Performance Impact of and Protocol Interdependencies of IEEE 802.15.4 Security Mechanisms

Feng Chen*†, Xiaolong Yin*, Reinhard German* and Falko Dressler*

*Dept. of Computer Science, University of Erlangen, Germany
†Siemens AG, Industry Automation Division, Germany

Abstract

The use of wireless technology is continuously gaining interest in industrial automation. With the standardization of the IEEE 802.15.4 protocol, low-power sensor network protocols have been introduced in this field. Recently, we investigated the real-time communication capabilities of this protocol. This study is now extended by incorporating the security mechanisms as provided by the protocol standard. In contrast to other papers, which studied the effectiveness of these security techniques, we are interested in whether the real-time capabilities are affected by encryption and message authentication and to which extend. Based on extensive simulations, we investigated the interdependency of protocol parameters and available security options. The results can be used for optimally selecting such parameters according to the quality of service requirements of the application scenario.

1. Introduction

As pointed out by Willig [1] and Baronti et al. [2], the IEEE 802.15.4 standard [3] has become a recognized industry standard and, thus, well accepted by industrial users. It provides specifications for the Physical Layer (PHY) and Medium Access Control (MAC) sublayer. Products that implement this standard are commercially available at an acceptable low cost. For example, the Siemens Industry Automation Devision is currently evaluating such Wireless Sensor Network (WSN) technologies for use in automation environments.

In this context, ZigBee [4] has recently gained much attention. It is an open specification built on top of the IEEE 802.15.4 standard and focuses on the establishment and maintenance of low-rate sensor networks. One of the main design goals of these standards has been energy efficient operation, whereas hard real-time aspects were not a primary concern. This, on the other hand, has been addressed in other protocol definitions such as WirelessHART [5], which has its primary roots in wired industrial networks.

Besides quality of service requirements, the reliability of the protocol is of high interest in such industrial application domains [1], [6]. Reliability is especially of interest w.r.t. signal distribution and channel properties [7], [8]. We will show that this can be (partially) handled by using appropriate planning tools. The third aspect touches security issues related to both security against attacks such as jamming or protocol level attacks [6], [9].

Focusing on evaluating the performance of IEEE 802.15.4, there have been a number of research activities that utilized evaluation techniques such as experimental lab measurements, analytical calculations, and simulation experiments. As such, simulation models have been developed for all major simulators [10]–[13].

As the protocol provides manifold configuration parameters, some of which are especially relevant to specific industrial application scenarios, many studies have been performed using the mentioned simulation models to characterize and to validate the protocol behavior such these different configurations. Typical performance metrics have been the Packet Loss Rate (PLR), the end-to-end delay, and the goodput with special focus on the energy consumption.

Looking into the security impact of IEEE 802.15.4, there is some essential work by Khan et al. on assessing the quality of the available security mechanisms and on the cost of key management [14], [15]. Furthermore, Sastry and Wagner studied the general security considerations of IEEE 802.15.4 [16]. Yet, there is still no comprehensive evaluation of the interdependency of security options and protocol parameters.

The contributions of this paper can be summarized as follows. We extended our earlier simulation model [12] to study the impact of the different standardized security mechanisms. This model has been calibrated for a specific hardware configuration; however, this can be updated to any other available measurement data without influencing the simulation model. Based on extensive simulation experiments, we provide insight into the performance behavior of IEEE 802.15.4 protocol options in conjunction with the different security settings. This study furthermore reveals some interesting interdependencies between protocol configuration settings and security options that clearly impact the possible communication quality.

978-1-4244-5113-5/09/$25.00

2. A Brief Overview of IEEE 802.15.4

The IEEE 802.15.4 standard supports two network topologies: a star and a peer-to-peer topology. In star networks, the communication occurs only between end devices and a single central controller, which is called the Personal Area Network (PAN) coordinator and which manages the entire PAN. The peer-to-peer topology allows all the devices to communicate arbitrarily with each other as long as they are within a common wireless communication range.

In order to synchronize the communication at MAC layer, the PAN can optionally operate in the so called beacon-enabled mode. Here, each superframe is bounded by periodically transmitted beacon frames and consists of two parts: an active portion and an inactive period. In order to save energy, nodes may enter a low-power mode during the inactive portion. The two parameters Beacon Order (BO) and Superframe Order (SO) determine the structure of the superframe, in particular, the length of the Beacon Interval (BI) and the length of the active portion of the superframe, Superframe Duration (SD), respectively. The active portion of the superframe is further divided into three parts: a beacon, a Contention Access Period (CAP), and a Contention-Free Period (CFP). In this study, we only refer to the CAP, which relies on slotted CSMA/CA.

The IEEE 802.15.4 standard specifies security mechanisms operating at the MAC layer, which provide the following security services: data confidentiality, data authenticity, and replay protection. As shown in Table 1, the security suite specification defines eight security levels that provide different capabilities with respect to data confidentiality and data authenticity. The security level 0 (notated as SL0) is the unsecured model offering no security service. SL1, SL2, and SL3 provide only data confidentiality with an increasing length of authentication tag (4, 8, and 16 octets for Message Integrity Code (MIC) respectively). SL4 offers only encryption operation without data authenticity. The security levers SL5, SL6, and SL7 provide the same data authenticity protection as in SL1, SL2 and SL3 respectively, plus encryption for data confidentiality. If security is enabled, an auxiliary security header with a variable length up to 14 octets will be present in the secured MAC frame, specifying the desired security level and some keying material related informations.

Table 1. Security options in IEEE 802.15.4

Security level	Security attributes	Confidentiality / authenticity
SL0	None	OFF / NO
SL1	MIC-32	OFF / YES
SL2	MIC-64	OFF / YES
SL3	MIC-128	OFF / YES
SL4	ENC	ON / NO
SL5	ENC-MIC-32	ON / YES
SL6	ENC-MIC-64	ON / YES
SL7	ENC-MIC-128	ON / YES

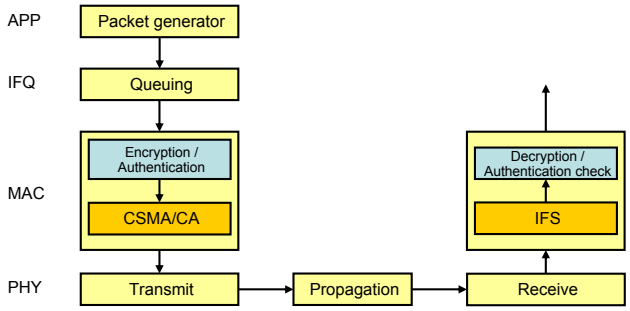


Figure 1. Simulation model including security-related operations

As a replacement of the security suites specified in the IEEE 802.15.4-2003 specification, the CCM* operation mode, which is a generic combined encryption and authentication block cipher mode for encryption and message authentication, is adopted in the IEEE 802.15.4-2006 standard. The block cipher used in the standard is the Advanced Encryption Standard (AES) with length of 128 Bit for both block size and symmetric keys. For data confidentiality, only MAC payload will be encrypted. For data authenticity, both MAC header and payload will be authenticated.

3. Simulation Model and Settings

We extended our IEEE 802.15.4 simulation model to study the impact of different security options and their interdependencies with other protocol settings (see Figure 1). The original model has been well validated in detailed studies of the standard protocol performance and to investigate possible improvements w.r.t. real-time capabilities and the application in industrial environments [12], [13].

We have considered three aspects in the security processing that may have major impacts on the QoS performance. First of all, as a result of security operation, the secured MAC frame has to be increased in length to accommodate additional contents required for security processing, including an auxiliary security header field and an appended MIC if data authentication is enabled. The correspondingly increased length varies between 5 and 21 octets, depending on the specific security level, if the key identifier field in the auxiliary security header is ignored.

The second aspect of the security model is the delay effect that is caused by the execution of cryptographic algorithms. We implemented a dedicated queue that models this behavior. Two aspects need to be considered. First, the encryption / authentication delay for packets to be sent and, secondly, for received packets. The first case needs appropriate artificial delay in the simulation model before the packet is forwarded to the PHY. The latter case is rather

simple as only some fixed decryption time needs to be added. In our current model, we assume that the MAC can precess only one data transmission task including security processing at a time. This means that the additional delay caused by security has strong impact not only on the end-to-end delay of the packet currently in transmission, but also on the overall performance of the whole network, such as PLR and throughput.

Since the CCM* operation model specified in the standard uses AES in a Cipher Block Chaining (CBC) mode, the required time for security processing can be determined by the number of AES rounds, which depends on the length of the packet. The execution time needed for each round of AES with 128-bits block size and key length is about $26\,\mathrm{ms}$, according to the work presented in [17]. The number of AES rounds can be calculated as follows (h being the header length, p the length of the payload, and 16 the AES block size):

$$r_{AES} = \begin{cases} 0 & \text{SL0} \\ \left\lceil \frac{h+p+7}{16} \right\rceil + 2 & \text{SL1–SL3} \\ \left\lceil \frac{p}{16} \right\rceil & \text{SL4} \\ \left\lceil \frac{h+7}{16} \right\rceil + (\left\lceil \frac{p}{16} \right\rceil \times 2) + 2 & \text{SL5–SL7} \end{cases}$$

The third criterion is the security cost w.r.t. energy consumption due to additional computational cost. Our battery model defines three CPU states: active, idle, and sleep. We assume that the CPU is active for packet transfer and during executing security algorithms. The CPU will go to sleep during the inactive period of the superframe, if it has no security task to process. In the rest of time, CPU stays in the idle state. The CPU power in different states can be calibrated to any real hardware type, according to its specifications or measurement results.

In the performance study performed to investigate the interdependency between protocol settings and security options, we use the same network topology that we used to validate the original model is presented in [12]. Twenty sensor nodes and one PAN coordinator are forming an IEEE 802.15.4 based star network. Each sensor node periodically sends its data to the PAN coordinator using slotted CSMA/CA in the beacon-enabled mode. Table 2 summarizes the most important model parameters. The battery and processing parameters have been calibrated for an ATmega Atmel micro controller and a Chipcon CC2420 radio [17], [18].

In all our experiments, statistical significance of the simulation results has been considered. For each simulation with the same input parameters, we run five independent replications. The simulation time required for each simulation varies drastically with the input traffic and parameter settings, however, it has been chosen long enough to guarantee that more than 5000 packets are received by the sink at the end of each running. In the depicted graphs, the mean value of the selected performance measure is plotted as a single point. Error bars are not shown because the values of the relative standard deviation in the obtained results were always less than $1\,\%$, which would be unobservable on the graphs.

4. Simulation Results

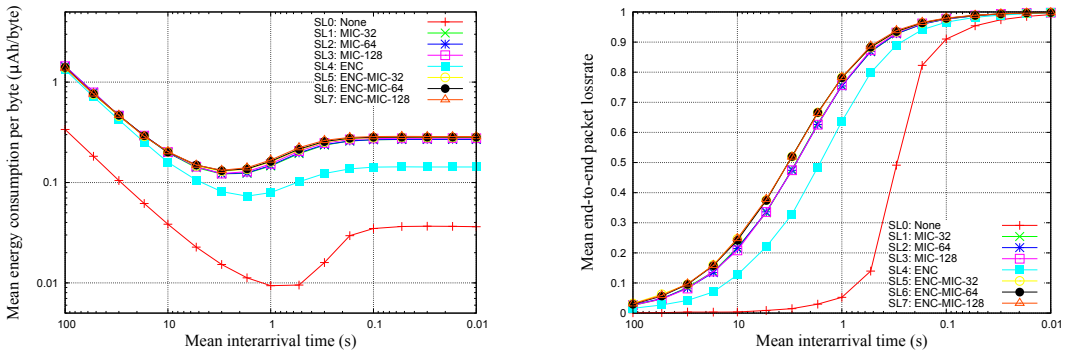
In order to investigate the performance impact of the various security options in IEEE 802.15.4 and the relation between these options and the other protocol parameters, we performed extensive simulations in different scenarios with various (BO,SO) combinations and traffic patterns, including fixed and various payload sizes. For each scenario, we evaluated each of the eight security levels. We measured four typical performance metrics, including energy consumption per received payload byte, PLR, end-to-end delay and goodput. Due to space restrictions, we only present four selected scenarios in two sets of experiments. We selected these results because they clearly show the performance impact and the interdependencies of both the security and the protocol options.

In a first set of experiments, we considered a fixed payload size of $50\,\mathrm{Byte}$ and varied the packet interval within a wide range, covering from light to heavy traffic loads. (BO,SO) is configured with (1,0) and (8,7) in two scenarios, which result in the same duty cycle of $50\,\%$ but different beacon intervals of $0.03\,\mathrm{s}$ and $3.98\,\mathrm{s}$.

The simulation results for (BO,SO) set to (1,0) are shown in Figure 2. The trend of the SL0 curve for every metric has already been analyzed in detail in our previous performance study [12]. In comparison with the SL0 curve, we can see

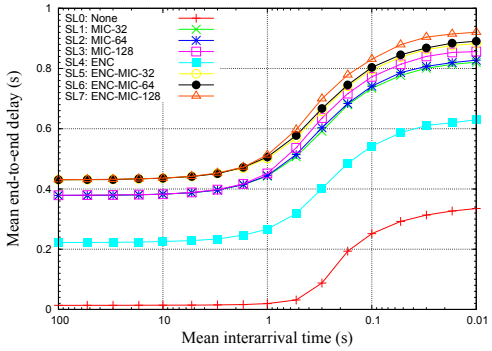
Table 2. Model Parameters

PHY Module Parameters	
Channel number, bitrate	11, $250\,\mathrm{kbit/s}$
Transmitter power	$1\,\mathrm{mW}$
Transmission range	$172\,\mathrm{m}$
Carrier sense sensitivity	$-85\,\mathrm{dB}$
MAC Module Parameters	
Synchronization mode	beacon-enabled
Data transfer model	direct with ACK enabled
IFQ and Traffic Module Parameters	
IFQ size	1
Traffic type	exponential
Battery Module Parameters	
Radio power in sleeping	$0.02\,\mathrm{mA}$
Radio power in idle	$0.37\,\mathrm{mA}$
Radio power in receiving	$19.47\,\mathrm{mA}$
Radio power in sending	$14.6\,\mathrm{mA}$
CPU power in active	$7.6\,\mathrm{mA}$
CPU power in idle	$3.3\,\mathrm{mA}$
CPU power in standby	$0.237\,\mathrm{mA}$

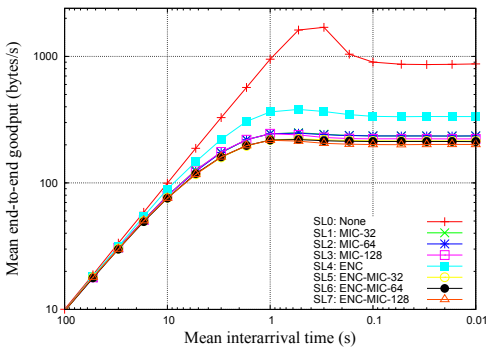


(a) Mean energy consumption per payload byte

(b) End-to-end PLR



(c) Mean end-to-end delay



(d) End-to-end goodput

Figure 2. Performance for (BO,SO) set to (1,0), 50 Byte payload and various packet interval times

that the curves of other seven security-enabled modes vary in scaling, while keeping a similar shape. As one might expect, the results show that the deployment of higher level of security scheme leads to higher energy consumption, PLR, and end-to-end delay, but lower goodput. An exception occurs at the curve for SL4 with only encryption enabled, which is located between SL0 with no security and other six security levels. As described in the previous section, the cost of security operation arises in two ways, the added frame length and the extra latency due to security processing. Compared to other security-enabled modes with authentication operation that will add an extra MIC at the end of MAC payload field, the encryption-only mode does not change the length of the payload field. With respect to the required security processing time according to the equations shown in Section 3, SL4 always needs less number of AES rounds than other security-enabled modes. Thus, among all security modes, SL4 has the lowest cost and the smallest impact on the performance.

For (BO,SO) set to (8,7), we only show the measured mean end-to-end delay (Figure 3). The other measures have a similar trend to the (1,0) configuration. The delay results are of special interest due to the following two observations. First, as the traffic load increases (i.e., the packet interval

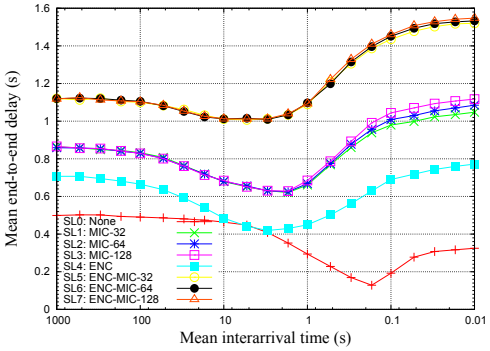
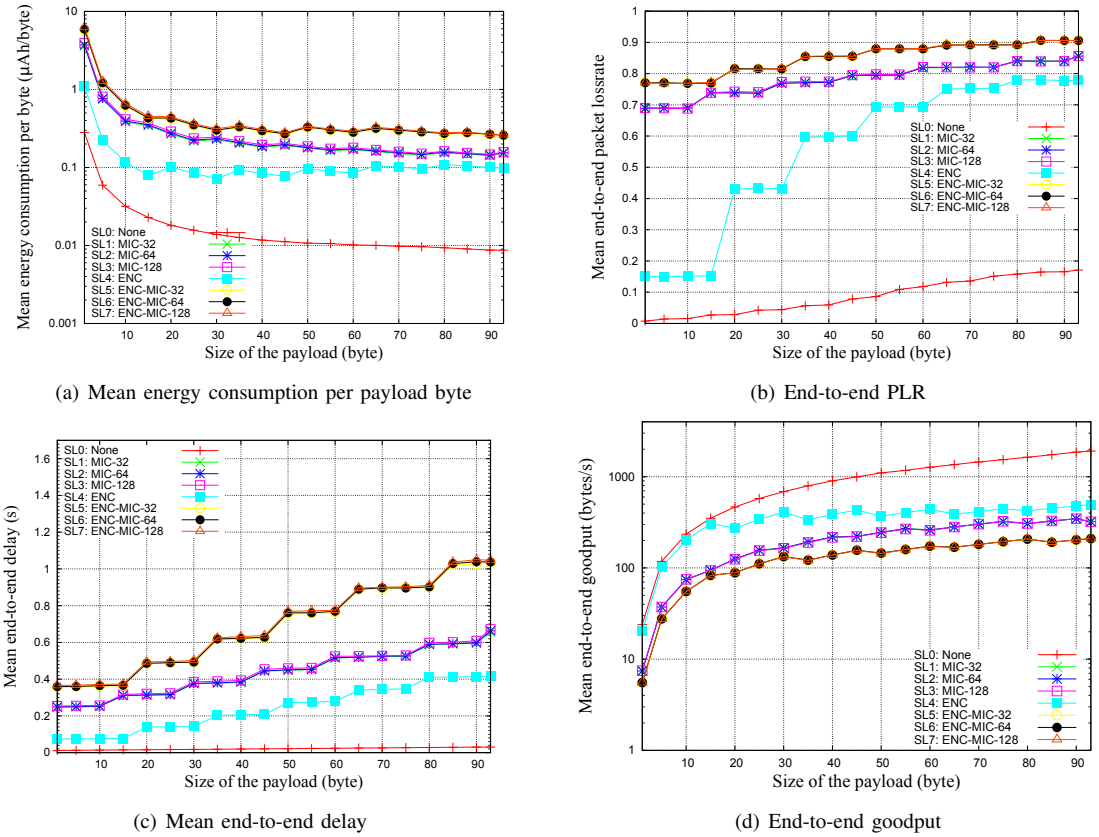


Figure 3. Mean end-to-end delay for (BO,SO) set to (8,7) and 50 Byte payload

decreases), each single delay curve declines, before it ascends again. This phenomenon is mainly caused by the state change in the radio for those packets that experienced a long latency in the sleeping period. Secondly, we can see that under high traffic loads the applied security contents have greater impact on the delay performance than the packet length. For example, the delay values for the group of SL5–SL7 stay almost the same in all traffic conditions, but clearly differ from those for the group of SL1–SL3.



(a) Mean energy consumption per payload byte

(b) End-to-end PLR

(c) Mean end-to-end delay

(d) End-to-end goodput

Figure 4. Performance for (BO,SO) set to (1,0), 1 s packet interval, various payload and security suites

In our second set of experiments, we fixed the packet arriving interval to a moderate value of 1 s and varied the payload size from 1–93 Byte. The simulation results for (BO,SO) set to (1,0) are depicted in Figure 4. The obtained results underline the effect of the different protection schemes on the protocol performance (an exception being again SL4). As shown in Figure 4(a), the decreasing trend of the energy curve along with the increasing payload size is caused by the fact that the same amount of energy is more efficiently used for transmitting payloads. The stepping shape observed in both PLR and delay curves is mainly the result of the round based operation of the AES encryption.

Finally, the measured mean end-to-end delay for (BO,SO) set to (8,7) depicted in Figure 5 also needs further explanation. The SL0 curve shows an unusual trend, in which the mean delay decreases slightly as the payload size increases. This effect is mainly caused by a large variation in the measured individual delay values. A closer look at the statistics of the shown mean values outlines that in this special case a higher variance can be observed. Both the median and the quartiles show the expected increasing trend. The obtained median of the magnitude of several milliseconds is very close to the minimum. However, the maximum is of the magnitude of several seconds. Therefore, the reason for the decreasing in the mean delays is the increasing loss rate of the packets with large delay values, because those packets may suffer from a long sleeping period (at about 2 s in this case) or retransmissions.

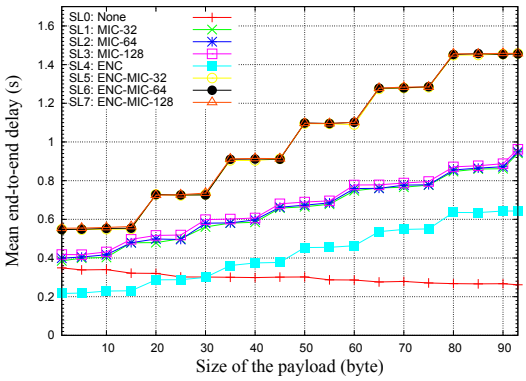


Figure 5. Mean end-to-end delay for (BO,SO) set to (8,7) and 1 s packet intervals

5. Conclusion

We analyzed the capabilities of the industry standard IEEE 802.15.4 protocol for application in industrial automation scenarios. As such, we extended our earlier analysis of the real-time capabilities of the standard protocol to the evaluation of the performance impact of security mechanisms and interdependencies between the protocol parameters and the available security options.

As we can see from the obtained performance metrics, the performance impact is not linear (as might be expected) and needs to be carefully addressed especially for time-critical industrial applications. Further work is planned to include the simulation model into an industrial planning toolkit. Such systems are strongly needed to prepare wireless network applications in industrial automation fields – that also have clear security requirements.

References

[1] A. Willig, "Recent and Emerging Topics in Wireless Industrial Communications: A Selection," *IEEE Transactions on Industrial Informatics*, vol. 4, no. 2, pp. 102–124, May 2008.

[2] P. Baronti, P. Pillai, V. W. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards," *Elsevier Computer Communications*, vol. 30, no. 7, pp. 1655–1695, May 2007.

[3] "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)," IEEE, IEEE Sandard 802.15.4-2006, 2006.

[4] Zigbee Alliance, "Zigbee Specification," Tech. Rep., 2006.

[5] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle, "When HART goes wireless: Understanding and implementing the WirelessHART standard." in *13th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 2008)*. Hamburg, Germany: IEEE, September 2008, pp. 899–907.

[6] H. Wang, "The Application and Research of Wireless Technology in Industrial Network," in *4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCom 2008)*, Dalian, China, October 2008, pp. 1–4.

[7] A. Willig, K. Matheus, and A. Wolisz, "Wireless Technology in Industrial Networks," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1130–1151, June 2005.

[8] M. Kunz, "Wireless LAN planning is a science, not an art!" *The Industrial Ethernet Book*, vol. 34, September 2006. [Online]. Available: http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=1353

[9] V. B. Misic, J. Fung, and J. Misic, "MAC Layer Security of 802.15.4-Compliant Networks," in *2nd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (IEEE MASS 2005): 1st IEEE International Workshop on Wireless and Sensor Networks Security (IEEE WSNS 2005)*, Washington, DC, November 2005.

[10] J. Zheng and M. J. Lee, "A Comprehensive Performance Study of IEEE 802.15.4," in *Sensor Network Operations*. IEEE, 2006, pp. 218–237.

[11] A. Koubaa, M. Alves, and E. Tovar, "A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks," in *5th IEEE International Workshop on Factory Communication Systems (WFCS 2006)*, Torino, Italy, 2006, pp. 183–192.

[12] F. Chen, N. Wang, R. German, and F. Dressler, "Performance Evaluation of IEEE 802.15.4 LR-WPAN for Industrial Applications," in *5th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (IEEE/IFIP WONS 2008)*. Garmisch-Partenkirchen, Germany: IEEE, January 2008, pp. 89–96.

[13] ——, "Simulation study of IEEE 802.15.4 LR-WPAN for industrial applications," *Wiley Wireless Communications and Mobile Computing (WCMC)*, 2009, to appear.

[14] M. Khan, F. Amini, J. Misic, and V. B. Misic, "The Cost of Security: Performance of ZigBee Key Exchange Mechanism in an 802.15.4 Beacon Enabled Cluster," in *3rd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (IEEE MASS 2006): 2nd IEEE International Workshop on Wireless and Sensor Networks Security (IEEE WSNS 2006)*, Vancouver, Canada, October 2006, pp. 876–881.

[15] M. Khan and J. Misic, "Security in IEEE 802.15.4 cluster based networks," in *Security in Wireless Mesh Networks*, ser. Wireless Networks and Mobile Communications, Y. Zhang, J. Zheng, and H. Hu, Eds. Boca Raton, FL: Auerbach Publications, CRC Press, 2008, vol. 6.

[16] N. Sastry and D. Wagner, "Security considerations for IEEE 802.15.4 networks," in *WiSe '04: Proceedings of the 3rd ACM workshop on Wireless security*. New York, NY: ACM, 2004, pp. 32–42.

[17] M. Passing and F. Dressler, "Experimental Performance Evaluation of Cryptographic Algorithms on Sensor Nodes," in *3rd IEEE International Conference on Mobile Ad Hoc and Sensor Systems (IEEE MASS 2006): 2nd IEEE International Workshop on Wireless and Sensor Networks Security (IEEE WSNS 2006)*. Vancouver, Canada: IEEE, October 2006, pp. 882–887.

[18] O. Landsiedel, K. Wehrle, and S. Götz, "Accurate Prediction of Power Consumption in Sensor Networks," in *Second IEEE Workshop on Embedded Networked Sensors (EmNetS-II)*, Sydney, Australia, May 2005.