ISSN: 0067-2904

Encryption Symmetric secret Key in Wireless Sensor Network Using AES Algorithm

Sahar Najah Hussein[1], Ali Hamzah Obaid[2], Ali Jabbar[3]
[1]*Department of Computer Science, College of Science for Women, University of Babylon, Hillah, Iraq*
[2]*Al-Furat Al-Awsat Technical University Technical Institute of Babylon*
[3] *Department of Software, College of Information Technology, University of Babylon, Hillah, Iraq.*

Received: 24/9/2021 Accepted: 2/3/2022 Published: 30/11/2022

Abstract

Wireless sensor network (WSN) security is an important component for protecting data from an attacker. For improving security, cryptography technologies are divided into two kinds: symmetric and asymmetric. Therefore, the implementation of protocols for generating a secret key takes a long time in comparison to the sensor's limitations, which decrease network throughput because they are based on an asymmetric method. The asymmetric algorithms are complex and decrease network throughput. In this paper, an encryption symmetric secret key in wireless sensor networks (WSN) is proposed. In this work, 24 experiments are proposed, which are encryption using the AES algorithm in the cases of 1 key, 10 keys, 25 keys, and 50 keys. In each experiment, two chains are combined by using a hash function (SHA-2) to produce secret keys. The Network Simulator Version 2 (NS2) was used to assess the network throughput for the generated key. The randomness of the suggested LWM method has been tested by using the Diehard statistical test and the Entropy test. The results of the tests show that the encryption secret keys have a high level of data randomness.

Keywords: NS2, WSN, Network throughput, Star Topology, Lightweight, SHA2.

مفتاح سري متماثل للتشفير في شبكة المستشعر اللاسلكية باستخدام خوارزمية AES

سحر نجاح حسين[1] ,علي حمزه عبيد[2] ,علي جبار[3]
[1] قسم علوم الحاسوب، كلية العلوم للبنات، جامعة بابل، الحلة، العراق.
[2]جامعة الفرات الاوسط التقنية – المعهد التقني بابل.
[3] قسم البرمجيات، كلية تكنولوجيا المعلومات، جامعة بابل، الحلة، العراق.

الخلاصة

يعد أمان شبكة المستشعرات اللاسلكية (WSN) مكونًا مهمًا لحماية البيانات من المهاجم. تقنيات التشفير، والتي تنقسم إلى نوعين من التشفير المتماثل وغير المتماثل لتحسين الأمان. لذلك، يستغرق تنفيذ البروتوكولات لإنشاء مفتاح سري وقتًا طويلاً مقارنةً بقيود المستشعر التي تقلل من إنتاجية الشبكة لأنها تستند إلى طريقة غير متماثلة. تعد الخوارزميات غير المتماثلة معقدة وتقلل من إنتاجية الشبكة. في هذا البحث، تم اقتراح المفتاح السري للتشفير المتماثل في شبكة المستشعرات اللاسلكية (WSN). في هذا العمل، تم اقتراح 24 تجربة، وهي تشفير باستعمال خوارزمية AES في حالات مفتاح واحد و10 مفاتيح و25 مفتاحًا و50

*Email: asssdali44@gmail.com

مفتاحًا. في كل تجربة، يتم الجمع بين سلسلتين باستعمال دالة تجزئة (SHA−2) لإنتاج مفاتيح سرية. تم استخدام Network Simulator الإصدار 2 (NS2) لتقييم معدل نقل الشبكة للمفتاح الذي تم إنشاؤه. تم اختبار عشوائية طريقة LWM المقترحة باستعمال اختبار Diehard الإحصائي واختبار Entropy. تظهر نتائج الاختبارات أن مفاتيح التشفير السرية تتمتع بمستوى عالٍ من عشوائية البيانات.

Introduction

Wireless sensor networks are built on the haphazard deployment of a large number of small, low-cost, and resource-constrained sensor nodes into or near the phenomenon to be monitored. The level of security provided by WSNs varies depending on the application. A military implementation, for example, is highly security-sensitive and a network breach may result in severe consequences such as the seepage of sensitive military information or the disablement of combat device systems, while habitat monitoring is a relatively benign application [1].

WSNs are used in battlefield control, security surveillance, health monitoring systems, physical environment monitoring, military applications, and other similar applications. These are made up of a large number of wireless sensor nodes with minimal sensing, processing, and transmission (radio) capabilities [2].

Network security refers to the provisions and policies placed in place by a network administrator to avoid and control unauthorized access, system modification, misuse, or denial of a computer network and its resources. Essentially, network protection is the authorization of data access on a network, which is managed by the network administrator [3].

The Network Simulator (Version 2) (NS2) is a simple, event-driven simulation tool that has effectively proven useful in studying the dynamic nature of communication networks. Both (wired and wireless network) services and protocols can be simulated by the NS2 network simulator (e.g., routing algorithms, TCP, UDP). In general, NS2 allows users to define network protocols and simulate their corresponding behaviors. NS2 is an open-source event-driven simulator designed primarily for research into computer communication networks. NS2 also includes modules for a wide range of network components, including routing, transport layer protocols, and applications. NS2 has evolved into the most popular open-source network simulator, as well as one of the most extensively used network simulators [4].

Therefore, the implementation of protocols for generating a secret key takes a long time in comparison to the sensor's limitations, and they decrease network throughput because they are based on an asymmetric method. The asymmetric algorithms are complex, and they decrease network throughput.

The objective of this research study is to improve the performance of the system through increasing network and node throughput by using light-weight methods (LWMs), which are implemented faster than asymmetric algorithms. The following is the rest of the paper: In Section 1, WSN is explained. Section 2 explains the related work. Section 3 explains the proposed work. Section 4 shows the research methodology. Section 5 shows the result. Section 6 concludes the paper.

Related work

The work related to researchers who work in this field: The authors in [5] proposed multiple key protocols (MKP) to produce a series of keys using the ECC algorithm. The multiple keys run in parallel, which ensures that the system's throughput and performance improve, resulting in shorter execution times and lower energy consumption. In [6], induced randomness is a new low-complexity method for rapidly generating secret keys in static situations. To generate high-rate shared randomness, use a simple approach in which legitimate participants inject locally generated randomness into the channel. To ensure that the keys generated by this methodology are indeed random, the NIST statistical test suite is used. [7] proposed a Secret Key Generation (SKG) protocol to extend the network lifetime while maintaining WSN security. The SKG protocol distributes a portion of the secret key among the network's sensor nodes while the remainder is kept on the WSN nodes. Each node in the network generates the secret keys using the two components. Using an NS2 network simulator, the protocol is examined, and the results suggest that the recommended SKG protocol can increase WSN performance while consuming less energy for key distribution. The proposed system has a higher network throughput than the researcher, and the results of the proposed system outperformed the results of the researcher when NS2 simulation was used as well as the researcher. In [8], it was proposed to generate a key chain from asymmetrical algorithms using the KCMA approach. These chains are created by combining two separate techniques with the hash functions SHA2 and XOR. The diehard test was used to evaluate the randomness of the secret key generated. The results showed that the randomness was increased by utilizing SHA2, indicating that the system was secret and secure. For the produced keys, the time was calculated in Java. In terms of security and time consumption, SHA2 was the best. The proposed system has higher randomness (more security) than the researcher, whose results outperformed those of the researcher. [9] proposed research into PHYSEC methods that use channel reciprocity to generate a secret key, often known as secret key generation (SKG) systems. Efforts were concentrated on developing a simple SKG scheme by omitting the information reconciliation stage to lower the high computational and communication costs, proposing a modified Kalman (MK) approach and combining it with multilevel quantization, i.e., coupled multilevel quantization (CMQ). The methodology generates a basic SKG method for its large boost in reciprocity, allowing two legitimate users to receive an identical secret key without going through the information reconciliation stage.

Proposed work

This study proposes an encryption symmetric secret key in wireless sensor networks (WSN) to improve a security system. The data is encrypted using the generated secret keys and network throughput in the simulator NS2 environment to improve network performance, which is used in six experiments based on the TEA, XTEA, and RC5 algorithms. The work creates the generated secret keys in each experiment. To produce the secret keys, the two algorithms are merged using the SHA-2 function.

Lightweight cryptography (XTEA, TEA, and RC5) is more effectively used, requiring fewer resources and providing high productivity, conservatism, and low energy consumption.

The randomness of the secret keys generated from the six experiments is tested by using a Diehard test and an entropy test. The Diehard test is used for evaluating the randomness of the ciphertexts. The NS2 simulator is used to simulate transferring and receiving data in a simulated WSN. The security strength of the proposed LWM scheme is heavily dependent on randomness. The proposed LWM scheme should satisfy confidentiality.

The proposed system is designed in three phases. They are hand shaking, key generating, and data transferring. During the hand-shaking phase, the sender and receiver agree on critical information about the secret key generation. In the hand shaking phase, the information is encrypted using a public-key cryptosystem.

In the second phase (key generating), a chain of the secret key should be generated. The secret key number is determined through the hand shaking phase between the sender and receiver. The key generating phase includes implementing a set of functions to compute the secret key.

The third phase is data transfer. It is the last phase. The data is encrypted before being sent to the sender's side, and it is decrypted on the receiver's side. The generated keys in the previous phase (key generating) are used for ciphering and deciphering. The AES algorithm is based on WSN for data confidentiality, as shown in Figure 1.

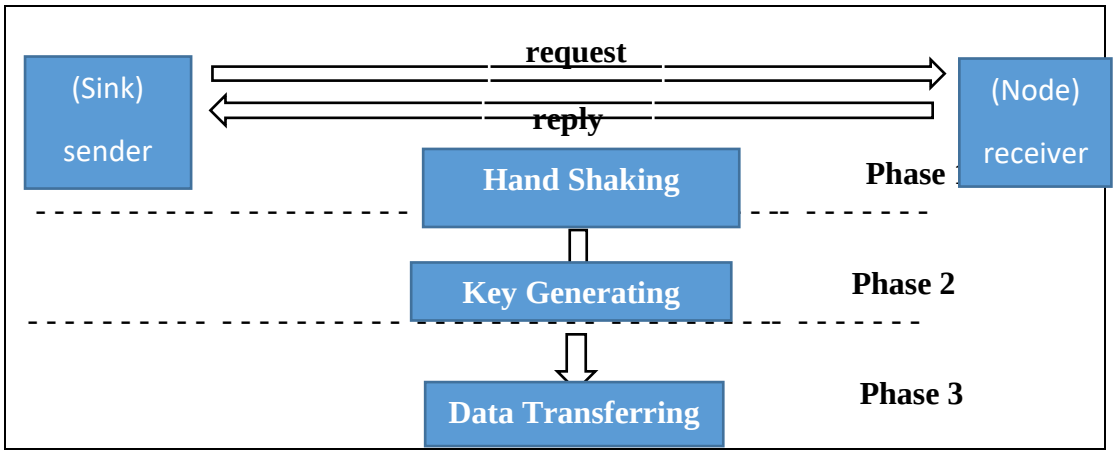

Figure 1: The Proposed System Design.

Research Methodology

This section shows how to evaluate the proposed LWM scheme using some main metrics through tests.

Network Throughput test

An NS2 simulator has been used to measure the network throughput by the proposed LWM method. A code to simulate a WSN with fifteen nodes has been implemented. A code to simulate a WSN with fifteen nodes has been implemented. The NS2 environment simulated building a small WSN with fifteen sensor nodes distributed in a star topology around a coordinator node. The NS2 environment simulated transferring thirty groups of packets at different data rates. The operation of transferring data packets is repeated thirty times for each data rate. An average of thirty transfer operations is calculated for each data rate. Network throughput is a significant metric for measuring network performance. Network throughput is the amount of data transmitted in a given amount of time. The rate of data transmission in the network across simulation time is referred to as node throughput. The rate of all nodes' throughput is divided by the number of nodes in the network throughput [10].

Result

Randomness test

This section shows the results of ciphertext randomness.

Ciphertext Randomness Result

Using 1 key, the RC5 & RC5 algorithms in data encryption result in significantly higher

safe values and are considered the most powerful ones in terms of security. The XTEA & XTEA algorithms result in significantly lower safe values. The TEARC5 algorithm results in significantly higher doubt values. The XTEA & XTEA algorithms result in significantly lower doubt values. The XTEA & XTEA algorithms result in significantly higher failure values, while the TEARC5 algorithm results in significantly lower failure values.

Using 10 keys, the XTEATEA algorithm results in significantly higher safe values and is considered the most powerful one in terms of security, while the RC5 & RC5 algorithms result in significantly lower safe values. The RC5&RC5 algorithms result in significantly higher doubt values, while the XTEA & XTEA and XTEARC5 algorithms result in significantly lower doubt values. The TEA&TEA algorithm results in significantly higher failure values, while the XTEATEA algorithm results in significantly lower failure values.

Using 25 keys, the XTEA & XTEA algorithms result in significantly higher safe values and are considered the most powerful ones in terms of security, while the RC5 & RC5 algorithms result in significantly lower safe values. The XTEARC5 algorithm results in significantly higher doubt values, while the TEA & TEA algorithms result in significantly lower doubt values. The TEA & TEA algorithms result in significantly higher failure values, while the XTEARC5 algorithm results in significantly lower failure values.

Using 50 keys, the TEARC5 algorithm results in significantly higher safe values and is considered the most powerful one in terms of security, while the TEA & TEA algorithms result in significantly lower safe values. The XTEARC5 algorithm results in significantly higher doubt values than the TEARC5 algorithm, which results in significantly lower doubt values. The XTEA & XTEA algorithms result in significantly higher failure values, while the XTEATEA algorithm results in significantly lower failure values, as shown in Figure 2.

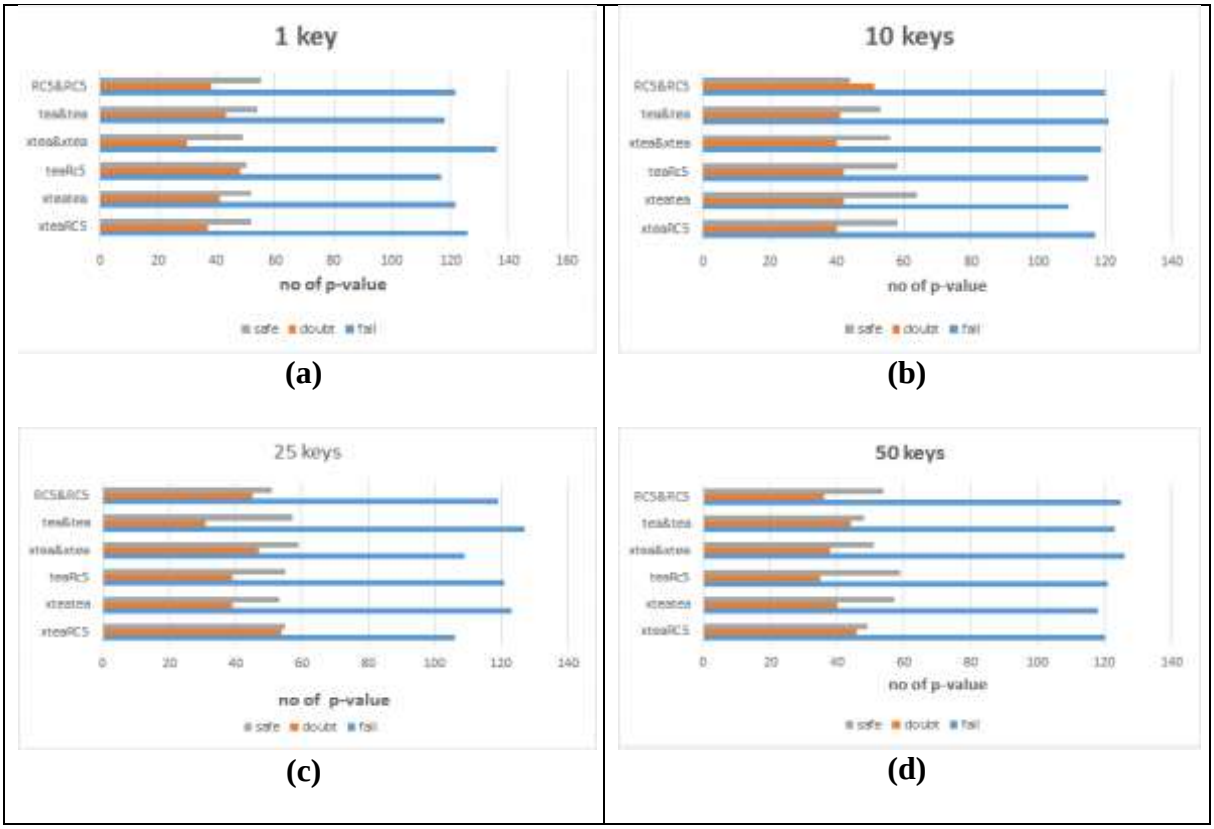

Figure 2: The p-values of ciphertext Randomness Test

Entropy test

Table 1 illustrates the ciphertext's entropy result. These results are extremely close to the ideal entropy value of 8, indicating that the suggested algorithm is resistant to entropy attacks.

Table 1: Entropy of the Ciphertext based with multiple keys

Entropy	1Key	10 keys	25 keys	50 Keys
XTEATEA	7.999980020873702	7.999982818112229	7.999982831057734	**7.999980792201126**
XTEARC5	7.999984956161785	7.999984416917465	7.999982333271195	**7.999983475096004**
TEARC5	7.999984627855257	7.999983498584925	7.999981848598848	**7.999983622801022**
XTEA&XTEA	7.999984044139211	7.999980870819826	7.999979735518554	**7.999981947330041**
TEA&TEA	7.999983839094575	7.999978439566082	7.999981016322970	**7.999984882244313**
RC5&RC5	7.999982988126686	7.999981153032624	7.999981999404382	**7.999983584675538**

Throughput Test

To assess network throughput in five scenarios where the number of keys is "100, 200, 300, 400, 500."The graph demonstrates that as the number of keys increases, network throughput decreases. As a result, the key number "500" had less network throughput than the key number "100." As illustrated in Figures 3, 4, 5, 6, 7, and 8,

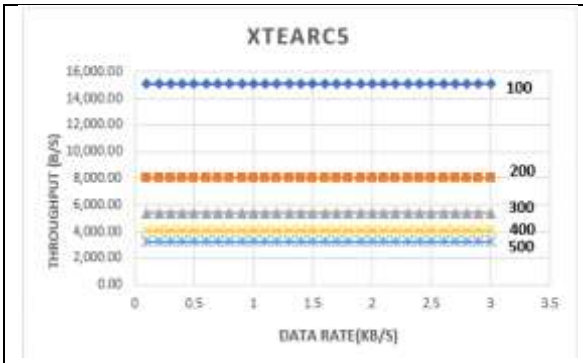

Figure 3: Network Throughput of the XTEARC5

Figure 4: Network Throughput of the XTEATEA

Figure 5: Network Throughput of the TEARC5

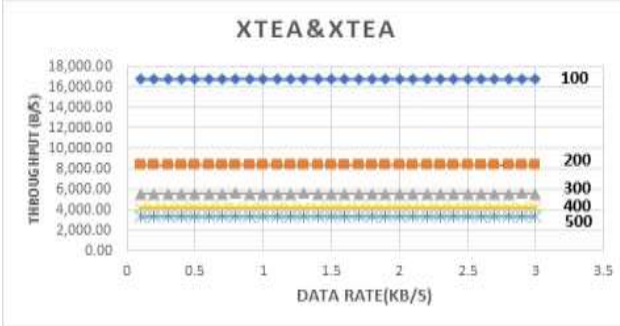

Figure 6: Network Throughput of the XTEA&XTEA

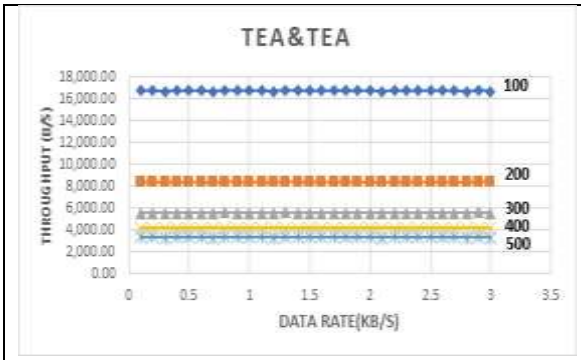

Figure 7: Network Throughput of the TEA&TEA

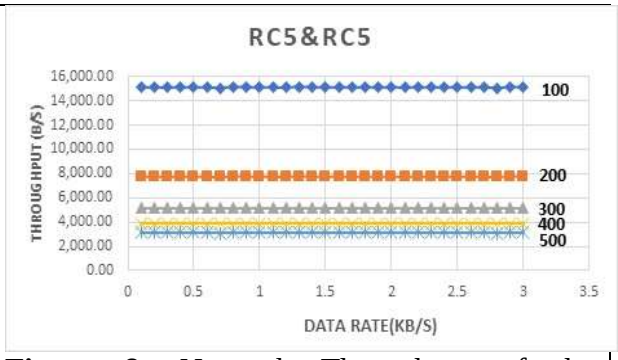

Figure 8: Network Throughput of the RC5&RC5

To measure network throughput, Based on the LWM Method in six experiments with a case number of keys of 100, the chart shows that network throughput is increased in XTEARC5 and XTEA&XTEA and network throughput is decreased in XTEATEA, as illustrated in Figure 9.

To measure network throughput, Based on the LWM Method in six experiments in case number of the keys of 200, the chart shows that network throughput is increased in XTEATEA and network throughput is decreased in RC5&RC5, as illustrated in Figure 10.

To measure network throughput, Based on the LWM Method in six experiments in the case number of the keys of 300, the chart shows that network throughput is increased in XTEATEA and network throughput is decreased in RC5&RC5, as illustrated in Figure 11.

To measure network throughput, Based on the LWM Method in six experiments in the case number of the keys of 400, the chart shows that network throughput is increased in XTEATEA and network throughput is decreased in RC5&RC5, as illustrated in Figure 12.

To measure network throughput, Based on the LWM Method in six experiments in the case number of the keys of 500, the chart shows that network throughput is increased in XTEA&XTEA and network throughput is decreased in RC5&RC5, as illustrated in Figure 13.

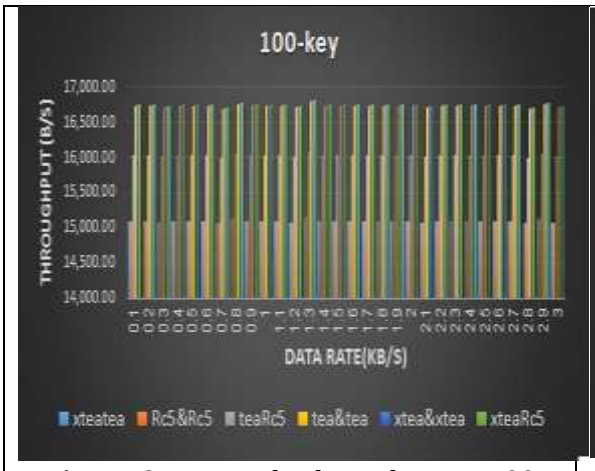

Figure 9: Network Throughput in 100 keys based on the LWM Methods

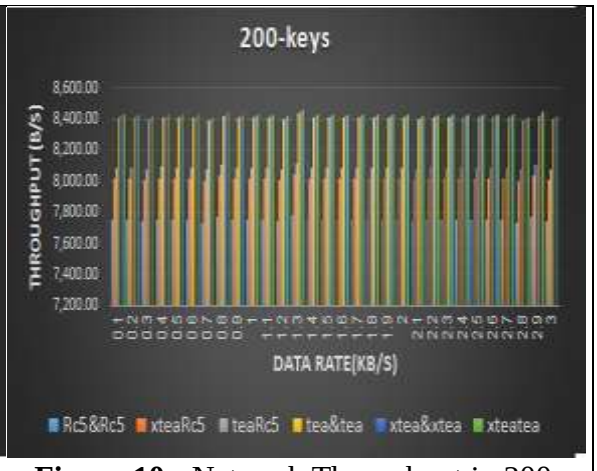

Figure 10: Network Throughput in 200 keys based on the LWM Methods

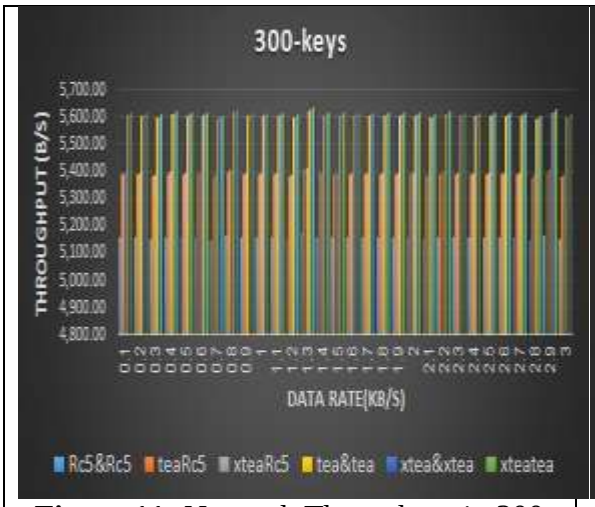

Figure 11: Network Throughput in 300 keys based on the LWM Methods

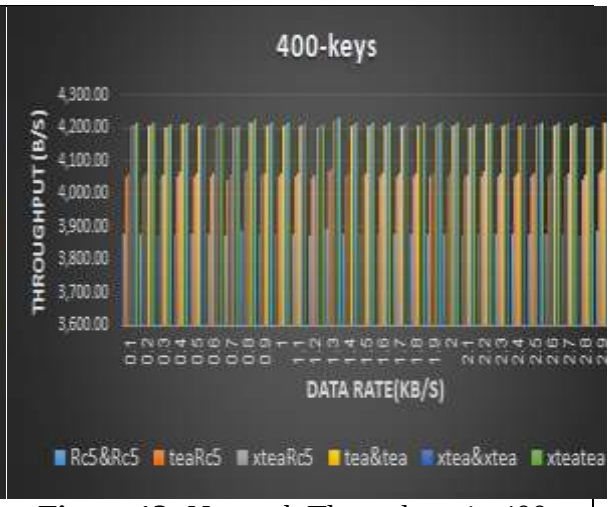

Figure 12: Network Throughput in 400 keys based on the LWM Methods

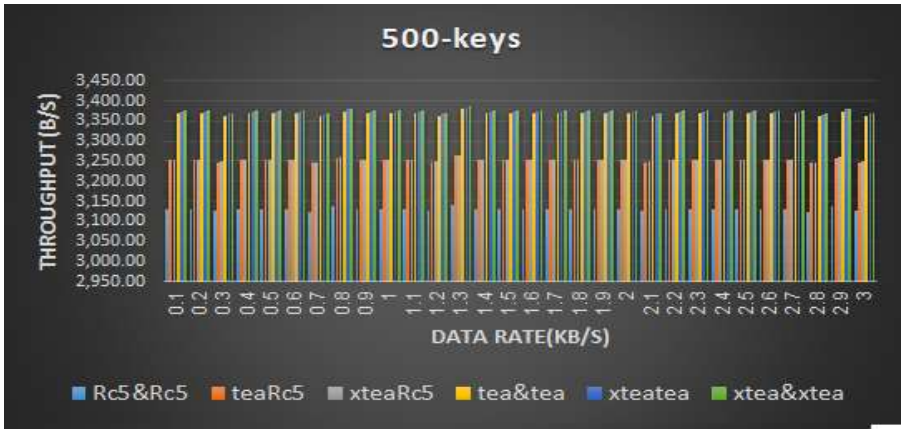

Figure 13: Network Throughput in 500 keys based on the LWM Methods

To measure network throughput, based on the LWM Method in six experiments and each experiment in case number of the keys (100,200,300,400,500), the chart shows that network throughput is best in the XTEATEA experiment, and worst in the RC5&RC5 experiment, and between the best and the worst is the TEA& TEA and TEARC5 experiments, as illustrated in Figure 14.

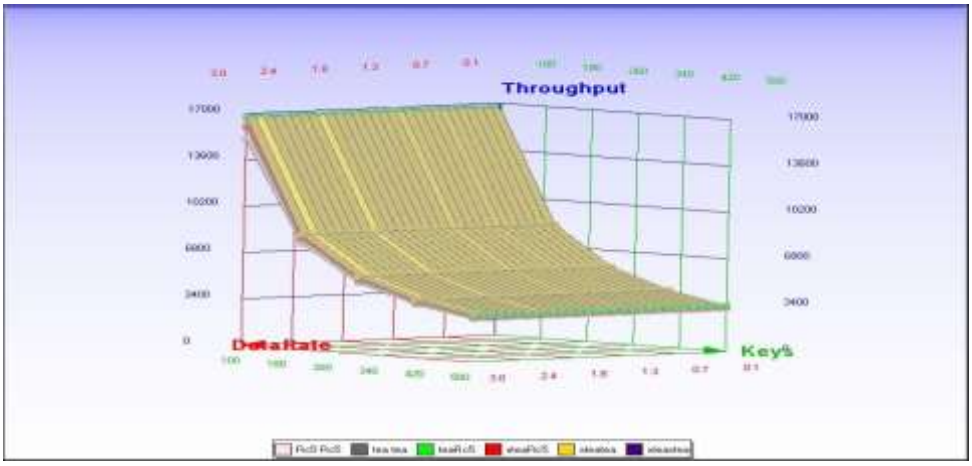

Figure 14: Network Throughput of the LWM Methods

Conclusion

Improving WSN system performance by increasing network throughput, the NS2 simulator is used to simulate transferring and receiving data in simulated WSN.AES algorithm in encryption leads to an increase in the data security level because it increases the randomness of the ciphertext. Using 1 key, the highest entropy is the XTEARC5 algorithm, and the lowest entropy is the XTEATEA algorithm. Using 10 keys, the XTEARC5 algorithm has the highest entropy, and the TEA&TEA algorithm has the lowest. Using 25 keys, the XTEATEA algorithm has the highest entropy, and the XTEA-XTEA algorithm has the lowest. Using 50 keys, the highest entropy is the TEA & TEA algorithm, and the XTEATEA algorithm has the lowest. Using the SHA-2 function boosted the system's security while also increasing network throughput. As the number of keys decreases, network throughput increases; as the number of keys increases, network throughput decreases; therefore, network throughput is inversely related to security.

References

[1] Sun, F., Zhao, Z., Fang, Z., Du, L., Xu, Z., & Chen, D., "A review of attacks and security protocols for wireless sensor networks," *Journal of Networks*, vol. 9, no. 5,pp. 1103, 2014.

[2] Janardhan, N. and K. Nandhini , "Wireless Sensor and Actuator Networks (WSANs): Insights and Scope of Research," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11, pp.1607-1615,2019.

[3] Pawar, M. V. and J. Anuradha, "Network security and types of attacks in network," *Procedia Computer Science*, vol. 48, pp.503-506, 2015.

[4] Nayak, A. K., Rai, S. C., & Mall, R., "*Computer Network simulation using NS2*," *CRC Press*, 2016.

[5] Al-Alak, S., Zukarnain, Z., Abdullah, A., & Subramiam, S., "Randomness improvement of AES using MKP," *Research Journal of Information Technology*, vol. 5,pp. 24-34, 2013.

[6] Aldaghri, N. and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692-2705, 2020.

[7] Bashaa, M. H., Al-Alak, S. M., & Idrees, A. K., "Secret key generation in wireless sensor network using public key encryption," *Paper presented at the Proceedings of the international conference on information and communication technology*, 2019.

[8] Obaid, A. H., & Obayes Al-Husseini, K. A., "Study the impact of electronic tests using Moodle program on student achievement," In *CEUR Workshop Proceedings*, vol. 2475, pp. 232–240. CEUR-WS, 2019.

[9] Hamza, A. H. and S. M. K. Al-Alak, "Evaluation key generator of Multiple Asymmetric methods in Wireless Sensor Network (WSNs)," *Journal of Physics: Conference Series, IOP Publishing*, 2021.

[10] Al-Husseini, K.A.O., Obaid, Ali. H., "Interaction between project tasks and risk management tasks in software development," *Periodicals of Engineering and Natural Sciences this link is disabled*, vol. 8, no. 4, pp. 2300–2308, 2021.

[11] Yuliana, M., "A simple secret key generation by using a combination of pre-processing method with a multilevel quantization," *Entropy*, vol.21, no. 2, pp.192, 2019.

[12] Rao, V. P., "The simulative investigation of Zigbee/IEEE 802.15. 4," *Dresden University of Technology*, 2005.

[13] Sahar Najah Hussein and Saif Mahmood Al-Alak, "Secret Keys Extraction Using Light Weight Schemes for Data Ciphering," *J. Phys.: Conf. Ser.*, 1999 012114, 2021.