Flynn, C., "Secure Initial Configuration of Resource Constrained Wireless Smart Objects," *SoftCOM 2010 – Workshop Track*. Sept 2010. Available: http://www.newae.com/tiki-download_wiki_attachment.php?attId=71

[15] IEEE Std 802.15.4e-D0.01/r5 (UNAPPROVED DRAFT STANDARD). IEEE. Available: https://mentor.ieee.org/802.15/dcn/09/15-09-0604-06-004e-ieeestd802-15-4e-d0-x.pdf