# *Investigation of Continuous Wave Jamming in an IEEE 802.15.4 Network*

J. Rewienski[1], M. Groth[2] L. Kulas[3], *Senior Member, IEEE* and K. Nyka[4], *Member, IEEE*
Department of Microwave and Antenna Engineering
Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology
Gdansk, Poland
[1] jakub.rewienski@eti.pg.gda.pl, [2] mateusz.groth@eti.pg.gda.pl, [3] lukasz.kulas@eti.pg.gda.pl, [4] nyx@eti.pg.gda.pl

***Abstract*—This paper presents how continuous wave jamming affects IEEE 802.15.4 network. To this end, an office-based measurement setup has been proposed. Within the measurement area, 25 nodes have been set up in order to create a IEEE 802.15.4 tree-based test network structure. A dedicated jamming device that generates and transmits a continuous wave signal has been developed. Several tests have been conducted and presented to demonstrate the network's vulnerability to jamming attacks for different jammer power levels and its positions across the scene.**

***Keywords— IEEE 802.15.4; jamming; Internet of Things; continuous wave; channel access.***

## I. INTRODUCTION

The nature of wireless communication makes wireless networks vulnerable to different types of hostile attacks ranging from intentional jamming to eavesdropping and impersonating the correct transceiver [1]. Since the communication takes place over the open environment, there is no physical barrier between the channel and potential intruder [2][3]. This problem arises also in IEEE 802.15.4 based wireless personal area networks (WPAN) and wireless sensor networks (WSN) since they are becoming popular, bringing the technologies of short range connectivity to everyday use. The rapid development of Internet of Things (IoT) implies the growing necessity of taking the threat of jamming into consideration during the design, development and utilization of the wireless network [4][5].

## II. JAMMING TECHNIQUES

Radio jammer is a device for intentional directing electromagnetic energy onto a communication system to disrupt or prevent signal transmission [6]. There can be distinguished two types of jammers: software, which base on higher levels of ISO-OSI model, and hardware, which radiate certain radio signal of intended frequency. In this paper we focus on the latter [7]. The simplest method of jamming is to continuously transmit a non-modulated signal of a desired frequency. The main disadvantages of such approach is large power consumption and that it can be fairly easily filtered. What is more, this method is ineffective in case of communication with some of the spectrum spreading methods implemented, such as OFDM. Another kind of jamming is a narrow-band noise transmission, which bases on propagation of spectrum similar to Gaussian distribution [8]. There are also methods to sweep the frequency across the whole frequency band of the system to interfere the broader frequency range (swept jamming). Other solution is called Barrage/Partial-band jamming [9] – in this case a series of single tones is transmitted covering a part of the frequency band. It can be realized by transmitting tones on a few frequencies at a time or using a fast broadband transmitter. The broadband noise jamming can also be realized as a transmission of noise in the whole frequency band. Contrary to broadband techniques, tone jamming can also be applied by transmitting narrow-band signals at selected frequencies [10]. One of the most popular approaches is the pulsed-noise jamming, which bases on periodic switching of a broadband high-energy pulse signal – usually Additive Gaussian White Noise [11]. Among more complex kinds of jamming we can distinguish Deception Jamming, which bases on sending fake messages and Reactive Jamming, where specific packets are being attacked [12] – in this case a precise synchronization is necessary to achieve proper jamming results.

For the measurements reported in this paper, a narrow-band continuous wave (CW) jammer was selected. The main reason of this choice is that it is easy to implement and fulfills the requirement of being able to block the communication in the network under investigation.

## III. TEST SYSTEM ARCHITECTURE

### A. IEEE 802.15.4-based JenNet-IP Network

For the measurements of jamming effects a network of 25 nodes based on JN5168 microcontrollers with integrated transceivers was deployed. The devices were operating under a JenNet-IP stack, which is a combination of NXP JenNet protocol and Internet Protocol. WPAN nodes communicate with each other via JenNet protocol (based on IEEE 802.15.4 standard) and with LAN/WAN (Local/Wide Area Network, e.g. Internet) via IPv6 protocol. The two protocols are connected by 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) technology [13].

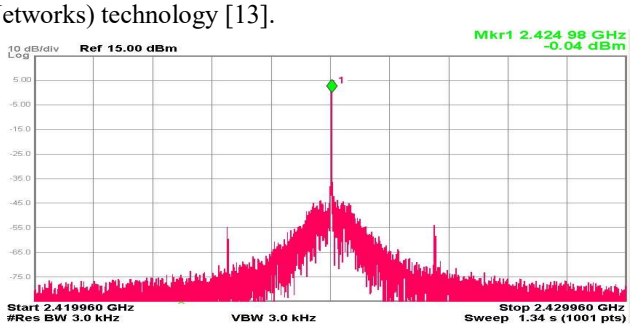


Fig. 1. Measured jammer output signal at power level set to 0 dBm.

*This work was supported by SCOTT (www.scott-project.eu) project that has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.*

The described measurement environment falls into a general framework of the Internet of Things (IoT). The sensor nodes are connected to a WPAN. One of them plays a role of a network coordinator which is the root of the network. This node, when connected to a host machine (computer with Linux OS) via serial interface, functions as a Border-Router, which connects the WPAN to WAN. IEEE 802.15.4 packets are translated into IPv6 packets and routed by 6LoWPAN technology. IEEE 802.15.4 is a standard for Low-Rate Wireless Networks and describes the lowest one and a half of ISO-OSI model layers, which are: Physical Layer (PHY, Layer 1) and Medium Access Control (MAC) layer - a sublayer of Data Link Layer (Layer 2) [14]. The standard offers three frequency bands, of which the 2400-2483.5 MHz band is used in the presented experiments. The CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism is used for channel access. It is a "listen-before-talk" strategy implemented in MAC sublayer, which periodically requests PHY layer to check if channel is "Clear To Transmit". To decide if channel is free for transmission a CCA (Clear Channel Assessment) mechanism is employed. It can operate in one of three modes:

- Energy above threshold mode – If level of energy detected in the sampled medium is above threshold, CCA reports a busy channel.
- Carrier sense mode – If a signal with the modulation and spreading characteristics of IEEE 802.15.4 is detected in the sampled medium, CCA reports a busy channel.
- Carrier sense with energy above threshold mode – If a signal with the modulation and spreading characteristics of IEEE 802.15.4 and level of energy above the threshold are detected in the sampled medium, CCA reports a busy channel.

The network utilized during the measurements presented in this paper was operating on the IEEE 802.15.4 standard channel no. 15, which is centered on 2.425 GHz and has a 5 MHz bandwidth. The CCA mechanism was set to energy above threshold mode. The WPAN was configured in a tree topology, where data can be sent either upstream (to nodes' parent) or downstream (to one of nodes' children). Each node can connect to only one parent at a time. If the connection to parent is unavailable then the node becomes orphaned so the communication also breaks between WAN and this node or any of its children. By searching for a new parent for this orphaned node the network tries to reconfigure in order to recover upstream connection.

Jamming can break connection between a node and its parent. This can make a major part of the network unavailable, therefore disturbing operation of the whole system.

### *B. Jammer*

An additional node, also based on JN5168 microcontroller was used as a jamming device. The nodes' software has been modified to transmit continuous wave signal at one of three power levels: -22 dBm, -11 dBm and 0 dBm. The network operates on center frequency of 2.425 GHz, and the same setting was applied to the jammer. The signal characteristics were measured using a spectrum analyzer and are shown in Fig. 1. The jamming signal was transmitted by a dipole antenna of 1.5 dBi gain.

Fig. 2. Partial view of the scene from the corridors corner. Network nodes are marked with red circles.

The employed CW jamming method affects the channel assessment. CCA mechanism operating in energy above thershold mode probes the channel and when strong jamming signal in the medium is detected it decides that channel is busy. Therefore the network nodes do not even try to communicate because of such the CCA judgement.

## IV. Measurements

The experiments prepared for this paper aim to simulate a real-life scenario. The WPAN network is regularly used as a part of the radio frequency positioning system (developed earlier at the university). An outlook of the scene is shown in Fig. 2 - five nodes being a part of the tested network are marked by red circles. A map of the test scene with real positions of the network nodes is shown in Fig. 3. Nodes are represented as dots, and their connections as lines. Different colors represent depth levels in the topology tree – the warmer color (red, yellow) the closer to the root of the network. Red nodes are connected directly to the root, the orange nodes connect to the root by a node at the red level etc.

During the measurements, the following procedure was performed:

1) Waiting 2 minutes for all nodes to join the network.
2) Jammer was placed.
3) All nodes were reset via JenNet (for network to reform quicker)
4) The Jammer was turned on.
5) The Network topology was checked. 6) The Jammer was turned off.

All results were automatically placed on the map of the scene in form of nodes and connections between them. Nodes that could not connect to the network were marked as grey dots. The results were later analyzed and an approximated jammer influence region (jamming range) was plotted onto the map. The choice of influence region was based on three principals:

1) The region is an ellipse.
2) The region must cover all nodes affected by jamming.
3) The region should cover as few nodes not affected by jamming as possible.

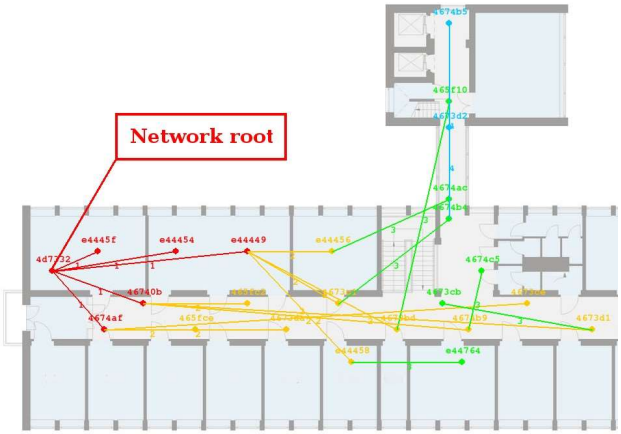


Fig. 3. Network topology without jamming.

The regions defined in this way depict areas in which nodes are likely to be jammed. Such a simplified approximation of the influence regions, which did not involve measurements of actual jammer's signal distribution, was used only in order to roughly visualize detected jamming range. Therefore, the regions may also cover some of the not affected nodes. 25 different locations of jammer were used to observe its influence in function of its position in the environment. Measurements were repeated for three different jammer power levels mentioned before. In total a series of 75 tests was conducted.

The network vulnerability to jamming for various jammer placements can be observed in Fig. 4 to Fig. 7. It can be noticed that the location of jamming device has a decisive influence on how the jamming disturbs network connectivity. In Fig. 4, the jammer is placed in a closed space (i.e. room) so only the nearest nodes are affected by its signal. Therefore, only a single node (placed in the same room as jammer) could not connect to the network. When the jammer was located in more open space area, like the corridor, much more nodes were affected. This effect can be observed in Fig. 5 and Fig. 6, where up to 12 nodes are affected. The difference of behavior is related to the fact, that wireless signal propagates well in free-space and is attenuated when meets obstacles such as room walls. In an open space jamming signal attenuates less and remains above the energy threshold (in CCA mechanism) further from the signal source than in a closed space. This leads to the conclusion that well grained networks in an office area exhibit better resistance to jamming than connections in open spaces.

Similar series of tests were done with higher and lower levels of jamming signal. An example of results of those tests can be seen in Fig. 7. As one can observe, jammer set to higher signal power has a significantly stronger destructive influence on the network communication – only nodes distant from the jammer can connect to the network, while the rest of the nodes have problem joining the network due to channel assessment. On the other hand, when jammer is set to lower power level, only the nearest nodes become disconnected.

As it is not possible to use LQI (Link Quality Indicator) or PER (Packet Error Rate) due to the communication breakage between nodes affected by jamming and rest of the network, we propose a different jamming influence measure – Network Jamming Resistance Ratio (NJRR) which can be described as:

$$NJRR = \frac{N_A - N_J}{N_A} \cdot 100\% \quad (1)$$

where $N_A$ is the number of all nodes in the network, $N_J$ is the number of nodes affected by jamming (nodes that did not manage to connect to network). NJRR equal to 100% would mean that whole network was operable – jamming did not affect any of the nodes. NJRR of 25% would mean that only 25% of nodes were operable – the rest could not join the network.

TABLE I. JAMMING INFLUENCE ON IEEE 802.15.4 NETWORK

| Jamming power | Placement | Mean NJRR | Minimal NJRR | Maximal NJRR |
|---|---|---|---|---|
| 0 dBm | Closed space (room) | 58% | 4% | 92% |
| | Open space (corridor) | 31% | 8% | 76% |
| -11 dBm | Closed space (room) | 93% | 76% | 100% |
| | Open space (corridor) | 47% | 40% | 92% |
| -22 dBm | Closed space (room) | 99% | 96% | 100% |
| | Open space (corridor) | 47% | 40% | 92% |

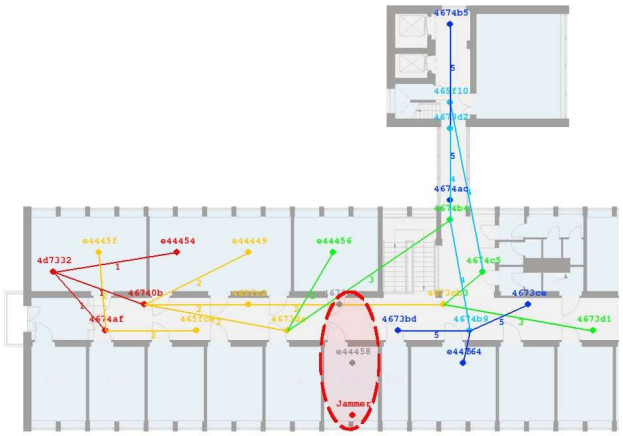


Fig. 4. Jammer placed in a closed space (room), jamming signal power level set to -11 dBm, 2 nodes affected

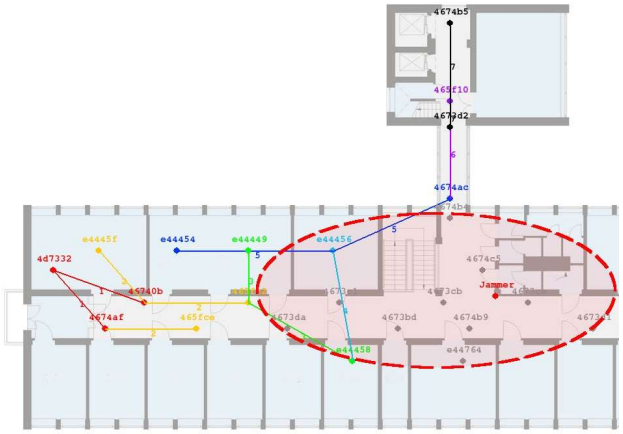


Fig. 5. Jammer placed in an open space (corridors corner), jamming signal power level set to -11 dBm, 10 nodes affected.


Fig. 6. Jammer placed in an open space (corridors corner), jamming signal power level set to -11 dBm, 12 nodes affected.


Fig. 7. Jammer placed in an open space, jamming signal power level set to 0 dBm, 15 affected nodes.

The results of measurements for various locations and signal power levels are presented in Table I. Two phenomena can be observed. The first noticeable effect is the impact of jammer placement on its influence on the network. For jamming power level of -11 dBm, the mean number of nodes that connect to network falls from 93% to 47% when the jamming device is moved from a closed area to open space area. Secondly, Table I also depicts the influence of jammer signal power. For jamming signal set to 0 dBm power level, in closed space, mean NJRR of 58% was measured, where for signal with power level of -11 dBm, measured mean NJRR raised to 93%.

## V. Conclusions

Analyzing measurement results the following conclusions can be drawn:

1) A strong relation exists between jammer placement and its influence on IEEE 802.15.4 network. In relatively open spaces (e.g. corridor, hall, workspace area) the jamming has a stronger influence than in more divided spaces (e.g. office areas, home spaces).

2) Network can be, to some extent, resistant to jamming.

Measurements show, that in an office environment, the IEEE 802.15.4 tree topology network can rebuild around a jamming device. If the network is dense enough, only the closest nodes will be affected by jamming.

3) Network Jamming Resistance Ratio (NJRR) defined as a the ratio between nodes connected to network to all nodes can be a simple and useful measure when other measures of jamming are unavailable.

Conducted measurements prove that threat of jamming has to be taken into consideration when IEEE 802.15.4 network is utilized. Since some part of the network may remain operable if the nodes are optimally located, proper design of the system may help protecting it against jamming attacks.

## References

[1] A. G. Dinker and V. Sharma, "Attacks and challenges in wireless sensor networks," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, March 2016, pp. 3069–3074.

[2] P. B. Hari and S. N. Singh, "Security issues in wireless sensor networks: Current research and challenges," in *2016 International Conference on Advances in Computing, Communication, Automation (ICACCA) (Spring)*, April 2016, pp. 1–6.

[3] A. A. Alsahli and H. U. Khan, "Security challenges of wireless sensors devices (motes)," in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, Jan 2014, pp. 1–9.

[4] A. M. Gamundani, "An impact review on internet of things attacks," in *2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, May 2015, pp. 114–118.

[5] A. Blilat, A. Bouayad, N. E. H. Chaoui, and M. E. Ghazi, "Wireless sensor network: Security challenges," in *2012 National Days of Network Security and Systems*, April 2012, pp. 68–72.

[6] A. Mpitziopoulos and D. Gavalas, "An effective defensive node against jamming attacks in sensor networks," *Security and Communication Networks*, vol. 2, no. 2, pp. 145–163, 2009.

[7] B. Yu and L. Y. Zhang, "An improved detection method for different types of jamming attacks in wireless networks," in *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)*, Nov 2014, pp. 553–558.

[8] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd ed. Norwood, MA, USA: Artech House, Inc., 2011.

[9] "Matlab R2016b Documentation," 2017. [Online]. Available: https://www.mathworks.com/help/phased/ug/barrage-jammer.html

[10] A. A. Hassan, W. E. Stark, and J. E. Hershey, "Error rate for optimal follower tone-jamming," *IEEE Transactions on Communications*, vol. 44, no. 5, pp. 546–548, May 1996.

[11] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems: Operating Principles, Analysis Methods, and Performance Evaluation*. Springer Publishing Company, Incorporated, 2011.

[12] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proceedings of the Fourth ACM Conference on Wireless Network Security*, ser. WiSec '11. New York, NY, USA: ACM, 2011, pp. 47-52.

[13] *JenNet-IP WPAN Stack User Guide*.

[14] "IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std. 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006)*, pp. 1–314, Sept 2011.