VERSITA

Annales UMCS Informatica AI XI, 3 (2011)
117–127; DOI: 10.2478/v10065-011-0018-3

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

Influence of CCM, CBC-MAC, CTR and stand-alone encryption on the quality of transmitted data in the high-performance WSN based on Imote2

Damian Rusinek*, Bogdan Księżopolski†

Institute of Computer Science, Maria Curie-Sklodowska University,
pl. M. Curie-Sklodowskiej 1, 20-031 Lublin, Poland

Abstract

In this paper we examine the influence of different types of encryption and authentication on the quality of transmitted data in the high-performance WSN based on Imote2. The performance has been tested in the wireless sensor network using Collection Tree Protocol. The examined types and modes of encryption are provided by the hardware of used sensor platforms Intelmote2 and its integrated radio chip CC2420. The presented results can be helpful to choose which cryptographic modules should be implemented according to the acceptable packet loss.

1. Introduction

Most Wireless Sensor Networks are used for various types of monitoring (Health Monitoring, Structural Health Monitoring, etc.). The aim of these networks is to collect data and transfer it to the server, which analyses the results. These networks may be implemented using different topologies (ie. star, mesh, tree), which may be changed depending on the situation.

*E-mail address: damian.rusinek@gmail.com

†E-mail address: bogdan.ksiezopolski@umcs.lublin.pl

Topologies consist of three types of nodes:

- leaf - a sensing node, which only collects data and sends it to the gateway,
- routing node - a node, which is in the middle between leaves and the gateway; it may also sense data,
- sink - the gateway, which receives all data from sensing nodes and forward it to the server (ie. via wired collection).

In the case of collecting data by one gateway, the tree topology seems to be the most effective and in this paper the protocol that uses this topology is applied.

In some situations the security is very important when collecting data, especially confidentality 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.

In this paper 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 interspaces between two samples and test the increase of packet loss when using different cryptographic modules provided by a high performance sensor platform.

2. Environment

In this section we describe each element that has been used in our tests. Firstly, we describe the CTP protocol [**1**] and TinyOS [**2**] operating system for which the protocol has been implemented. We also describe the encryption mechanisms present in the CC2420 radio that Intelmote2 is equipped with. At last we depict the scenarios of our tests.

2.1. CTP

The Collection Tree Protocol provides the best-effort anycast datagram communication to one of the collection roots in a network [**1**]. It is a tree-based protocol used to collect data from many nodes to one node called ”the sink”. The example of the tree-based network created by CTP is presented in Fig. 1. The white nodes are sensing nodes that send collected data through the network to the black node – the sink.

The tested network is shown in Fig. 2. We use four nodes deployed accross 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.

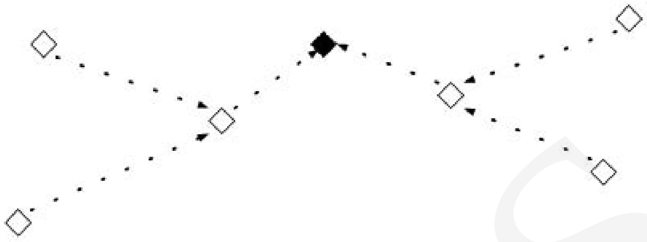

Fig. 1. The example of tree-based network.

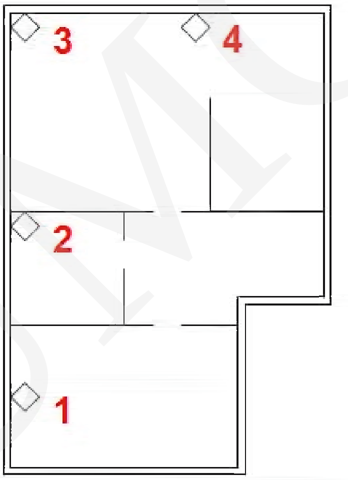

Fig. 2. The tested network.

2.2. TinyOS

As the operating system TinyOS [**2**] has been chosen – the most popular operating system for wireless sensor network applications. It it an open-source project designed for low-power wireless devices, such as those used in sensor networks, ubiquitious 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 ([**3, 4, 5**]).

In the research the CTP protocol implemented for TinyOS by Rodrigo Fonseca et al. has been used [**1**]. The procotol 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 has been implemented.

2.3. Cryptographic modules

In the research there was used the Intelmote2 (IPR2400) sensor board [**6**] equipped with CC2420 radio chip [**7**]. The Intelmote2 is a high performance sensor board compared to other popular sensors, ie. micaz, telosb, etc. The radio chip is IEEE 802.15.4 compliant RF transceiver with baseband modem and MAC support. It supports a 250 kb/s data rate with 16 channels in the 2.4 Ghz band.

CC2420 radio gives possibility to use two types of security operations. Firstly, it features hardware IEEE 802.15.4 MAC security operations, which include counter mode (CTR) encryption / decryption, CBC-MAC authentication and CCM encryption + authentication [**7**]. Secondly, it provides stand-alone AES encryption (without decryption), in which one 128 bit plaintext is encrypted to a 128 bit ciphertext. All above security operations are based on the AES encryption algorithm using 128 bit keys.

To use the first type of operations, the developer has to choose and assign the security operation to the message to be sent. He can choose either encryption only (CTR) or authentication only (CBC-MAC) or both (CCM). The last two types of operations increase length of the packet as they add MAC to it. The length of MAC can be chosen from the three values: 4, 8 or 16 bytes.

The stand-alone AES encryption differs from the previous security operations because it can be used not only on frames, but on any data declared in the developed application as long as it is 128 bit long. The encrypted data does not have to be transmitted and does not have to be placed in TXFIFO as a frame because the stand-alone encryption operation has separate buffers. The stand-alone operations do not include decryption, therefore the encryption / decryption operation similar to the CTR mode has been implemented.

3. Tests

The aim of the research is to check the increase of packet drop when cryptographic modules are used in real time wireless sensor networks. When environment information us collected with 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. The following tests examine the increase of packet drop for seven sensing frequencies in the network presented in Figure 2. The interspaces between two different 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 plaintext in the stand-alone encryption. All optional features of TinyOS radio stack (LPL, PLL) [**8**] were disabled and signal strength was set to assure communication through the protocol's tree network. Manipulating signal strength does not have influence on the packet loss [**8**].

Before the tests of cryptographic modules were launched, non-secured transmission test had been performed to compare with further results. Similarly to the cryptographic modules division, tests in the research were divided into two groups. Firstly, the stand-alone encryption and secondly all MAC security operations were tested.

3.1. Stand-alone encryption

In the first group – stand-alone operations were tested including encryption operation only. CC2420 radio does not provide stand-alone decryption. It may be caused by the fact that CC2420 provides only those modes that need ecryption algorithm, which are: CTR, CBC-MAC and CCM.

As the implementation of stand-alone AES encryption of CC2420 the authors used [**9**] and made some modifications to obtain the decryption operation.

The modifications were similar to block cipher modes that need only encryption algorithm. Firstly, a nonce value is generated and encrypted with the key that is installed on the sink node and sensing node. After encryption, the ciphertext is xored with the message. To decrypt data, the receiver needs nonce, therefore it must be transmitted within the message. The length of nonce is 4 bytes and the rest of encrypted plaintext is filled with zeros.

To sum up, 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.

3.2. MAC security operations

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 informations, therefore the delays in communication may be caused only by the calculation time. 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. Therefore the delays may be caused not only by the calculation time but also by the fact that more data must be transmitted. The authentication code can have one of the three lengths: 4, 8 and 16 bytes.

4. Results

In this section the results are presented. They are grouped and ordered similarly to the tests order described in the previous section.

Firstly, the results of non-secured transmission test (no cryptographic operations) are presented in Table 1. The size of message is 27 bytes: header - 11 bytes; data - 16 bytes.

Table 1. Results for non-secured network.

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	0	74.25	81.75
Packet loss (node 3) (%)	0	0	0	0	0.5	3.75	44.75
Packet loss (node 4) (%)	0	0	0	0.5	0	4	58.25
Avg. packet loss (%)	0	0	0	0.17	0.17	27.33	61.58

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

4.1. Encryption (stand-alone)

The results for the stand-alone encryption are presented in Table 2. The size of message is 31 bytes: header - 11 bytes; data - 16 bytes; nonce - 4 bytes.

Table 2. Results for stand-alone encryption.

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	1	68.25	59.75
Packet loss (node 3) (%)	0	0.5	0.25	0.25	0	14.75	72.75
Packet loss (node 4) (%)	0	0.25	0.75	0	0	5.5	43.75
Avg. packet loss (%)	0	0.25	0.33	0.08	0.33	29.5	58.75

The stand-alone encrytpion increases packet drop for the interspaces 50 and 25 ms, but no difference is shown for the interspace 75 ms and langer. 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 interspace 75 ms, which are considered as the lowest interspace according to the results for non-secured communication test.

4.2. Encryption (CTR)

The results for the CTR encryption are slightly worse than for the stand-alone one and are presented in Table 3. The size of message is 33 bytes: header - 11 bytes; security header - 6 bytes; data - 16 bytes.

Table 3. Results for the CTR encryption.

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	12	78.25	89.75
Packet loss (node 3) (%)	0.25	0	0	0	2.5	20.75	54.75
Packet loss (node 4) (%)	0	0	0	0	2	9.75	57
Avg. packet loss (%)	0.08	0	0	0	5.5	36.25	67.17

The CTR mode encryption increases the packet drop for 75 ms interspace 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.

The following two tests include the message authentication code (MAC) which must be transmitted in the message which 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. Tests were performed for all three MAC lengths for both CBC-MAC and CCM.

4.3. Authentication (CBC-MAC)

The results for CBC-MAC are presented in Tables 4, 5, 6 for MAC, lengths 4, 8 and 16 bytes respectively. The sizes of messages are 33, 37 and 41 bytes: header - 11 bytes; security header - 6 bytes; data - 16 bytes; mac - 4, 8, and 16 bytes respectively.

Table 4. Results for CBC-MAC (4 bytes).

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	19.75	80	89.75
Packet loss (node 3) (%)	0	0	0.75	1	2	23.5	57.5
Packet loss (node 4) (%)	0.25	0	0	0	3.25	10.5	55
Avg. packet loss (%)	0.08	0	0.25	0.33	8.33	38	67.42

The results of CBC-MAC tests show that including the authentication code increases the packet loss significantly. All differences concern the 75 ms interspace, because for larger interspaces there is no packet loss increase. Compared

Table 5. Results for CBC-MAC (8 bytes).

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	21.75	77.5	89.25
Packet loss (node 3) (%)	0	0	0.5	0.25	3.25	20.5	57.25
Packet loss (node 4) (%)	0	0	0	0	2	17	56.75
Avg. packet loss (%)	0	0	0.17	0.08	9	38.33	67.75

Table 6. Results for CBC-MAC (16 bytes).

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	38	76.5	90
Packet loss (node 3) (%)	0	0	0	0	4.5	35.25	58.5
Packet loss (node 4) (%)	0	0.75	0	0.25	2.5	15.75	58
Avg. packet loss (%)	0	0.25	0	0.08	15	42.5	68.83

to the non-secured test, CBC-MAC (4 bytes) increases the cumulated packet loss by 25%, 8 bytes by 27% and 16 bytes by 45%. However, if the interspace is 100 ms or higher, even CBC-MAC (16 bytes) does not increase the packet loss.

4.4. Encryption and authentication (CCM)

The results for CCM are presented in Tables 7, 8, 9 for the MAC lengths 4, 8 and 16 bytes respectively. The sizes of messages are 33, 37 and 41 bytes: header - 11 bytes; security header - 6 bytes; data - 16 bytes; mac - 4, 8, and 16 bytes respectively.

Table 7. Results for CCM (4 bytes).

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	38.25	79.5	80.5
Packet loss (node 3) (%)	0	0	0	0.25	1	21.25	59.5
Packet loss (node 4) (%)	0	0	0	0	2.75	17.75	55
Avg. packet loss (%)	0	0	0	0.08	14	39.5	65

CCM (16 bytes) is the only one that increases the packet loss for the interspace 100 ms – the increase is approx. 10%. Lower interspaces provide approx. 50% greater packet loss than their equivalents in the CBC-MAC mode. Furthermore, the packet loss for 75 ms interspace in CCM is approximately the sum of packet losses of CTR and CBC-MAC for the same MAC size.

Table 8. Results for CCM (8 bytes).

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	0	0	21.5	76.5	85.75
Packet loss (node 3) (%)	0	0	0	0.25	4.5	24.75	55.25
Packet loss (node 4) (%)	0.25	0	0	0.25	5.75	14.5	57
Avg. packet loss (%)	0.08	0	0	0.17	10.58	38.58	66

Table 9. Results for CCM (16 bytes).

Interspace (ms)	250	200	150	100	75	50	25
Packet loss (node 2) (%)	0	0	1.25	3.75	49.75	79.25	77.25
Packet loss (node 3) (%)	0	0.25	0	3.5	8.5	13.75	76.25
Packet loss (node 4) (%)	0	0	0	2.75	6.25	38.25	53.25
Avg. packet loss (%)	0	0.08	0.42	3.33	21.5	43.75	68.92

4.5. Nodes results

This subsection 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 interspace. The results for each cryptographic module for a particular interspace are presented in one column, therefore it is easier to compare them. Tables 10, 11, 12 present the results for nodes 2, 3 and 4 respectively.

Table 10. Packet loss results for node 2.

Interspace (ms)	250	200	150	100	75	50	25
CCM (8)	0	0	0	0	21.5	76.5	85.75
CBC-MAC (8)	0	0	0	0	21.75	77.5	89.25
CTR	0	0	0	0	12	78.25	89.75
SA Encryption	0	0	0	0	1	68.25	59.75
No Encryption	0	0	0	0	0	74.25	81.75

One can see that using the stand-alone encryption entails lower packet loss than using the hardware 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.

Table 11. Packet loss results for node 3.

Interspace (ms)	250	200	150	100	75	50	25
CCM (8)	0	0	0	0.25	4.5	24.75	55.25
CBC-MAC (8)	0	0	0.5	0.25	3.25	20.5	57.25
CTR	0.25	0	0	0	2.5	20.75	54.75
SA 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 12. Packet loss results for node 4.

Interspace (ms)	250	200	150	100	75	50	25
CCM (8)	0.25	0	0	0.25	5.75	14.5	57
CBC-MAC (8)	0	0	0	0	2	17	56.75
CTR	0	0	0	0	2	9.75	57
SA Encryption	0	0.25	0.75	0	0	5.5	43.75
No Encryption	0	0	0	0.5	0	4	58.25

5. Conclusions

The aim of the research was to check the impact of encryption and authentication methods from CC2420 radio integrated in particular in Intelmote2 sensor board on 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 range of cryptographic modules is wide and one can choose from the least consuming stand-alone encryption to the more complex and time consuming CCM encryption with authentication. If the protocol does not sense and transmit data with very high frequency, any of the tested methods can be deployed as this does not increase packet los for lower frequencies. In the case of larger networks, the tests presented in this paper should be repeated for them as the more forwarding nodes are in the network and the deeper the tree is, the larger packet loss is brought in by the deployed cryptographic modules. The research results can be used when implementing the scalable Quality of Protection modules [**10, 11**].

References

[1] Fonseca R., Gnawali O., Jamieson K., Kim S., Levis P., Woo A., The Collection Tree Protocol; http://www.tinyos.net/tinyos-2.x/doc/html/tep123.html (2007)

[2] TinyOS; http://www.tinyos.net (2010)

[3] Rice, J. A. and Spencer Jr., B. F., Structural health monitoring sensor development for the Imote2 platform, Proc. SPIE Smart Structures/NDE. (2008)

[4] 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 Transdisciplinary Conference on Distributed Diagnosis and Home Healthcare (D2H2) (2006)

[5] Gao T., Pesto C., Selavo L., Chen Y., Ko J., Kim J., Terzis A., Watt A., Jeng J., Chen B., Lorincz K., Welsh M., Wireless medical sensor networks in emergency response: Implementation and pilot results, In HST Waltham, MA, USA (2008)

[6] Intelmote2 (IPR 2400), http://www.xbow.com.cn/LinkClick.aspx?fileticket=i7FK6%2B1oodU%3D&tabid=121 (2007)

[7] CC2420, http://focus.ti.com/lit/ds/symlink/cc2420.pdf (2010)

[8] Rusinek D., Księżopolski B., Kotulski Z., On effect of the communication factors on the protocol's goal availability service in high performance real-time Wireless Sensor Networks, (In Polish), Studia Informatica 32(3A(98)) (2011): 187.

[9] SJTU CIS Lab., The standalone aes encryption of CC2420, http://cis.sjtu.edu.cn/index.php/The_Standalone_AES_Encryption_of_CC2420_(TinyOS_2.10_and_MICAz) (2008)

[10] Księżopolski B., Kotulski Z., Adaptable security mechanism for the dynamic environments. Computers & Security 26 (2007): 246.

[11] Księżopolski B., Kotulski Z., Szalachowski P., Adaptive approach to network security. Communications in Computer and Information Science 158 (2009): 233.