

Article

## On the Effect of Security and Communication Factors in the Reliability of Wireless Sensor Networks

Damian Rusinek <sup>1,\*</sup> and Bogdan Ksiezopolski <sup>1,2,\*</sup>

<sup>1</sup> Institute of Computer Science, Maria Curie-Sklodowska University pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland

<sup>2</sup> Polish-Japanese Institute of Information Technology Koszykowa 86, 02-008 Warsaw, Poland

\* Authors to whom correspondence should be addressed;

E-Mails: damian.rusinek@umcs.lublin.pl (D.R.); bogdan.ksiezopolski@acm.org (B.K.);

Tel.: +48-81-537-2913 (D.R.); +48 81-537-2939 (B.K.).

*Received: 31 December 2013; in revised form: 7 February 2014 / Accepted: 8 February 2014 /*

*Published: 4 March 2014*

---

**Abstract:** The ensuring reliability of wireless sensor networks (WSN) is one of most important problems to be solved. In this article, the influence of the security and communication factors in the reliability of wireless sensor networks was analyzed. Balancing security against performance in WSN is another issue to be solved. These factors should be considered during security analysis of quality of protection of realized protocol. In the article, we analyze wireless sensor network where hierarchical topologies is implemented with high performance routing sensors that forward big amount of data. We present the experiment results which were performed by high-performance Imote2 sensor platform and TinyOS operating system.

**Keywords:** wireless sensor networks; security economics; quality of protection; reliability

---

### 1. Introduction

Recently, many solutions using wireless sensor networks have been presented. To optimize the communication within the network it should use particular topology suited to the situation in which WSN is implemented. Typical wireless sensor network topologies are described in the article [1] or can

be a modification of them [2]. The network topologies can include different types of nodes which have different function. Most common are:

- **Sensing Node**—it samples some kind of data (e.g., temperature, acceleration, *etc.*);
- **Head Node**—it collects data from sensing nodes and forwards it to gateway;
- **Gateway (Base Station)**—this nodes is directly connected to server and forwards received data to it (*i.e.*, via serial port).

One can enumerate following, main types of topology:

- **Star Topology**, consisting of the gateway node and sensing nodes only;
- **Tree Topology**, consisting of sensing nodes which form a tree and have two main tasks: sense the data and route data from their hierarchical children to their parent;
- **Cluster-Tree Topology**, where head nodes form a tree and route the data from their sensing nodes and other head nodes that are their children in tree;
- **Mesh Topology**, consisting of sensing and head nodes that may use many different paths to the gateway.

The example of real-time WSN with tree or cluster-tree topology is widely understood monitoring, e.g., *health monitoring* or *structural health monitoring (SHM)*. The main aim of health monitoring systems is to collect person's health data and process it in order to find any irregularity in patient's health. If any irregularity occurs, the doctor should be alarmed, e.g., via Internet. These systems can offer mobility to people suffering from, e.g., age related diseases.

The health monitoring systems has been presented in [2–4]. In [2] authors enumerate requirements of such systems: *wearability*, *security*, *reliable communication* and *interoperability*. They also describe prototype sensor network for health monitoring that monitors ECG activity, the upper body trunk position and person's activity. In [3] the smart shirt is presented. It measures electrocardiogram (ECG) and acceleration signals. In [4] authors present wearable belt-type ECG sensor node.

The another type of monitoring is structural health monitoring (SHM). The example of wireless sensor network used for monitoring in civil engineering is presented in [5,6]. Both these articles describes wireless sensor network to be deployed on the bridge to monitor its structural health. SHM can estimate the state of structural health, detect damage or deterioration and determine the structure condition [5]. The type of health monitoring systems described above needs to ensure very reliable communication because people's health and buildings' structural health depends on the sampled and transmitted data. Both above examples of usage of WSN are high performance real-time monitoring systems. They must sample data with high frequency to retrieve very precise data for later analysis, therefore big amount of data needs to be sent to base station and forwarded to servers.

In some solutions, other security attributes must be ensured. For example the security is very important when collecting data, especially confidentiality to hide secret information and authentication to prove the identity of the sender. This may be required in the situation where the condition of a

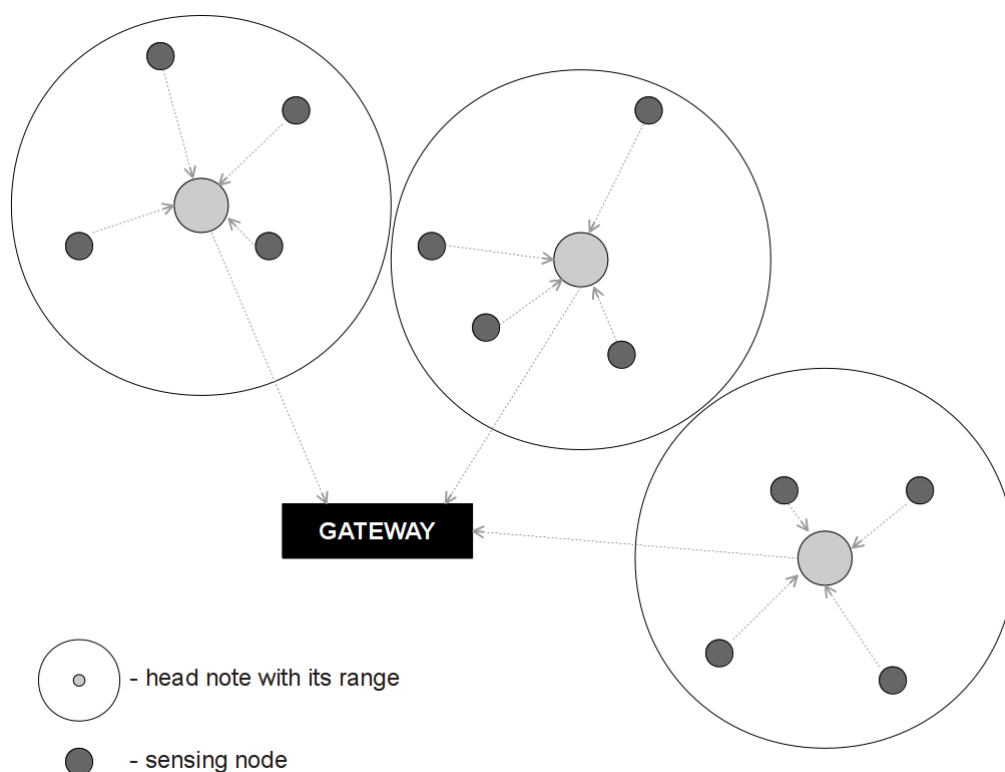
monitored person or building is secret or when important and secret actions are taken according to the collected data.

*1.1. Motivation and Contribution*

Security analysts must decide which security measures should be used for the system protection and whether the selection is sufficient. Authors consider the measures that have an effect on system performance. The methods that increase security and decrease needed resources are out of scope of this article. In the traditional way the security analysts choose the strongest security measures and then they are sure that the system is as secure as possible. Unfortunately, such reasoning leads to the overestimation of security measures which causes an unreasonable increase in the system load [7]. The solution may be determination of the required level of the protection and adjustment of some security measures [8] to these requirements. Such an approach can be achieved by means of the Quality of Protection systems [7,9–11] where the security measures are evaluated according to their influence on the system security.

In this paper authors have focused on efficiency of head sensors which are the part of a cluster-tree topology. This topology is presented on Figure 1. In this architecture, sensing nodes are sampling the data and then forward them to a high performance head node; finally, this node forwards the data to the base station. The high performance head node must transmit the data by establishing high reliable communication [2]. In many protocols, ensuring the quality of data transmission is one of the main goal of the protocol.

**Figure 1.** Cluster-tree topology for WSN.



One of the main contribution of the paper is the analyzing of communication factors which influence the reliability of Wireless Sensor Networks. Reliability is understood as providing the required efficiency of data transmission in real-time WSN where the performance of network plays the crucial role. The tested factors which influence reliability refer to the different settings of radio related factors. The authors have examined their influence on communication speed and packet loss. Another contribution is the analysis of the security factors which influence the WSN's reliability. We have focused on the performance of authentication and encryption methods in real-time wireless sensor networks. When data is sampled and transferred with high frequency, each additional operation may cause delays and can lead to an unacceptable level of packet loss. We provide tests for different values of intervals between two samples and test the increase of packet loss when using different cryptographic modules provided by a high performance sensor platform.

The factors presented in the article can be the part of the QoS systems modeled by QoS-ML [11] modeling language. The QoS-ML introduces the multilevel protocol analysis that extends the possibility of describing the state of the cryptographic protocol. Every single operation defined by the QoS-ML is described by the security metrics which evaluate the impact of this operation into the overall system security. The presented factors can be used as security metrics structure during QoS-ML modeling.

## 2. Communication Factors

In the experiment we test the communication factors that influence reliability security service. The following factors have been examined:

### 1. Payload Size

Packet includes header and payload. While header size is constant (it can change if some additional services are enabled or disabled) the payload size can be changed by developer. Authors check if the payload size manipulation can increase bandwidth.

### 2. Packet Linking Layer

This layer provides automatic retransmission functionality and is responsible for retrying a packet transmission if no acknowledgement was heard from the receiver. Packet Linking layer provides error correction functionality found in Layer 2 of the OSI model [12]. It also fixes the false acknowledgments issue described in [12]. PacketLink is activated on a per-message basis, meaning the outgoing packet will not use PacketLink unless it is configured ahead of time to do so [12]. This layer is turned off by default. This Layer is one of radio stack layers in TinyOS [13]. Authors check the delay in radio communications when the Packet Link layer is turned on.

### 3. Clear Channel Assessment (CCA)

This functionality [13] is provided by CC2420 radio [14] and can be controlled by TinyOS components. By default, the CC2420 radio stack performs a clear channel assessment (CCA) before transmitting. If the channel is not clear, the radio backs off for some short, random period of time before attempting to transmit again. This experiment investigates the influence of radio back off on communication.

#### 4. Low Power Listening (LPL)

Low Power Listening [15] has been introduced to extend batteries lifetime. Asynchronous low power listening is a strategy used to duty cycle the radio while ensuring reliable message delivery [15]. Turning off the radio when it is not used can significantly decrease battery consumption. The idea is to turn on the radio on receiving node and asynchronously performs short receive check. The responsibility for reliable communication is moved to transmitter node, which has to modulate the radio channel until the receiver detects incoming message. The aim of this experiment is to check if asynchronous low power listening has significant influence on transmission speed.

#### 2.1. Measurement Environment

In this section authors describe elements of the environment in which experiment has been carried out.

##### 2.1.1. The Node

In the experiment, authors have used high-performance Imote2 sensor platforms, equipped with a high performance, low power, PXA271 Intel XScale processor and a 802.15.4 CC2420 radio with a built in 2.4 GHz antenna [16]. The features of Imote2 has been presented in Table 1. The Imote2 is very powerful comparing to other small sensors, *i.e.*, micaz, telos, iris. It has been used in the project described in [6].

**Table 1.** Imote2 features.

<b>Feature</b>	<b>Value</b>
Clock speed (MHz)	13–416
Active Power (mW)	44 @ 13 MHz, 570 @ 416 MHz
Program flash (bytes)	32 M
Data Rate (kbps)	250
RAM (bytes)	256 K + 32 M external
Nonvolatile storage (bytes)	32 M (Program flash)
Size (mm)	48 × 36 × 7

##### 2.1.2. Operating System

As the operating system TinyOS [17] has been chosen—the most popular operating system for wireless sensor network applications. It is an open-source project designed for low-power wireless devices, such as those used in sensor networks, ubiquitous computing, personal area networks, smart buildings, and smart meters. As TinyOS is the open-source project, it is widely used in the wireless sensor network academic projects [18–20].

2.1.3. Protocol and Architecture

The Imote2 sensor platforms have been placed in a few meters distance with no obstacles between them. Additionally, there were no other wireless sensor networks in their range. The protocol used in the experiment authors is simple Echo Protocol [21].

With this simple protocol authors avoid the need of time synchronization. The time has been measured on the request-sensor only. Therefore the results include two steps of communication. Otherwise the time synchronization would have to be implemented to receive precise measurement of the time between sending message from the request-sensor and receiving by response-sensor.

The echo protocol has been repeated 100 times with 1 s delay while the request-sensor waits for 100 ms for the response. The packet loss determines the number of failed communications due to the loss of request or response packet.

2.2. Results

In this section the results of the experiment are presented. All tests include minimum, maximum and average value of communication duration.

In the Table 2 all factors are presented. On the left side the radio stack layers tested in experiment are itemized and at the top, different values of payload size are tested. In this experiment the influence of all layers used together has been tested. All four tests were performed for 3 values of payload size (32 B, 64 B, 116 B). The 116 B is the payload size limit.

**Table 2.** Influence of layers on communication speed.

Payload Size		Time (ms)		
		32 B	64 B	116 B
CCA	Min	9.95	13.93	21.09
LPL	Max	18.37	22.84	40.89
PacketLink	Avg	13.99	18.26	25.50
	Min	8.36	12.53	19.27
LPL	Max	9.96	14.13	20.84
PacketLink	Avg	8.41	12.56	19.31
	Min	8.03	12.16	18.89
PacketLink	Max	20.75	26.82	36.10
	Avg	8.17	12.33	19.08
	Min	7.60	11.75	18.49
None	Max	8.19	12.36	19.13
	Avg	7.62	11.78	18.51

First test included all three layers (Clear Channel Assessment, Low Power Listening and Packet Linking layer). In the second, CCA has been removed. In the third, only the Packet Linking layer was used and in the last one all above layers have been removed.

Second two tests examined the influence of all layers separately with payload sizes 32 B (Table 3) and 116 B (Table 4). All results should be compared to the first row ("None") because in this configuration the CCA, PacketLink and LPL are disabled.

**Table 3.** Independent influence of layers on communication speed with payload size = 32 B.

<b>Payload Size = 32 B</b>			<b>Time (ms)</b>		
<b>Layers</b>	<b>Min</b>	<b>Max</b>	<b>Avg</b>	<b>Mode (% occur.)</b>	<b>Packet Loss</b>
None	7.60	7.86	7.62	7.61 (56%)	3%
LPL	7.90	10.45	7.96	7.93 (82%)	0%
PacketLink	8.03	21.13	8.17	8.04 (54%)	0%
CCA	9.02	17.88	13.31	13.82 (3%)	0%

**Table 4.** Independent influence of layers on communication speed with payload size = 116 B.

<b>Payload Size = 116 B</b>			<b>Time (ms)</b>		
<b>Layers</b>	<b>Min</b>	<b>Max</b>	<b>Avg</b>	<b>Mode (% occur.)</b>	<b>Packet Loss</b>
None	18.49	19.13	18.51	18.49 (60%)	2%
LPL	18.77	21.33	18.83	18.81 (51%)	0%
PacketLink	18.89	36.10	19.09	18.92 (39%)	0%
CCA	19.90	28.78	24.19	24.96 (4%)	0%

The last table (Table 5) presents results of payload size tests. For this experiment the following configuration has been used: CCA disabled, PacketLink disabled, LPL disabled.

**Table 5.** Payload size test.

<b>Payload Size</b>	<b>Time (ms)</b>				
	<b>Min</b>	<b>Max</b>	<b>Avg</b>	<b>Mode (% occur.)</b>	<b>Packet Loss</b>
Default (28 B)	7.06	7.64	7.08	7.08 (52%)	2%
32 B	7.60	7.86	7.62	7.61 (56%)	3%
64 B	11.75	12.34	11.78	11.77 (52%)	2%
116 B	18.49	19.13	18.51	18.49 (60%)	2%

*2.3. Results Analysis*

The conclusions drawn from the result tables are described in this section. Authors divided the into groups connected with the factor they concern.

- **Payload Size**

The payload size has significant influence on communication speed. Of course, sending and receiving bigger packets takes longer time, but when one takes radio bandwidth into consideration one can notice that using bigger packets in communication significantly increases radio bandwidth. Indeed, according to Table 3 packet with 32 B of payload is sent and received with average bandwidth of 4,199 B/s, while packet with 116 B (Table 4) payload size is sent and received with average bandwidth of 6,266 B/s.

- **Packet Linking Layer**

This layer is responsible for retransmitting lost packets. It does not need much time to process packet (approx. 0.4 ms), however approximately twice much time is needed to retransmit the packet when one is lost. This may cause big delays in systems in which data is transmitted with high frequency.

- **Clear Channel Assessment (CCA)**

CCA brings some kind of randomness to the results, what can be seen in Table 3 or 4. Indeed, the occurrence percent of mode is very small (3–4%). It is caused by the fact that CCA waits for a random period of time before the radio sends packet. While delay in case of minimum is relatively small (approx. 1.4 ms), when average or maximum are considered it may rise to 5–10 ms. Additionally, delays are independent of payload size.

- **Low Power Listening (LPL)**

The delays in case of Low Power Listening are caused by the fact that radio is off and sensor has to wait until it turns on. The minimum delay is small (approx. 0.3 ms), but for maximum it may rise up to approx. 2–3 ms. However, average duration is very close to the minimum (approx. 0.34 ms), so the situation in which delay rises to some milliseconds is very rare.

### 3. Cryptographic Factors

The aim of these tests is to check the increase of packet loss when cryptographic modules are used in real time wireless sensor networks. When environment information is collected with a high frequency on each node, even negligible factors may have impact on the quality of transmitted data causing noises, delays or prevent the execution of the protocol. During the tests the stand-alone encryption and in-line encryption and MAC security operations were tested. These operations are provided by a CC2420 radio chip. Before the tests of cryptographic modules were launched, non-secured transmission test had been performed to compare with further results.

#### 3.1. Measurement Environment

The experiments have been carried out on Intelmote2 and the TinyOS operating system, these elements are described in Section 2.1.



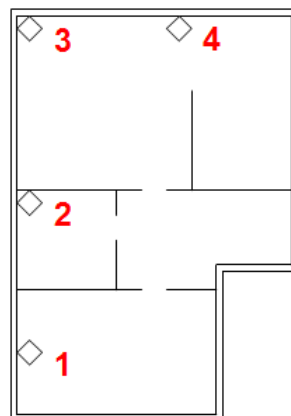
### 3.1.1. Protocol and Architecture

Authors have chosen the Collection Tree Protocol (CTP) [22] for these tests. The CTP provides the best-effort any-cast datagram communication to one of the collection roots in a network; however, the topology has been determined arbitrarily. The tested network is shown in Figure 2. We use four nodes deployed across the laboratory. Three of them sense data and send it to the sink node number 1. Nodes 3 and 4 send data to the sink through node 2.

The following tests examine the increase of packet loss for seven sensing frequencies in the network presented in Figure 2. The intervals between two successive measurements for these frequencies are: 250, 200, 150, 100, 75, 50 and 25 ms respectively. The payload length is 128 bits because it is the size of plain text in the stand-alone encryption. All factors which influence reliability (described in Section 2) were disabled. The experiment has been repeated 10 times and 1,000 packets were sent from each sensing node.

The CTP protocol has no default support for encryption and authentication methods provided by sensor board used in the research. Therefore, the additional TinyOS components for using cryptographic modules in CTP have been implemented.

**Figure 2.** The tested network.



### 3.1.2. Cryptographic Modules

In the research the Intelmote2 (IPR2400) sensor board [16] equipped with CC2420 radio chip [14] was used. It supports a 250 kb/s data rate with 16 channels in the 2.4 GHz band. The CC2420 radio gives possibility to use the following security operations:

#### 1. Stand-Alone Encryption

In the first group, stand-alone operations were tested including encryption operation only. CC2420 radio does not provide stand-alone decryption. As the implementation of stand-alone AES encryption of CC2420, the authors used [23] and made some modifications to obtain the decryption operation. The advantage of this type for encryption is the fact that only payload is encrypted and it is encrypted only once in the sensing node and decrypted once in the sink node. The weakness of this type is the nonce, which has to be transmitted in the message and increases the length

of the message by 4 bytes. The size of nonce should be adjusted to the specific realization of cryptographic protocol and should be increased in the scenario with high risk.

**2. In-Line Security Modes**

The second group of tests includes CTR, CBC-MAC and CCM without any modifications. Encryption with the CTR mode does not require to send additional information. In the CBC-MAC and CCM modes the message authentication code is calculated and it must be transmitted to the receiver to compare it with the code calculated by the receiver. The authentication code can have one of the three lengths: 4, 8 and 16 bytes. Authors use the 16 bytes size for MAC in the experiment. The size of MAC should be adjusted to the specific realization of cryptographic protocol and should be increased in the scenario with high risk.

**3.2. Results**

This section presents the results for each node separately. The tables present the percentage packet loss for each node comparing the authentication and encryption methods depending on a chosen interval between measurements. The results for each cryptographic module for a particular interval are presented in one column. Tables 6–8 present the results for nodes 2, 3 and 4 respectively.

**Table 6.** Packet loss results for node 2.

	<b>Percentage Packet Loss (%)</b>						
Measurements interval (ms)	250	200	150	100	75	50	25
CCM mode (16 B)	0	0	1.25	3.75	49.75	79.25	77.25
CBC-MAC mode (16 B)	0	0	0	0	38	76.5	90
CTR mode	0	0	0	0	12	78.25	89.75
Stand-alone encryption	0	0	0	0	1	68.25	59.75
No encryption	0	0	0	0	0	74.25	81.75

**Table 7.** Packet loss results for node 3.

	<b>Percentage Packet Loss (%)</b>						
Measurements interval (ms)	250	200	150	100	75	50	25
CCM mode (16 B)	0	0.25	0	3.5	8.5	13.75	76.25
CBC-MAC mode (16 B)	0	0	0	0	4.5	35.25	58.5
CTR mode	0.25	0	0	0	2.5	20.75	54.75
Stand-alone encryption	0	0.5	0.25	0.25	0	14.75	72.75
No encryption	0	0	0	0	0.5	3.75	44.75

**Table 8.** Packet loss results for node 4.

	Percentage Packet Loss (%)						
Measurements interval (ms)	250	200	150	100	75	50	25
CCM mode (16 B)	0	0	0	2.75	6.25	38.25	53.25
CBC-MAC mode (16 B)	0	0.75	0	0.25	2.5	15.75	58
CTR mode	0	0	0	0	2	9.75	57
Stand-alone encryption	0	0.25	0.75	0	0	5.5	43.75
No encryption	0	0	0	0.5	0	4	58.25

### 3.3. Results Analysis

These results show that the quality of transmitted data is very poor for the measurement interval equal 50 ms and lower. The packet loss increases the most for the forwarding node number 2, which cannot forward packets from nodes 3 and 4 and send its own packet.

The stand-alone encryption increases packet loss for the intervals 50 and 25 ms, but no difference is shown for the interval 75 ms and larger. Therefore one can see that the additional 4 bytes (nonce) in the message do not have influence on the quality of the transmitted data for interval 75 ms, which is considered as the lowest interval according to the results for non-secured communication test. One can see that using the stand-alone encryption entails lower packet loss than using the in-line CTR encryption. It may be caused by the fact that when using the stand-alone encryption the message is encrypted and decrypted only once, while in the case of CTR the encryption message is encrypted and decrypted on each forwarding node.

The results for the CTR encryption are slightly worse than for the stand-alone one. The size of message is 33 bytes: header—11 bytes; security header—6 bytes; data—16 bytes. The CTR mode encryption increases the packet loss for 75 ms interval to approx. 12% in the forwarding node. This may be caused by the fact that the packet is encrypted/decrypted in each node, even forwarding while in the stand-alone case not only the packet is encrypted and decrypted once, but also the header is not encrypted at all.

In case of CBC-MAC and CCM modes the message authentication code (MAC) must be transmitted in the message what increases packet size and transmission time. Therefore, one of three MAC lengths can be chosen to balance between the strength of MAC and the packet size. The results include MAC of 16 bytes length. The size of message is 49 bytes: header—11 bytes; security header—6 bytes; data—16 bytes; MAC—16 bytes. The results of CBC-MAC tests show that, including the authentication code, it increases the packet loss significantly. All differences concern the 75 ms interval, because for larger intervals there is no packet loss increase. Compared to the non-secured test, CBC-MAC (16 bytes) increases packet loss to 38%. However, if the interval is 100 ms or higher, even CBC-MAC does not increase the packet loss. The CCM (16 bytes) is the only one that increases the packet loss for the interval 100 ms—the increase is approx. 4%. Furthermore, the packet loss for 75 ms interval in CCM is approximately the sum of packet loss of CTR and CBC-MAC for the same MAC size.

#### 4. Conclusions

The aim of the research was to check the impact of security and communication factors on the reliability in wireless sensor networks. Reliability is understood as providing the required efficiency of data transmission in real-time WSN where the performance of network plays the crucial role. We have checked the influence of radio related factors on radio communication speed and packets loss. The results show that many improvements can be included in high performance real time protocols and it can significantly increase the radio bandwidth.

On the other hand, we can use different cryptography modules to implement different levels of confidentiality or authentication. Therefore, we have also checked encryption and authentication methods from CC2420 radio, integrated in particular with an Intelmote2 sensor board, in terms of the quality of transmitted data, especially the packet loss. The presented results show that hardware cryptographic modules present in the devices should be taken into consideration. They may fulfill security requirements without packet loss increase, therefore the quality of the transmitted data would remain high and the protocol would be secured.

The cryptographic protocols can be analyzed on different levels of security analysis by means of QoP-ML modeling language. Owing to that the QoP analysis can take into consideration any presented factors which influence the overall system security. In this article the benchmark of cryptographic operations are presented which can be used as the security metrics structure [11] in the QoP-ML approach.

#### Author Contributions

- Introduction—Damian Rusinek and Bogdan Ksiezopolski.
- Research plan of communication and cryptographic factors—Damian Rusinek and Bogdan Ksiezopolski.
- Experiments of communication and cryptographic factors—Damian Rusinek.
- Results analysis and conclusions—Damian Rusinek and Bogdan Ksiezopolski.

#### Conflict of Interest

The authors declare no conflict of interest.

#### References

1. Baronti, P.; Pillai, P.; Chook, V.W.; Chessa, S.; Gotta, A.; Fu, Y.F. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards. *Comput. Commun.* **2007**, *30*, 1655–1695.
2. Milenkovic, A.; Otto, C.; Jovanov, E. Wireless sensor networks for personal health monitoring: Issues and an implementation. *Comput. Commun.* **2006**, *29*, 2521–2533.

3. Lee, Y.D.; Chung, W.Y. Wireless sensor network based wearable smart shirt for ubiquitous health and activity monitoring. *Sens. Actuators B Chem.* **2009**, *140*, 390–395.
4. Jeong, D.; Kew, H. Real-Time Monitoring of Ubiquitous Wearable ECG Sensor Node for Healthcare Application. In Proceedings of the International Conference on Computational Science and Its Applications (ICCSA 2009), Seoul, Korea, 29 June–2 July 2009; pp. 868–884.
5. Yin, A.; Wang, B.; Liu, Z.; Hu, X. Design and Implementation of the Structure Health Monitoring System for Bridge Based on Wireless Sensor Network. In Proceedings of the 6th International Symposium on Neural Networks (ISNN 2009), Wuhan, China, 26–29 May 2009; pp. 915–922.
6. Gao, Y.; Spencer, B.F., Jr. *Structural Health Monitoring Strategies for Smart Sensor Networks*; Technical Report; Newmark Structural Engineering Laboratory, University of Illinois at Urbana-Champaign: Urbana, Illinois, USA, 2008.
7. Ksiezopolski, B.; Kotulski, Z.; Szalachowski, P. Adaptive approach to network security. *Commun. Comput. Inf. Sci.* **2009**, *158*, 233–241.
8. Szalachowski, P.; Ksiezopolski, B.; Kotulski, Z. CMAC, CCM and GCM/GMAC: Advanced modes of operation of symmetric block ciphers in the Wireless Sensor Networks. *Inf. Process. Lett.* **2010**, *110*, 247–251.
9. Ksiezopolski, B.; Kotulski, Z.; Szalachowski, P. On QoP Method for Ensuring Availability of the Goal of Cryptographic Protocols in the Real-Time Systems. In Proceedings of the 1st European Teletraffic Seminar, Poznan, Poland, 14–16 February 2011; pp. 195–202.
10. Ksiezopolski, B.; Kotulski, Z. Adaptable security mechanism for the dynamic environments. *Comput. Secur.* **2007**, *26*, 246–255.
11. Ksiezopolski, B. QoP-ML: Quality of protection modelling language for cryptographic protocols. *Comput. Secur.* **2012**, *31*, 569–596.
12. Moss, D.; Levis, P. TEP 127: Packet Link Layer. Available online: <http://www.tinyos.net/tinyos-2.x/doc/html/tep127.html> (accessed on 3 September 2013).
13. Moss, D.; Hui, J.; Levis, P.; Choi, J.I. TEP 126: CC2420 Radio Stack. Available online: <http://www.tinyos.net/tinyos-2.x/doc/html/tep126.html> (accessed on 3 September 2013).
14. CC2420. Available online: <http://focus.ti.com/lit/ds/symlink/cc2420.pdf> (accessed on 1 September 2013).
15. Moss, D.; Hui, J.; Klues, K. TEP 105: Low Power Listening. Available online: <http://www.tinyos.net/tinyos-2.x/doc/html/tep105.html> (accessed on 3 September 2013).
16. *ITS400, Imote2 Basic Sensor Board*; Crossbow Technology Inc.: San Jose, CA, USA, 2007.
17. TinyOS. Available online: <http://www.tinyos.net> (accessed on 1 September 2013).
18. Rice, J.A.; Spencer, B.F., Jr. Structural Health Monitoring Sensor Development for the Imote2 Platform. In Proceedings of SPIE Sensors and Smart Structures Technologies for Civil, Mechanical, and Aerospace Systems, San Diego, CA, USA, 9 March 2008; doi:10.1117/12.776695.
19. Virone, G.; Wood, A.; Selavo, L.; Cao, Q.; Fang, L.; Doan, T.; He, Z.; Stankovic, J. An Advanced Wireless Sensor Network for Health Monitoring. In Proceedings of Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare, Arlington, VA, USA, 2–4 April 2006; pp. 2–4.

20. Gao, T.; Pesto, C.; Selavo, L.; Chen, Y.; Ko, J.; Kim, J.; Terzis, A.; Watt, A.; Jeng, J.; Chen, B.; *et al.* Wireless Medical Sensor Networks in Emergency Response: Implementation and Pilot Results. In Proceedings of 2008 IEEE Conference on Technologies for Homeland Security, MA, USA, 12–13 May 2008; pp. 187–192.
21. Postel, J. Echo Protocol. Available online: <http://tools.ietf.org/html/rfc862> (accessed on 3 September 2013).
22. Fonseca, R.; Gnawali, O.; Jamieson, K.; Kim, S.; Levis, P.; Woo, A. The Collection Tree Protocol. Available online: <http://www.tinyos.net/tinyos-2.x/doc/html/tep123.html> (accessed on 3 September 2013).
23. SJTU CIS Lab. The Standalone aes Encryption of CC2420. Available online: [http://cis.sjtu.edu.cn/index.php/The\\_Standalone\\_AES\\_Encryption\\_of\\_CC2420\\_\(TinyOS\\_2.10\\_-and\\_MICAz\)](http://cis.sjtu.edu.cn/index.php/The_Standalone_AES_Encryption_of_CC2420_(TinyOS_2.10_-and_MICAz)) (accessed on 4 September 2013).

© 2014 by the authors; licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/>).