Employing Chaotic Encryption for IEEE 802.15.4-based LR-WPANs

Cuneyt Bayilmis, Unal Cavusoglu, Akif Akgul, Abdullah Sevin, and Sezgin Kacar

Abstract—Low-Rate Wireless Personal Area Networks (LR-WPANs) have widespread usage for industrial applications because of being small, power-efficient, and low-cost. Therefore security is an important issue for LR-WPANs. The IEEE 802.15.4 standard is one of the most common solutions for LR-WPANs and defines only the physical and data-link layers of the OSI model. For this reason most of security issues are ignored owing to scope of this standard. Hence, security mechanisms should be implemented in the applications. This paper presents using chaotic-based encryption in the IEEE 802.15.4 standard to secure communication. In addition, modelling and simulation of the proposed structure have been realized using OPNET Modeler.

Keywords—Security, Chaotic, IEEE 802.15.4, R-WPANs.

I. INTRODUCTION

Security is an important research topic in Low-Rate Wireless Personal Area Networks (LR-WPAN). If security is not provided, the data can be found out and operation of the network can be prevented. There are many security protocols and encryption algorithms to ensure data security in LR-WPANs. Security protocols and encryption algorithms contain powerful mathematical operations generally thus increasing energy consumption. Because of LR-WPANs have limited hardware resources such as amount of memory, storage space, area code etc. therefore, the resource usage in the design of security protocol must be considered. Using these limited resources has to perform the procedures [1, 2].

Security issue deals with security protocols and encryption algorithms in LR-WPAN. A number of security protocol and encryption methods for reliable data transfer in low-rate wireless personal area networks have been developed.

Examples of security protocols are given Tinysec [3], Sensec [4], Minisec [5], Fsmac [6], Spins [7], WSNSec [8]. On the other hand, examples of encryption algorithms are given Skipjack [9], AES [10], SEA [11].

Tinysec protocol is robust against to repetition attacks. It is used as intrusion detection and defense techniques on CSMA / CA protocol, is formed. Each node has its own mechanism to defend. Therefore, there is a scattered defense mechanism. Spins protocol is composed of two secure building block as called mTesla and SNEP. Spins protocol is strong against repetition and eavesdropping attacks. Data confidentiality, integrity provide.

Nowadays chaotic encryption is also used for WSNs. Chaotic systems are very limited studies conducted using encryption for WSNs. Shuai and Xia-xin have developed discrete chaos system and Feistel structure using a new block encryption algorithm [12]. Liu and colleagues developed a new method for chaotic encryption algorithm. This method has been compared with the performance of RC5-RC6 algorithms and developed chaotic system shows more effective results [13]. Fang et al; widely used in the literature for a cryptographic application with chaotic systems realized for WSN. The methodology developed has been shown to provide security with less cost [14].

In this study, employing chaotic encryption for IEEE 802.15.4 based LR-WPAN is proposed and its implementation has been realized using OPNET Modeler software. Also, performance evaluation carry out according to end-to-end delay and energy consumption.

The remainder of the paper is organized as follows. Section 2 deals with IEEE 802.15.4. Section 3 details the chaotic encryption based security mechanism. In Section 4 simulation results from presented system are provided, followed by final remarks in the last section.

II. IEEE 802.15.4

The IEEE 802.15.4 standard defines physical and MAC
layer protocols of the Low-Rate Wireless Personal Area Networks that is the lower layers of OSI reference model. LR-WPANs have long battery life, low-cost, ease of installation, reliable data transfer and low-throughput features that communicates in short-range wirelessly [15].

There are three types of data rates at standard such as 250 kbps, 40 kbps, 20 kbps that can be operates in 2.4 GHz, 868 MHz and 915 MHz bands. 16 channels can be used in the 2.4 GHz ISM band, 10 channels in the 915 MHz band, and 1 channel in the 868 MHz band. The standard supports two addressing modes that are 16-bit short and 64-bit IEEE addressing and also two medium access mechanism which are CSMA-CA or ALOHA for contention-based access and TDMA for contention-free access [16]. These are some general features of the IEEE 802.15.4 standard and Figure 1 shows the superframe structure.

Fig. 1 IEEE 802.15.4 superframe structure

There are two modes in the IEEE 802.15.4 standard: beacon-enabled and nonbeacon-enabled. In nonbeacon-enabled mode, there is no synchronization within the network. Therefore only random access mechanism is active for medium access. In beacon-enabled mode, PAN coordinator transmits periodic beacons that contains information about the superframe structure [17]. After beacon, CSMA-CA or ALOHA mechanism is utilized in Contention Access Period (CAP) and TDMA mechanism in Contention Free Period (CFP). Guaranteed time slots (GTSs) are allocated to devices for access the channel with low-latency or specific data bandwidth [15]. During the inactive period (IP) nodes enter sleep mode for energy efficiency. Limited number of (only 7) slots and absence of priority mechanism are constraints of GTS allocations [18].

III. CHAOTIC SYSTEM

Recently, modern and strong cryptographic algorithms are predicted that can be solved a certain time. Concerning studies of encryption, some researchers emphasized that unlike standard encryption methods, between chaos and cryptography science is a strong relationship because of their special behavior of chaotic systems [19]. Chaotic systems have broadband, noise-like, difficult to predict and non-periodic feature. Chaotic signals, due to sensitive dependence on initial values and parameters [20], come to the fore in secure communication.

Keys required for encryption are produced separately for each bit with chaos maps. Sending data be encrypted with this keys that generated for each bit separately, using a non-linear equations. In the developed system, The resolution of the encoded data have made it more complicated on account of the use of a non-linear equation, and performing the encryption producing a separate key for each bit of data.

In this study, chaotic system was used to increase randomness in the generation of switches needed for coding. Chaos generators used in this coding is Logistic Map. Figure 2 exhibits bifurcation diagram of the Logistic Map. The value of r control parameter in the equation was 0-4. The r value must be between 3.5699 and 4 for the system to enter chaos.

\[ X_{n+1} = r \times X_n \times (1-X_n) \]  

X value in Equation 1 is n value and the system variable is the number of repetitions. The system will produce as many switches for coding as the bytes of data to be used in the application.

![Bifurcation diagram of logistic map](image)

IV. PERFORMANCE EVALUATION

The example networking scenario and its simulation have been realized using the OPNET Modeler software [17]. We used Open-ZB (open-source toolset) [18] for the IEEE 802.15.4 protocol and implemented chaotic-based encryption mechanism on this model. The performance assessment was presented according to energy consumption and end-to-end delay metrics under various traffic loads. In addition, the used parameters are given in Table I.

<table>
<thead>
<tr>
<th>TABLE I SIMULATION PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
</tr>
<tr>
<td>Data rate</td>
</tr>
<tr>
<td>Number of SNs</td>
</tr>
<tr>
<td>Frequency of nodes</td>
</tr>
<tr>
<td>Transmission power</td>
</tr>
<tr>
<td>Simulation time</td>
</tr>
<tr>
<td>Traffic</td>
</tr>
<tr>
<td>Area size</td>
</tr>
</tbody>
</table>

We create the scenario using OPNET Modeler that includes 10 nodes, 1 coordinator and analyzer module that collects the statistical data for network scenario. Figure 3 shows the example application scenario that gives us to performance of presented system.
Fig. 3 Simulation model of application using the OPNET modeler

Figure 4 shows the end-to-end delay for various rate of packet in chaotic-based encryption and non-encryption model. Average delay difference between models is 0.01618 ms approximately. Results are roughly equivalent for varied data rate as seen in Figure 4. As results, chaotic-based encryption model delay is reasonable.

Fig. 4 End-to-end delay between node1 and coordinator during simulation time

Figure 5 illustrates the consumed energy for various rate of packet with chaotic-based encryption and non-encryption model. Average energy consumption of chaotic-based encryption model is 0.52344 joule more than non-encryption model. The energy consumption result from encryption process are acceptable for LR-WPANs constraints.

Fig. 5 Consumed energy for node 1 during simulation time

V. CONCLUSION

In the presented work, a chaotic-based encryption security mechanism implemented to the IEEE 802.15.4. We have evaluated the system performance in a simulation environment using OPNET Modeler. End-to-end delay and consumed energy parameters are used to compare models. Most important outcome of the presented design is the results to be close to each chaotic-based encryption and non-encryption model.

ACKNOWLEDGMENT

This research work was supported by the Ministry of Science, Industry and Technology of Turkey under the contract SANTEZ 0200.STZ.2013-1 and Research Fund of the Sakarya University, Project Number: 2013-09-10-001.

REFERENCES


[21] OPNET Modeler, Opnet Technologies Inc.