Computers, Materials & Continua
DOI: 10.32604/cmc.2022.028520
Article

Tech Science Press

ESSD: Energy Saving and Securing Data Algorithm for WSNs Security

Manar M. Aldaseen[1], Khaled M. Matrouk[1], Laiali H. Almazaydeh[2,*] and Khaled M. Elleithy[3]

[1]Computer Engineering Department, Al-Hussein Bin Talal University, Ma'an, Jordan
[2]Software Engineering Department, Al-Hussein Bin Talal University, Ma'an, Jordan
[3]Computer Science and Engineering Department, University of Bridgeport, CT, Bridgeport, USA
*Corresponding Author: Laiali H. Almazaydeh. Email: laiali.almazaydeh@ahu.edu.jo
Received: 11 February 2022; Accepted: 17 April 2022

Abstract: The Wireless Sensor Networks (WSNs) are characterized by their widespread deployment due to low cost, but the WSNs are vulnerable to various types of attacks. To defend against the attacks, an effective security solution is required. However, the limits of these networks' battery-based energy to the sensor are the most critical impediments to selecting cryptographic techniques. Consequently, finding a suitable algorithm that achieves the least energy consumption in data encryption and decryption and providing a highly protected system for data remains the fundamental problem. In this research, the main objective is to obtain data security during transmission by proposing a robust and low-power encryption algorithm, in addition, to examining security algorithms such as ECC and MD5 based on previous studies. In this research, the Energy Saving and Securing Data algorithm (ESSD) algorithm is introduced, which provides the Message Digest 5 (MD5) computation simplicity by modifying the Elliptic Curve Cryptography (ECC) under the primary condition of power consumption. These three algorithms, ECC, MD5, and ESSD, are applied to Low Energy Adaptive Clustering Hierarchy (LEACH) and Threshold-sensitive Energy Efficient Sensor Network Protocol (TEEN) hierarchical routing algorithms which are considered the most widely used in WSNs. The results of security methods under the LEACH protocol show that all nodes are dead at 456, 496, and 496, respectively, to ECC, MD5, and ESSD. The results of security methods under the TEEN protocol show that the test ends at 3743, 4815, and 4889, respectively, to ECC, MD5, and ESSD. Based on these results, the ESSD outperforms better in terms of increased security and less power consumption. In addition, it is advantageous when applied to TEEN protocol.

Keywords: Cryptography; ECC; energy consumption; ESSD; LEACH; MD5; RSA; TEEN; WSNs

1 Introduction

Wireless Sensor Networks (WSNs) comprise hundreds or even a considerable number of tiny devices, each with detecting, handling, and correspondence abilities to screen present reality conditions. They have various applications with vastly varying sensing interactions with the environment. These applications range from basic military reconnaissance to woodland fire checking and climate observing sooner than later [1].

Sensor networks may consist of many different resource-constrained nodes (i.e., hardware, visual, infrared, radar, etc.). These nodes have restricted preparing ability, low stockpiling limit, obliged correspondence data transfer capacity, constrained vitality, and physical size of the sensor hubs. Because of these limitations, it is hard to utilize the customary security systems in WSNs. To upgrade the customary security calculations for WSNs, it is essential to know about the requirements of sensor hubs [2].

Notwithstanding customary security issues like secure directing and secure information collection, security instruments conveyed in WSNs likewise ought to include coordinated efforts among the hubs because of the decentralized idea of the systems and the nonappearance of any framework.

In the genuine universe of WSNs, the sensor hubs cannot be thought to be a reliable convent. The analysts in WSNs security have, in this way, centered around building a sensor trust strategy to tackle the issues which are past the capacities of conventional cryptographic systems. Since, as a rule, the sensor hubs are unattended and indeed shaky, weakness to physical assault is a significant issue in WSNs. Various recommendations exist in the literature for protection against a physical assault on sensor hubs. Structure and usage of secure WSNs is, in this manner, an especially testing task. Since these systems are typically conveyed in remote places and left unattended, they ought to be outfitted with security components to safeguard against assaults [3].

WSNs are vulnerable to various types of attacks. These attacks can be broadly categorized as follows [4]:

1) **Attacks on privacy and authentication**: standard cryptographic procedures can ensure the mystery and legitimacy of correspondence channels from pariah assaults, for example, spying, parcel replay assaults, and change or parodying of bundles.

2) **Attacks on network availability**: are regularly alluded to as DoS assaults. A secretive assault against administration: in a subtle assault, the aggressor's objective is to cause the system to acknowledge bogus information esteem. For instance, an assailant bargains a sensor hub and infuses bogus information esteem through that sensor hub.

Several algorithms were used to address the problem of information security in the WSNs [5,6]. These algorithms did not consider the amount of energy consumption in the sensor nodes. Energy is the most significant requirement for WSNs. Energy utilization in sensor hubs can be arranged in three sections: (I) Energy for the sensor transducer, (II) Energy for correspondence among sensor hubs, and (III) vitality for chip calculation. Accordingly, correspondence is costlier than calculation in WSNs [7]. Any message extension brought about by security components comes at a considerable expense. Consequently, finding the right algorithm that achieves the least energy consumption in data encryption and decryption and providing a highly protected system for data remains the key problem.

In this paper, the proposed algorithm provides a robust security technique and, at the same time, reduces the amount of energy consumption in the sensor nodes, which increases the lifetime of the wireless sensor network.

In this paper, the main contribution can be summarized as follows:

- Improving the selection of keys of the encryption algorithm.
- Improving the lifetime of the sensor.
- Implementing a light-weight algorithm and at the same time, it should properly protect sensed data.
- Mapping the results with other studies under identical conditions in the WSNs area.

This paper is organized as follows: Section 2 offers the related research. Section 3 describes the proposed methodology. Section 4 demonstrates the experimental results and evaluation. Section 5 summarizes how the research objectives are being achieved and future works.

2 Related Works

2.1 Cryptography

WSNs are vulnerable to various types of attacks. These attacks can be broadly categorized. That lead to cryptography, a security system utilized to ensure WSNs against external attacks. It guarantees numerous security administrations, including integrity and verification by checking the information parcel source and its substance using cryptographic algorithms, which can be categorized into three classes, symmetric-key algorithms, asymmetric-key algorithms, and hash functions [8,9].

Knowledge about cryptography and its unique customization with WSNs case studies will provide the research community with the latest updates in cryptographic techniques and bring a new perspective to security, power consumption, and many other areas of high importance in WSNs [10].

It is difficult decision to decide which cryptographic techniques should be used, how often they are used, and which network performance metrics are used to evaluate the design and security analysis. The first choice may be, "when does one use symmetric cryptography, and when does one use asymmetric cryptography?"

Symmetric encryption is also called single-key cryptography. In this encryption process, the receiver and the sender have to agree upon a single secret (shared) key. Given a message (plain text) and the key, encryption produces one intelligible data, about the same length as the plain text. Decryption is the reverse of encryption and uses the same key as encryption [11]. On the other hand, asymmetric encryption is also called public-key cryptography. It uses two keys: a public key, which is known to the public, used for encryption, and a private key, which is known only to the user of that key, used for decryption. The public and private keys are related by any mathematical means. In other words, data encrypted by one public key can be encrypted only by its corresponding private key [12].

The main distinguishing feature of asymmetric encryption is that it allows the establishment of secure communication between individuals without the requirement of a previously shared a single cryptographic key. Asymmetric cryptography came up with a radical change of paradigms [13]. In [14] Alshammari and Elleithy proposed a protocol that utilizes the existing cryptographic primitives and leverages asymmetric encryption to achieve key distribution and node authentication in one step and using only one frame to avoid communication overhead.

Two popular asymmetric schemes are Rivest-Shamir-Adleman (RSA) [15] and Elliptic Curve Cryptography (ECC) [16,17]. It is widely admitted that RSA is computationally intensive and usually executes thousands or even millions of multiplication instructions to perform a single-security operation [18]. Further, a microprocessor's public key algorithm efficiency is primarily determined by the number of clock cycles required for multiplication instruction [19]. At [20], they found that public

key algorithms such as RSA usually require on the order of tens of seconds and up to minutes to perform encryption and decryption operations in resource-constrained wireless devices, which exposes a vulnerability to the attacks.

In [21], they quantified the energy cost of authentication and key exchange based on public-key cryptography, RSA, and ECC on an 8-bit microcontroller platform. A comparison has been presented on two public-key algorithms, RSA and ECC, considering mutual authentication between two parties. The result shows that even software-based public key cryptography is feasible for an 8-bit microcontroller platform. Moreover, ECC shows significantly better results than RSA in terms of reduced computation time and the amount of data that needs to be stored and transmitted. Consequently, ECC requires less energy than RSA [8,21,22]. Further, the ECC-based key exchange protocol outperforms the RSA-based key exchange protocol on the server-side, and there is almost no difference in the energy cost for these two key exchange protocols on the client-side [23]. In addition, the relative performance advantage of ECC over RSA increases as the key size increases.

Anderson et al. questioned if "you can show that asymmetric encryption is feasible in sensor networks at a certain level of cost, it becomes possible to invent new security protocols or adapt existing ones for sensor networks" [24].

For the above reasons, in this research we adopted security algorithms that are more energy-efficient and have fewer processing operations possible to maintain the sensor's life, such as ECC as asymmetric algorithm and Message Digest 5 (MD5) as hash algorithm. In addition, we propose Energy Saving and Securing Data algorithm (ESSD) and then apply ECC, MD5, and ESSD to LEACH and TEEN routing algorithms, which are considered the most widely used in WSNs.

A quick overview of both ECC algorithm and MD5 algorithms in the following:

2.1.1 ECC

According to the designers of the ECC, an EC is a plane curve defined by an elliptic curve, which is the set of points that satisfy a specific mathematical equation [25]. The equation for an elliptic curve is:

$$y^2 = x^3 + ax + b \tag{1}$$

Where (x,y,a,b) $\in$R Λ (a,b) $\neq$ 0,

R: a real number field,

The constants (a and b) control the shape of the ECC graph and any change in any of these numbers changes the scheme too.

Equations based on elliptic curves have a characteristic that is very valuable for cryptography purposes: they are relatively easy to perform, and extremely difficult to reverse.

ECC has two main advantages [26]: (1) ECC public keys are smaller for the same level of security as RSA solutions, thus reducing the number of bits that need to be exchanged; and (2) ECC public-key operations require fewer computations than conventional public-key methods.

2.1.2 MD5

It was developed by Rivest [27] for providing data integrity. It is a widely used cryptographic hash function processing a variable-length message into a fixed-length output of 128 bits.

2.2 Hierarchical Routing Protocols (HRP)

In WSNs, the energy consumption is one of the most critical issues. The traditional routing protocols for WSN may not be optimal in energy consumption [28]. HRPs are more energy-efficient than other protocols [29]. HRP follows the clustering mechanisms; clustering techniques can be efficient in energy and scalability [30]. By using a clustering technique, they greatly minimize the consumption of energy in collecting and disseminating (fusion and aggregation) data. HRP minimizes energy consumption by dividing nodes into different clusters. In each cluster, higher energy nodes, i.e., the Cluster Heads (CHs), can process and send the information to the Base Station (BS). In contrast, low energy nodes, i.e., the cluster members, can be used to perform the sensing in the proximity of the target and send it to its CH. This means that the creation of clusters and assigning particular tasks to CH can significantly contribute to overall system scalability, lifetime, and energy efficiency, reducing the size of the routing table by localizing the route setup within the clusters and conserving the communication bandwidth of the network [31–33].

A quick overview of both LEACH and TEEN routing algorithms in the following:

2.2.1 LEACH

It is the most popular energy-efficient hierarchical routing algorithm proposed by Heinzelman et al. [34] for WSNs to reduce power consumption.

In LEACH, direct communication is used by each CH to forward the data to the BS. LEACH divides the network into several clusters. Since energy dissipation of the sensor depends on the distance, LEACH attempts to transmit data over short distances and reduce the total number of transmission and reception operations [35].

2.2.2 TEEN

It is a hierarchical routing protocol proposed in [36] for time-critical applications, where the sensor nodes sense the medium continuously, but the data transmission is done less frequently.

In TEEN, the CH sends aggregated data to higher-level CH until the data reaches the base. Thus, the sensor network architecture in TEEN is based on a hierarchical grouping where closer nodes form clusters, and this process goes on to the second level until the BS (base) is reached.

3 Materials and Methods

In this paper, the main objective is to achieve data security during transmission by proposing strong, low-power encryption algorithm and mapping the results with (MD5 and ECC) based on previous studies. All then will be applied to two of the most used protocol types (TEEN and LEACH) protocols in wireless networks.

3.1 Proposed Algorithm (ESSD)

Our proposed Energy Saving and Securing Data algorithm (ESSD) is designed to generate a set of encryption key numbers. It starts with points, Ax, Bx, Cx on the ECC curve and P prime number, then takes the start points' integer part. In order to generate the rest of the sequence using the sum of all points modulo (P) and stop the sequence at the index (3P), the last step is to remove the repetition of numbers. Finally, get the set of integers which are the encryption keys. The steps of the ESSD method are illustrated in Algorithm 1.

Developed Algorithm ESSD (Energy Saving and Securing Data) in keys generation

Algorithm 1: The developed algorithm called ESSD (Energy Saving and Securing Data) has been depicted below

a, b node location
p: prime number
ESSD using just sum for choice in next step
choice AX, BX, CX
k1 = AX+BX+CX mod p
k2 = AX+BX+CX +k1 mod p
k3 = AX+BX+CX +k1+k2 mod p
. . . k3p = AX+BX+CX+k1+k2+k3 . . . . +k3p-1 mod p
continuous until 3P
using sequence number finished in 3p

For Example:

Let, Ax = 1, Bx = 1, Cx = 5, P = 13,

The next point is 7; (1+1+5) mod 13 ≡ 7 mod 13

The next point is 1; (1+1+5+7) mod 13 ≡ 1 mod 13

And so on as represented in Tab. 1.

Table 1: Points value with the index

Index	1	2	3	4	5	6	7	8	9	10	11	12	13
Value	1	1	5	7	1	2	4	8	3	6	12	11	9
Index	14	15	16	17	18	19	20	21	22	23	24	25	26
Value	5	10	7	1	2	4	8	3	6	12	11	9	5
Index	27	28	29	30	31	32	33	34	35	36	37	38	39
Value	10	7	1	2	4	8	3	6	12	11	9	5	10

Tab. 1 shows the generated points until the stop point 3P which equal to $3 \times 13 = 39$ in the example. In the previous step, we allow repetition in generating the key sequence, but the result should be a unique sequence without repetition.

So, the next step is to remove the repeated values and get the final sequence, as shown in Tab. 2,

Table 2: Index points without repetition used as keys

Index	1	2	3	4	5	6	7	8	9	10	11	12
Value	1	5	7	2	4	8	3	6	12	11	9	10

Tab. 2 shows the key sequence for a specific example. Thus, we have the key sequence with the least number of computations and take the ECC security in order.

3.2 Radio Energy Dissipation Model

The simple radio model which describes the energy dissipation through the electronic devices, transmitter, power amplifier and receiver is shown in Fig. 1 [37].

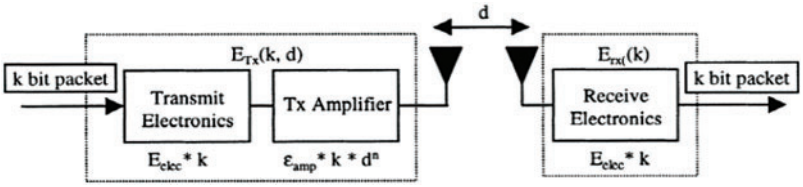

Figure 1: The simple radio model [38]

In this work, we use MATLAB [38,39] for modeling & simulating the ESSD method.

Consider the following:

1) The equations of transmission and receiving the energy of the basic radio model [40] have been considered. The equations are listed below:

$$ETX = Eclec * K + Eamp * d\,\hat{}\,2 * K \tag{2}$$

$$ERX = Eclec * K \tag{3}$$

Where,

ETX = Transmission Energy (The amount of energy consumed from the node when transmitting k of bit).

ERX = Receiving Energy (The amount of energy consumed from the node when Receiving k of bit).

Eclec (Energy used to run Transmitter Circuit) = 50 nJ/bit.

Eamp (Energy Amplifier) = 100 pJ/bit/m2.

k = number of bits to transmit or receive.

d = distance between source and destination.

Efs = Transmit Amplifier types-free space loss = 10^ (-12) * 1.

Emp = Transmit Amplifier types - multi path loss = 10^ (-15) * 1.3.

2) It's known that Eq. (4) is not defined for a distance equal to zero. That is the reason for using a close in the distance do [41], which is in the following equation:

$$do = \left(\frac{freespaceloss\,(Efs)}{multipathloss\,(Emp)}\right)\hat{}\,0.5 \tag{4}$$

3) Computing the distance between nodes using the Euclidean distance.

4) The big number of counters to compute Statistics.

3.3 ESSD Cryptosystem

Fig. 2 shows the connection loop from the node until the base station and backward. The node collects data and converts it to plain text after the ESSD method converts plain text to ciphertext. The ESSD method takes the security connection configuration as the ECC method and runs from the start

points and uses a small prime number for creating a key sequence, which is the advantage of the MD5 hash key, which gives the ESSD method less number of computations.

The ESSD is a light method as the MD5 and secure as the ECC method since it takes the ECC idea and initialization.

In this chapter, we viewed the process of the ESSD method and the methodology of testing the security methods (ECC and MD5) with TEEN and LEACH protocols.

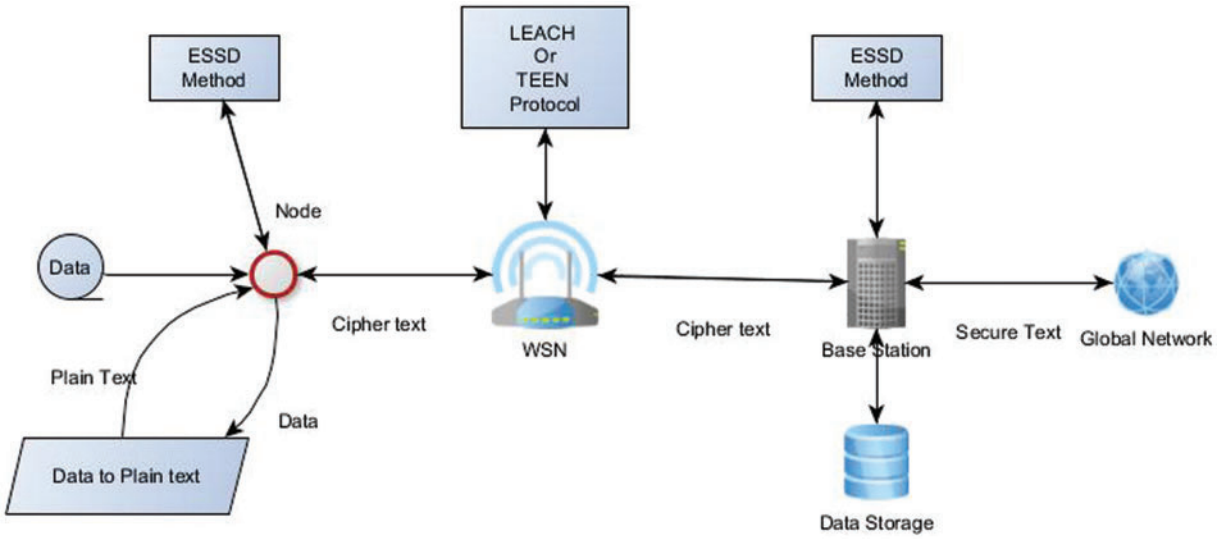

Figure 2: The ESSD diagram connection

3.4 ESSD Simulation

A MATLAB code has been developed to compare the lifetime of the best in literature routing protocols by enhancing the security services of these protocols by using the ESSD method. The implementation counts the number of dead nodes for each round (time) and shows how the proposed ESSD method outperformed the other key security algorithms such as MD5 and ECC. The proposed method has been implemented to conduct several tests.

The implementation code has been done under the following assumptions:

- In nature, all nodes are homogeneous
- All nodes start with the same initial energy
- Nodes have the location information
- The BS is situated at the center of the area space
- Clusters and nodes are static
- Normal nodes transmit directly to their respective
- All nodes are lying on the same surface. So the third dimension is ignored

The parameters used in the simulation are shown in Tab. 3.

The network lifetime in TEEN and LEACH are measured before and after applying security methods.

Table 3: Values of implementation

Parameter	Value
Nodes	100
Network size	100 m × 100 m
Base-Station location	(0,0)
Base sensor location	(50,50)
Radio propagation speed	3×10^8 m/s
Processing delay	50 μs
Data rate	1 Mbps
Data size	4000 bits
Maximum number of rounds	5000
The energy required to run circuity	5×10^{-8} Joules/bit
d_0	8.7706×10^{-11}
Heterogeneity percentage of nodes	0.1
Initial energy	2 Joules
Threshold value Alpha (α)	0.99
E_{fs}: Transmit Amplifier types-free space loss	1×10^{-12}
E_{mp}: Transmit Amplifier types - multi-path loss	1.3×10^{-15}

4 Experimental Results

This section shows the results of experimental tests with changing the security method used. All the results are the average of the 10000-time test.

4.1 Experimental Results on LEACH Routing Protocol

Fig. 3 shows the behavior of the LEACH protocol with all tested security methods.

Here, we compare with regards to energy consumption and show that the best result for energy consumption is when ESSD is used with LEACH, as the sensors began to die after 496 times (rounds) which is the longest time for all cases.

Tab. 4 shows the number of dead nodes and the time of death for each security method. As it appears, the longest time when ESSD is used, it is less energy-consuming. The most energy-consuming is when using ECC because the first 10 sensors begin to die at 412 times. The least energy-consuming is when using the ESSD method because the first 10 sensor nodes are to die at 549, and hence it shows that the best position for energy consumption is when we use ESSD with the LEACH protocol.

4.2 Experimental Results on TEEN Routing Protocol

Fig. 4 shows the behavior of TEEN protocol with all tested security methods.

Tab. 5 shows the number of dead nodes and the time of death for each security method. This table compares the numbers of sensors that die for each algorithm and shows that its best result was ESSD as, at the time, 4317 began the death of the first ten sensors. This means that we received the lowest power consumption and the confidentiality and authentication of essential security services.

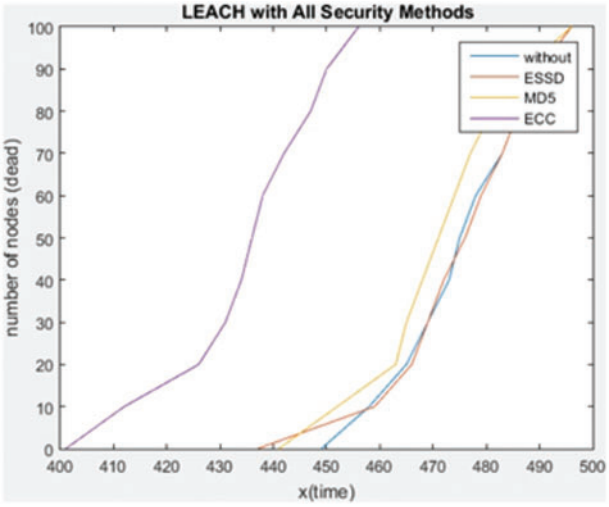

Figure 3: The LEACH Protocol with all tested security method

Table 4: The LEACH protocol with all tested security methods

Number of dead nodes		10	20	30	40	50	60	70	80	90	100
Security method	ECC	412	426	431	434	436	438	442	447	450	456
	ESSD	459	466	469	472	476	479	483	486	490	496
	MD5	452	463	465	468	471	474	477	481	487	496
	Without	458	465	469	473	475	478	483	486	490	496

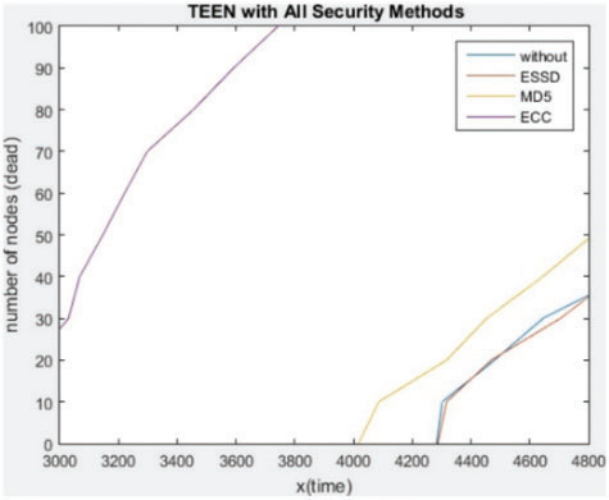

Figure 4: The TEEN protocol with all tested security method

The ESSD mapped the confidentiality from the MD5 method steps and mapped the authentication from the ECC method steps since the ESSD comes from the idea of generating MD5 and ECC.

Note: The word "Non" used in Tab. 5 describes that the test ends when it reaches the maximum number of rounds which is 5000 rounds.

Table 5: The TEEN protocol with all tested security methods

Number of dead nodes		10	20	30	40	50	60	70	80	90	100
Security method	ECC	2783	2911	3030	3068	3147	3221	3298	3455	3592	3743
	ESSD	4317	4469	4704	4889	Non	Non	Non	Non	Non	Non
	MD5	4086	4317	4453	4644	4815	Non	Non	Non	Non	Non
	Without	4302	4480	4645	4925	Non	Non	Non	Non	Non	Non

5 Conclusion and Future Works

The WSNs are mainly resource-constrained connected devices, so we must design and implement a lightweight algorithm. The proposed method of ESSD provides the security for the wireless sensor networks, as we aim to improve the selection of keys of the encryption, increase the node lifetime, and use a light-weight algorithm. These are accomplished with ESSD method by comparing the results under the same conditions with ECC and MD5. The ESSD is suitable as a secure algorithm, where the ESSD has the ECC security level and almost the same level of computing as the MD5.

We plan to apply the ESSD security method on other protocols than LEACH and TEEN in future work. Also, we will compare the results with other security methods and try to combine ECC and MD5 to get another security method that will be more efficient than ESSD.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Rawat, K. D. Singh, H. Chaouchi and J. M. Bonnin, "Wireless sensor networks: A survey on recent developments and potential synergies," *The Journal of Supercomputing*, vol. 68, no. 1, pp. 1–48, 2014.

[2] K. Sharma and M. K. Ghose, "Wireless sensor networks: An overview on its security threats," *IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs*, 1495 pp. 42–45, 2010.

[3] M. Burhanuddin, A. Mohammed, R. Ismail, M. Hameed and M. A. Kareem, "A review on security challenges and features in wireless sensor networks: IoT perspective," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 1–7, pp. 17–21, 2018.

[4] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," *Proceedings of the World Congress on Engineering*, vol. 1, no. 20, pp. 876–3423, 2015.

[5] N. Saqib and U. Iqbal, "Security in wireless sensor networks using ECC," in *2016 IEEE Int. Conf. on Advances in Computer Applications (ICACA)*, USA, pp. 270–274, 2016.

[6] J. Li, "A symmetric cryptography algorithm in wireless sensor network security," *International Journal of Online Engineering (iJOE)*, vol. 13, no. 11, pp. 102–110, 2017.

[7] M. Shafiq, H. Ashraf, A. Ullah and S. Tahira, "Systematic literature review on energy efficient routing schemes in WSN-A Survey," *Mobile Networks & Applications*, vol. 25, no. 3, pp. 882–895, 2020.

[8] G. Sharma, S. Bala and K. Verma, "Security frameworks for wireless sensor networks-review," *Procedia Technology*, vol. 6, no. 11, pp. 978–987, 2012.
[9] M. Panda, "Security in wireless sensor networks using cryptographic techniques," *American Journal of Engineering Research*, vol. 3, no. 1, pp. 50–56, 2014.
[10] A. Shamir, "Identity based cryptosystems and signature schemes," in *Proc. Crypto'84*, USA, pp. 47–53, 1984.
[11] J. Thakur and N. Kumar, "DES, AES and BlowFish: Symmetric key cryptography algorithms simulation-based performance analysis," *International Journal of Engineering Technology and Advanced Engineering*, vol. 1, no. 2, pp. 6–12 2011.
[12] G. Quirino, A. Ribeiro and E. Moreno, "Asymmetric encryption in wireless sensor networks," *Wireless Sensor Networks-Technology and Protocols*, pp. 219–232, 2012.
[13] W. Stallings, Network and internetwork security: Principles and practices. Prentice-Hall, Inc, USA, 1995.
[14] M. Alshammari and K. Elleithy, "Efficient and secure key distribution protocol for wireless sensor networks," *Sensors*, vol. 18, no. 10, pp. 3569, 2018.
[15] R. Rivest, A. Shamir and L. Adleman, "A Method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[16] N. Koblitz, "Elliptic curve crytosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.
[17] V. Miller, "Use of elliptic curves in cryptography," in *Conference on the Theory and Application of Cryptographic Techniques*, Springer, vol. 128, pp. 417–426, 1985.
[18] I. Mansour, G. Chalhoub and P. Lafourcade, "Key management in wireless sensor networks," *Journal of Sensor and Actuator Networks*, vol. 4, no. 3, pp. 251–273, 2015.
[19] D. Carman, P. Krus and B. Matt, "Constraints and approaches for distributed sensor network security. Glenwood, MD: NAI Labs, Network Associates Inc, Technical Report 00-010, 2000.
[20] M. Brown, D. Cheung, D. Hankerson, J. Hernandez and M. Kirkup, "PGP in constrained wireless devices," in *Proc. of the 9th USENIX Security Sym.*, Colorado, 2000.
[21] A. Wander, N. Gura, H. Eberle, V. Gupta and S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proc. of the 3rd IEEE Int. Conf. on Pervasive Computing and Communications*, USA, pp. 324–328, 2005.
[22] K. Piotrowski, P. Langendoerfer and S. Peter, "How public key cryptography influences wireless sensor node lifetime," in *Proc. of the 4th ACM workshop on Security of Ad Hoc and Sensor Networks*, NY, USA, pp. 169–176, 2006.
[23] J. Hill, R. Szewczyk, A. Woo, S. Hollar and D. Culler, "System architecture directions for networked sensors," in *Proc. of the 9th Int. Conf. on Architectural Support for Programming Languages and Operating Systems*, New York, ACM Press, pp. 93–104, 2000.
[24] R. Anderson, F. Bergadano, B. Crispo, C. Manifavas and R. Needham, "A new family of authentication protocols," *ACM SIGOPS Operating Systems Review*, vol. 32, no. 4, pp. 9–20, 1998.
[25] G. Quirino and E. Moreno, "Architectural evaluation of algorithms RSA, ECC and MQQ in ARM processors," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 5, no. 2, pp. 153–168, 2013.
[26] R. Watro, D. Kong, S. Cuti, C. Gardiner and C. Lynn, "TinyPK: Securing sensor networks with public key technology," in *Proc. of the 2nd ACM workshop on Security of Ad Hoc and Sensor Networks*, NY, USA, pp. 59–64, 2004.
[27] R. Rivest, "The MD5 Messege-Digest algorithm," in *RFC 1321*, USA, 1992.
[28] R. Mahapatra and R. Yadav, "Analysis of classical routing algorithms on different contention based MAC protocols for wireless sensor networks," *Journal of Information and Computing Science (JICT)*, vol. 9, no. 1, pp. 31–36, 2014.
[29] E. R. Neetika and S. Kaur, "Review on hierarchical routing in wireless sensor network," *International Journal of Smart Sensors and Ad- Hoc Networks (IJSSAN)*, vol. 2, no. 4, pp. 295–300, 2012.

[30] A. Bhattacharjee, B. Bhallamudi and Z. Maqbool, "Energy-efficient hierarchical cluster based routing algorithm in Wsn: A Survey," *International Journal of Engineering Research & Technology (IJERT)*, vol. 2, no. 5, pp. 302–311, 2013.
[31] S. Verma, R. Mehta and K. Sharma, "Wireless sensor network and hierarchical routing protocols: A Review," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, no. 8, pp. 2411–2416, 2013.
[32] W. Sun, G. Z. Dai, X. R. Zhang, X. Z. He and X. Chen, "TBE-Net: A three-branch embedding network with part-aware ability and feature complementary learning for vehicle re-identification," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–13, 2021.
[33] W. Sun, L. Dai, X. R. Zhang, P. S. Chang and X. Z. He, "RSOD: Real-time Small object detection algorithm in UAV-based traffic monitoring," *Applied Intelligence*, vol. 92, no. 6, pp. 1–16, 2021.
[34] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient communication protocol for wireless microsensor networks," in *Proc. of the 33rd Hawaii Int. Conf. on System Sciences*, Hawaii, pp. 1–10, 2000.
[35] S. Singh, M. Singh and D. Singh, "A Survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks," *International Journal of Advanced Networking and Applications*, vol. 02, no. 2, pp. 570–580, 2010.
[36] A. Manjeshwar and D. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," in *Proc. of the 15th Int. Parallel and Distributed Processing Sym. (IPDPS'01)*, CA, USA, vol. 1, pp. 189–2015, 2001.
[37] R. Mahapatra and R. Yadav, "Descendant of LEACH based routing protocols in wireless sensor network," *In proceedings of 3rd International Conference on Recent Trends in Computing (ICRTC-2015). Procedia Computer Science*, vol. 57, pp. 1005–1014, 2015.
[38] S. Attaway, MATLAB: A practical introduction to programming and problem solving. Elsevier. Inc, Boston, MA, USA, 2009.
[39] A. Gilat, MATLAB: An introduction with applications. John Wiley and Sons, USA, 2004.
[40] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
[41] N. Gura, A. Patel, A. Wander, H. Eberle and S. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Proc. of the 2004 6th Int. Workshop on Cryptographic Hardware and Embedded Systems (CUES 2004)*, Boston, 2004.