ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
https://doi.org/10.17559/TV-20150728112744

ENHANCED SECURE DATA TRANSFER FOR WSN USING CHAOTIC-BASED ENCRYPTION

Cüneyt Bayılmış, Ünal Çavuşoğlu, Akif Akgül, Sezgin Kaçar, Abdullah Sevin

Original scientific paper

Processes on Wireless Sensor Networks (WSN) and their areas of use have become more widespread, and the issue of net-work security has appeared as one of the primary necessities. As power of the processor, memory and energy sources are limited on wireless sensor network nodes, traditional encryption structures are not found effective. With these criteria taken into consideration, the need for less process load and energy consumption as well as a powerful encryption is obvious. In this study, a chaotic encryption system to meet the security need on WSN using chaotic systems was carried out. The chaotic system developed here and the commonly used Skipjack encryption were compared with the help of algorithm OPNET Modeller software and better results were achieved.

Keywords: *chaotic based encryption; performance evaluation; WSN security*

Poboljšani sigurni prijenos podataka za WSN uporabom koda zasnovanog na kaosu

Izvorni znanstveni članak

Postupci na bežičnim senzorskim mrežama - Wireless Sensor Networks (WSN) i njihovim područjima uporabe sve su češći pa problem sigurnosti mreže postaje sve važniji. Budući da su snaga procesora, memorija i izvori energije ograničeni na čvorove bežičnih senzorskih mreža, tradicionalno strukturirani kodovi više nisu učinkoviti. Uzevši to u obzir, očita je potreba za manjim procesnim opterećenjem i potrošnjom energije te učinkovitim kodom. U ovom se radu razvija kaotični kodni sustav za zadovoljenje sigurnosnih potreba na WSN. Uspoređuju se ovdje razvijeni kaotični sustav i uobičajeno korišteni Skipjack kod uz pomoć algoritma OPNET Modeller softvera i konstatira se da su postignuti bolji rezultati.

Ključne riječi: *kod zasnovan na kaosu; vrednovanje performanse; WSN sigurnost*

1 Introduction

By an increased use of wireless sensor networks in recent years, maintenance of safe communication has become one of the most significant issues. This is especially crucial in military, medicine and security applications [1]. To provide security on wireless sensor networks, methods like key generation, encryption algorithms, security protocols, safe redirection and authentication are used [2, 3]. To ensure safe communication, studies on encryption algorithms have become prominent among other methods. Since traditional encryption methods have more complex structures and need much more process power, these methods cannot be employed in wireless sensor networks. Wireless sensor network nodes are generally devices with limited memory and process capacity [4]. That is why it is crucial that the communication protocols and security algorithms have low energy consumption and less process load.

The literature of the field contains many studies about safe communication on WSNs. These studies have included many different encryption algorithms. Among these studies, Skipjack algorithm used by high performance TinySEC [5] security protocol, which is widely approved, is taken as reference. Skipjack [6] algorithm is a block encryption method that uses symmetrical key structure. In this algorithm, 64-bit unencrypted data blocks and 80-bit encryption key are used and encrypted data is acquired after 32 cycles. Increasing the number of cycles also increases the level of security exponentially. Skipjack is a high level security algorithm that can be used for the encryption of every kind of data.

Another security protocol developed to be utilized on structures with low resources within WSNs is SPINS [7]. SPINS (security protocol for sensor networks) security protocol operates on two security blogs to meet the different security needs. One of them is SNEP (security network encryption protocol) and the other one is TESLA (microtime efficient stream loss-tolerant authentication). SNEP security blog meets the needs of confidentiality, integrity, data authentication and freshness. To maintain data security, SNEP makes use of RC5 [8] algorithm, a blog encryption algorithm. TESLA security blog provides authentication for broadcast messages.

Ren et al. developed an energy-efficient security protocol. On LLSP [9] (Link layer security protocol) security protocol, data security is ensured by dint of AES [10] symmetric blog encryption algorithm and CBC blog encryption approach. AES is a high security blog encryption algorithm. Bandırmalı and Ertürk [11] made use of SEA encryption algorithm on WSNSec security protocol which they developed for WSNs. SEA [12] encryption algorithm was modelled in OPNET Modeller environment and compared with TinySEC protocol in which skipjack algorithm is employed.

In addition to studies mentioned above, there are also studies with chaotic based encryption for safe communication. Bayılmış et al. [13] performed a chaotic encrypted application that can be used in the structure of low rate wireless personal area networks (LR-WPANs) (IEEE-802.15.4). Chaotic based encryption algorithm was modelled in OPNET Modeller environment and the comparison of encrypted and unencrypted data communications was presented in terms of end to end delay and energy consumption parameters. Liu et al. [14] developed a new chaotic blog encryption algorithm to be run on wireless sensor networks. The study includes a description of the chaotic blog encryption algorithm as well as the performance analyses. During the performance analyses, the developed structure was comparatively evaluated with RC5 [8] algorithms in terms of memory usage amount and energy consumption. Yang et al. [15]

performed an analysis of an encryption algorithm which was achieved with chaotic block encryption method.

In this paper, the security algorithm is developed more efficient than the works in literature. Security algorithm using chaotic systems was implemented on WSN to provide secure communication on WSN. It was simulated on OPNET Modeller simulator and then it was compared with Skipjack algorithm in which TinySEC protocol was used in ZigBee standards. Comparison was made on average end to end delay figures, energy consumption and memory usage rates.

The rest of paper is organized as follows: Section 2 includes information about chaotic map and system model which are used for encryption. Section 3 presents the simulation of the proposed security model and performance evaluation according to simulation results. The conclusion section presents assessments and comments on the recommended method.

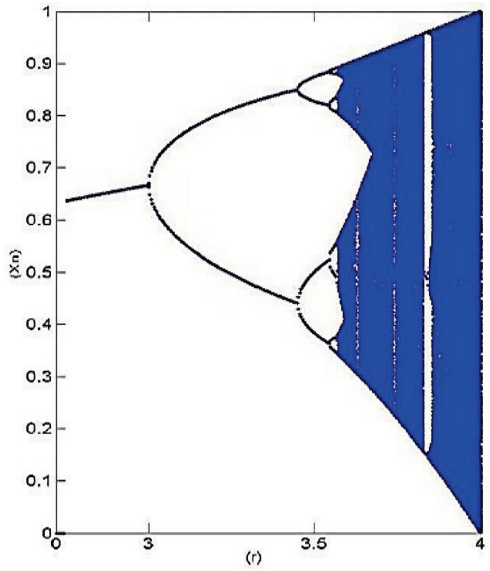

Figure 1 The logistic map branch diagram

2 The system model of chaotic based encryption

2.1 Chaotic map

There are many chaotic systems as discrete time and continuous time in the literature [16, 17]. Continuous systems can be divided into chaotic and hipper chaotic systems. For encryption application, in this paper is used discrete time chaotic system that is one dimensional logistic map, because it is basic and high encryption effective. Keys are obtained by Logistic map in encryption. For Logistic Map, bifurcation diagram is given in Fig. 1. In Eq. (1), the system parameter r was examined between 0÷4 values. As seen in Fig. 1, if the parameter r is between 0 and 3, the result is 1, if the parameter r is between 3 and 3,4, the result is 2. If the value r is around 3,5; 4 results are produced by chaotic system. And if the value r is less than 3,5699 and near the entering chaos the result is 8. As a result, bifurcation diagram in Fig. 1 shows that for r value must be chosen only 3,5699÷4 so that the system can enter chaos.

$$X[n+1] = r * X[n] * (1 - X[n]) \quad (1)$$

In equation, the parameter x is system variable and the value n is the number of iterations. In application, the number of data to be encrypted must be equal to the number of keys for encryption. Exemplarily, for 1000 bits original data there must be 1000 keys that are produced by chaotic system (Logistic Map).

2.1 Communication using chaotic encryption

Secure communication model of chaos based encryption algorithm is presented in Fig. 2. Data which are encrypted are transmitted with nonlinear function to communication channel. Then, data encrypted in the block diagram can be decrypted with the inverse of the function. In order to decrypt data encrypted in the application, one needs to know keys produced for each bit and the order of these keys, the chaotic system used, parameters in the chaotic system and initial values, and also non-linear equation and all parameters employed in this equation.

Algorithm 1 Chaos encryption algorithm pseudo code

Input $\leftarrow m, x1, fxm1$

Output $\rightarrow fxm$

for i = 1 to numsteps **do**

$fxm(i+1) = (2*(x(i))*(1+x(i)*m(i)+(1m(i)))+0.9)/4.8;$

if $i+1 <= numsteps$ **then**

$x(i+1) = R*fxm(i+1)*(1-fxm(i+1));$

end if

end for

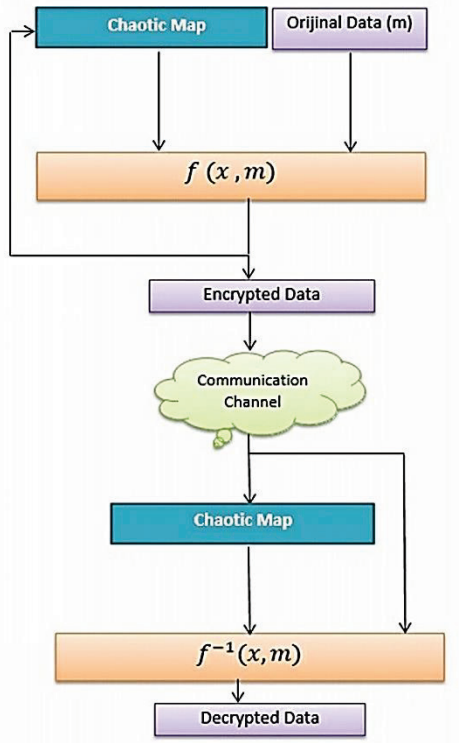

Figure 2 The system model of chaotic-based encryption block diagram

In improved application, for Logistic Map, pseudo code (Algorithm 1) structure is given in above for encryption. Keys are provided with chaos generator

(Logistic Map) in encryption. Also, a non-linear equation was used in order to increase security in encryption. Keys and original data are encrypted with nonlinear function in Eq. (2). x value in Eq. (2) represents the keys produced with chaos generators and m value represents the data to be encrypted in bits

$$2x\ (1 + xm + \ (1 - m)\ + \ 0{,}9)/4{,}8. \qquad (2)$$

3 Simulation result and discussion

Computer modelling and simulation experiments of an example of WSN application employing the chaotic encryption and Skipjack are performed using OPNET Modeller [18]. In the OPNET WSN simulation model, we used IEEE 802.15.4/ZigBee protocol developed by OPEN-ZB [19]. In addition, the example of WSN application scenario was simulated under various traffic loads. In this section, the effects of both chaotic-based encryption and Skipjack encryption algorithms were comparatively evaluated in terms of average end-to-end delay, energy consumption and memory usage. The used parameters in the simulation model are given in Tab. 1. Network traffic is generated using exponential distribution function. Also, the wireless networking environment is assumed to have a free space channel propagation model.

Table 1 Simulation Parameters

Parameters	Value
Data Rate	250 Kbps
Number of SNs	10 ÷ 100
Frequency of Nodes	2,4 GHz
Type of Sensor Nodes	MICAz
Transmission Power	1 mW
Battery	2 AA (1,5 V,2300 mAh)
Modulation	QPSK
Simulation Time	3600 s
Area Size	10 ÷ 10 m

3.1 Average end-to-end message delay

Effects of end-to-end message delay are discussed in terms of heavy network traffic and large scale application. Fig. 3 shows the ratios of the average end-to-end message delays of using chaotic-based encryption and Skipjack encryption applications under varying network load conditions.

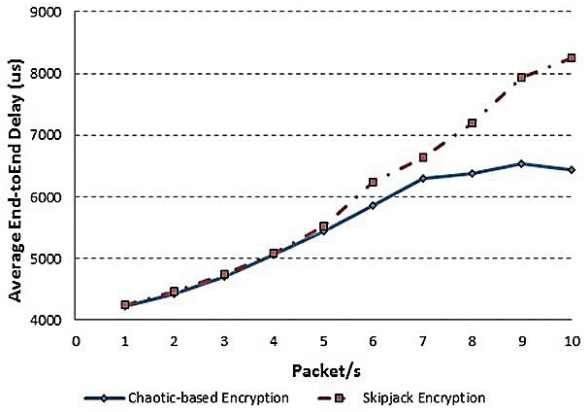

Figure 3 The average end to end message delay and packet number for the simulation model with chaotic based encryption and Skipjack algorithm

As seen in the figure, both encryption methods have approximately the same message delay values until 5 packet/s network load. However, chaotic-based encryption method has a lower latency ratio when number of the generated packet is more than 5 compared to Skipjack encryption. For example, the difference average end-to-end message delay between the two encryption algorithms is about 1500 us in 9 packet/s. As a result, chaotic-based encryption for WSN may be preferred in increasing networking loads instead of Skipjack algorithm.

One of the popular application areas of WNS is large scale applications. Therefore, we examined the effects of using chaotic-based encryption in large scale network in Fig. 4 which shows the ratios of the average end-to-end message delays of using chaotic-based encryption and Skipjack encryption applications as a function of varying number of the WSN nodes. Increasing the number of the WNS nodes from 10 to 100 nodes, the graphs show the proposed chaotic-based encryption gives better results according to Skipjack encryption. In the densest network, the end-to-end average message delay of WNS application using chaotic-based encryption is 6286 us while the average end-to-end message delay of WNS application using Skipjack encryption is 6416 us. Consequently, the chaotic-based encryption outperforms the Skipjack encryption in large scale network application.

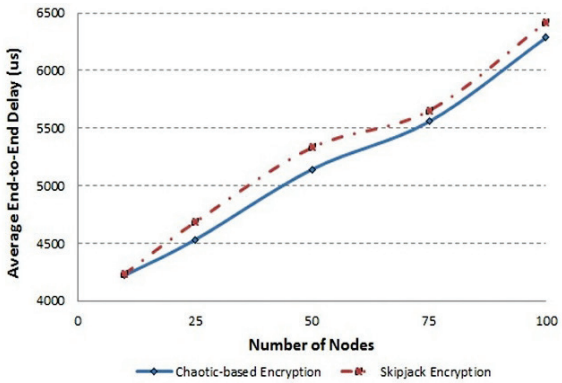

Figure 4 The average end to end message delay and number of nodes for the simulation model with chaotic based encryption and Skipjack algorithm

3.2 Energy consumption

One of the important performance metrics of WNS is energy consumption considering wireless sensor nodes having limited sources such as memory size, microprocessor capacity and battery etc. Energy consumption of the wireless sensor nodes is seen in Fig. 5, and Fig. 6 in terms of number of generated packets and number of sensor nodes respectively. As seen in Fig. 5 both encryption algorithms have close energy consumption rates under increasing network load conditions approximately. On the other hand, the chaotic-based encryption method leads to lower energy consumption compared to Skipjack encryption under increasing number of sensor nodes. It can be concluded from these results that using chaotic-based encryption may be preferred in large scale network application.

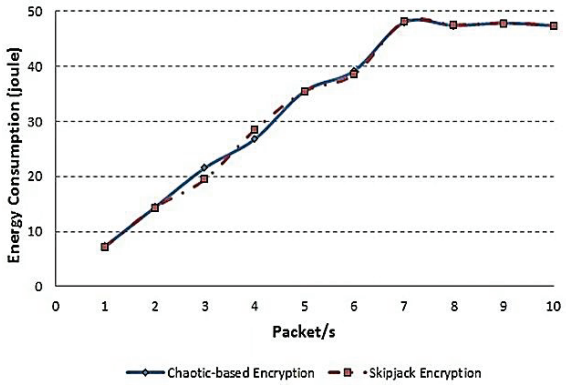

Figure 5 Energy consumption and packets number for the simulation model with chaotic based encryption and Skipjack algorithm

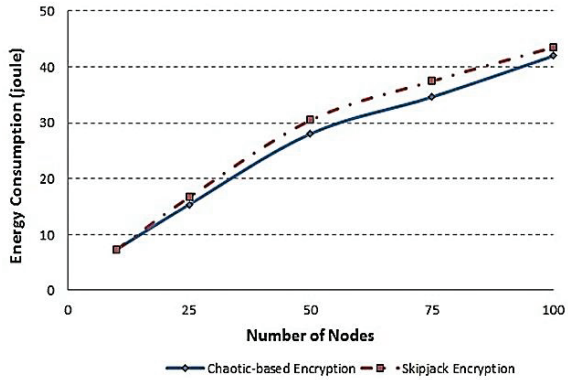

Figure 6 Energy consumption and number of nodes for the simulation model with chaotic based encryption and Skipjack algorithm

3.3 Data and code memory requirements

Another important performance metrics is data and code memory requirements. We used MICAz wireless nodes which include a 4 KB data memory, 128 KB code memory and 16 MHz ATMEGA 128L microcontroller in WSN application scenario. Accordingly, memory usage evaluation of chaotic based encryption and Skipjack encryption algorithms is used by AVRStudio5 software.

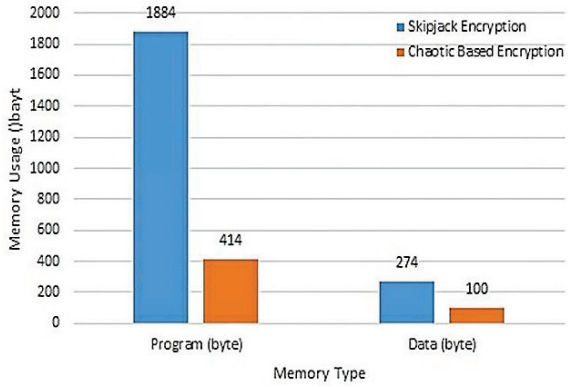

Figure 7 The program and data memory requirements of chaotic based encryption and Skipjack algorithm

Data and code memory usage of chaotic based encryption and Skipjack encryption algorithm is shown in Fig. 7. Chaotic encryption requires less in both data and code memory usage than Skipjack algorithm as seen in the figure. The code memory usage in the chaos based encryption is about four times lower than that of Skipjack algorithm and the data memory usage in the chaos based encryption is approximately three times lower than that of Skipjack algorithm.

4 Conclusion

Due to the nature of wireless communication, security on WSN is an issue of high sensitivity. Many protocols and algorithm designs have been developed on this issue. In this study, to maintain energy efficient secure communication on WSN, a chaotic-based security application was presented. The realization of the designed system was carried out on OPNET simulator and the success of chaotic-based encryption method was comparatively evaluated with Skipjack encryption used in ZigBee standards. Simulation results revealed that the chaotic-based encryption method has a lower average delay, program memory and data memory usage and on the other hand they have close energy consumption. In conclusion, chaotic-based encryption methods are appropriate to be used in WSNs.

5 Acknowledgments

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.

6 References

[1] Akyildiz, I. F.; Weilian, S.; Yogesh, S.; Erdal, C. Wireless sensor networks: a survey. // Computer networks. 4, 38(2002), pp. 393-422. https://doi.org/10.1016/S1389-1286(01)00302-4

[2] Sen, J. A survey on wireless sensor network security. // International Journal of Communication Networks and information security, (2010), pp. 59-82.

[3] Chen, X.; Kia, M.; Kang, Y.; Niki, P. Sensor network security: a survey. // Communications Surveys Tutorials, IEEE. 2, (2009), pp. 52-73. https://doi.org/10.1109/SURV.2009.090205

[4] Yick, J.; Biswanath, M.; Dipak, G. Wireless sensor network survey. // Computer networks. 52, 12(2008), pp. 2292-2330. https://doi.org/10.1016/j.comnet.2008.04.002

[5] Karlof, C.; Sastry, N.; Wagner, D. TinySec: A link layer security architecture for wireless sensor networks. // Proceedings of the 2nd international conference on Embedded networked sensor systems, ACM. (2004), pp. 162-175. https://doi.org/10.1145/1031495.1031515

[6] Brickell, E. F.; Denning, D. E.; Kent, S. T.; Maher, D. P.; Tuchman, W. SKIPJACK review, Interim Report: The Skipjack Algorithm, (1993).

[7] Perrig, A.; Szewczyk, R.; Tygar, J. D.; Wen, V.; Culler, D. E. SPINS: Security protocols for sensor networks. // Wireless networks. 8, 5(2001), pp. 521-534. DOI: 10.1023/A: 1016598314198

[8] Rivest, R. L. The RC5 Encryption Algorithm. // 1994 Leuven Workshop on Fast Software Encryption. (1994), pp. 86-96.

[9] Ren, J.; Tongtong, L.; Aslam, D. A power efficient link-layer security protocol (LLSP) for wireless sensor networks. // Military Communications Conference, MILCOM 2005, IEEE, (2005).

[10] Zhang, X.; Keshab, K. P. High-speed VLSI architectures for the AES algorithm. // Very Large Scale Integration (VLSI) Systems. 12, 9(2004), pp. 957-967. https://doi.org/10.1109/TVLSI.2004.832943
[11] Bandırmalı, N.; Ertürk, I. WSNSec: A scalable data link layer security protocol for WSN's. // Ad Hoc Networks. 10, 1(2012), pp. 37-45. https://doi.org/10.1016/j.adhoc.2011.04.013
[12] Standaert, F. X.; Piret, G.; Gershenfeld, N.; Quisquater, J. J. SEA: A scalable encryption algorithm for small embedded applications. // In Smart Card Research and Advanced Applications, Springer Berlin Heidelberg. (2006), pp. 222-236. https://doi.org/10.1007/11733447_16
[13] Bayilmis, C.; Cavusoglu, U.; Akgul, A.; Sevin, A.; Kacar, S. Employing Chaotic Encryption for IEEE 802.15.4-based LR-WPANs. // International Conference on Computer Science and Information Systems (ICSIS'2014), Oct 17-18, 2014, Dubai (UAE).
[14] Liu, Y.; Tian, S.; Hu, W.; Xing, C. Design and statistical analysis of a new chaotic block cipher for Wireless Sensor Networks. // Communications in Nonlinear Science and Numerical Simulation. 17, 8(2012), pp. 3267-3278. https://doi.org/10.1016/j.cnsns.2011.11.040
[15] Jiyun, Y.; Xiao, D.; Xiang, T. Cryptanalysis of a chaos block cipher for wireless sensor network. // Communications in Nonlinear Science and Numerical Simulation. 16, 2(2011), pp. 844-850. https://doi.org/10.1016/j.cnsns.2010.05.005
[16] Li, C.; Pehlivan, I.; Sprott, J. C.; Akgul, A. IEICE Electronics Express. 12, (2015), pp. 1-12
[17] Akgül, A.; Pehlivan, İ. A new three dimensional chaotic system without equilibrium points, its dynamical analysis. // Technical Gazette. 23, 1(2016), pp. 209-214. https://doi.org/10.17559/TV-20141212125942
[18] Web Page of OPNET Modeler - OpnetTechnologies Inc., URL:http://www.riverbed.com/products/performance-management-control/opnet.html
[19] Web Page of Open-ZB open-source toolset for the IEEE 802.15.4/ZigBee protocols, URL:http://www.open- zb.net

Authors' addresses

Cüneyt Bayılmış
Sakarya University
Faculty of Computer and Information Sciences
Esentepe Campus, 54187 Serdivan/Sakarya, Turkey
E-mail: cbayilmis@sakarya.edu.tr

Ünal Çavuşoğlu
Sakarya University
Faculty of Computer and Information Sciences
Esentepe Campus, 54187 Serdivan/Sakarya, Turkey
E-mail: unalc@sakarya.edu.tr

Akif Akgul
Sakarya University
Faculty of Technology
Esentepe Campus, 54187 Serdivan/Sakarya, Turkey
E-mail: aakgul@sakarya.edu.tr

Sezgin Kaçar
Sakarya University
Faculty of Technology
Esentepe Campus, 54187 Serdivan/Sakarya, Turkey
E-mail: skacar@sakarya.edu.tr

Abdullah Sevin
Sakarya University
Faculty of Computer and Information Sciences
Esentepe Campus, 54187 Serdivan/Sakarya, Turkey
E-mail: asevin@sakarya.edu.tr