Hindawi
Journal of Sensors
Volume 2021, Article ID 8878513, 8 pages
https://doi.org/10.1155/2021/8878513

Research Article

CoopECC: A Collaborative Cryptographic Mechanism for the Internet of Things

Wassim Jerbi, [1,2] Abderrahmen Guermazi, [1,2] Omar Cheikhrouhou, [3] and Hafedh Trabelsi [1]

[1] *CES LAB, National Engineering School of Sfax (ENIS), University of Sfax, Tunisia*
[2] *Higher Institute of Technological Studies of Sfax, 3099 El Bustan, Sfax, Tunisia*
[3] *College of CIT, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia*

Correspondence should be addressed to Wassim Jerbi; wassim.jerbi@isetn.rnu.tn

Received 24 April 2020; Revised 30 November 2020; Accepted 19 February 2021; Published 12 March 2021

Academic Editor: Mucheol Kim

The emergence of IoT applications has risen the security issues of the big data sent by the IoT devices. The design of lightweight cryptographic algorithms becomes a necessity. Moreover, elliptic curve cryptography (ECC) is a promising cryptographic technology that has been used in IoT. However, connected objects are resource-constrained devices, with limited computing power and energy power. Driven by these motivations, we propose and develop a secure cryptographic protocol called CoopECC which leverages the organization of IoT nodes into cluster to distribute the load of cluster head (CH) among its cluster members. This technique proves that it optimizes the resource consumption of the IoT nodes including computation and energy consumption. Performance evaluation, done with TOSSIM simulator, shows that the proposed protocol CoopECC outperforms the original ECC algorithm, in terms of computation time, consumed energy, and the network's lifespan.

1. Introduction

The emergence of IoT technology resulted in its integration in various applications including smart cities, healthcare, machine to machine systems, connected vehicles, and smart homes. Moreover, IoT technology was used within other cutting-edge technologies such as cloud computing, big data, and blockchain. This widespread of IoT integration raises the security issues and pushes the requirement of a reliable security protocols. However, the limited resource characteristic of IoT devices makes the development of lightweight algorithms a challenge.

Moreover, the big data volume generated by IoT devices increases the necessity of lightweight cryptographic algorithm to encrypt such data in privacy aware applications.

Although these security needs, recent studies [1] show that existing security protocols fail to fulfill the characteristics and requirements of IoT devices.

Moreover, as security protocols are based on cryptographic algorithms, their efficiency mainly depends on the efficiency of these cryptographic algorithms. Therefore, recent studies [2] have focused on the cryptographic algorithm for IoT.

Cryptographic systems are currently divided into two main areas: symmetric cryptography and asymmetric cryptography. While symmetric cryptography is often used for symmetric encryption, asymmetric cryptography encompasses two main use cases: asymmetric encryption and digital signature. Asymmetric cryptography is the choice of the most system due to its level of security. The most used asymmetric cryptographic methods are RSA [3] and ECC [1].

However, the RSA algorithm is not adapted to IoT devices due to its high key length [4]. An alternative to the RSA algorithm is the ECC algorithm. Indeed, ECC offers the same level of encryption strength for much shorter keys up to 160 bits instead of 1024 bits for the RSA. Therefore, ECC provides better security level while reducing computation power. Shorter keys make ECC more adequate for devices with limited storage capacity and processing power, such as those used in the Internet of Things.

However, elliptic curve operations still require a computation power that is not supported by IoT devices. The main complex ECC operations are the point multiplication, which is also called the scalar multiplication.

In this paper, we have used the paralleling technique. The latter makes it possible to distribute the tasks between the various nodes to accelerate the computation of the scalar multiplications. The proposed solution benefits from the massive node deployment and leverage the cooperation of these nodes to achieve the cryptographic task.

More precisely, our solution is more adapted to cluster-based network architecture, and it allows the cluster head (CH) to break down the computation task between the different members of the cluster. This permits to lighten the cryptography processing at IoT nodes.

The organization of this article is presented as follows: in Section 2, we present overviews of related works. Then, Section 3 is devoted to the presentation of the CoopECC for asymmetric cryptography. Subsequently, Section 4 presents the simulation results of the CoopECC protocol in relation of work subsequent and discussions. Finally, Section 5 concludes this paper and describes future perspectives.

2. Related Works

The clustering technique consists in partitioning the network into a set of clusters as presented in Figure 1. Each cluster contains a leader sensor node called CH. The role of CH consists of coordinating between the members of its cluster, thus collecting data and aggregating it and then transmitting it to the base station. The CH is selected to facilitate this role according to specific metrics including remaining energy power, its position. The most known protocols for clustering are LEACH [5] and HEED [6].

WSN are subject to various attacks like all computer networks. To mitigate these attacks, the adequate solution is to protect the data circulating between the nodes with the installation of a set of techniques and security mechanisms. Moreover, one must consider the resources of the sensor (computation power, energy level, etc.). The candidate security techniques must meet the main security requirements including integrity, confidentiality, authentication, and freshness of data. Integrity means that the data must not be modified during transmission [7]. Confidentiality ensures that information should never flow in a clear way between nodes, especially in critical applications such as military and healthcare. The data will be encrypted and, therefore, not interpretable and understandable by eavesdroppers [8]. Then, authentication protects the network against identity theft attacks by verifying the identity claimed by a node. Subsequently, the freshness technique ensures that the data received are recent.

In [9], the key Distribution Protocol to Secure Routing (KDSR) presents an efficient process to share local key distribution. Extend the OneTime Password (OTP) principle and propose a novel approach of OTP generation that relies on the ECC algorithm in order to ensure IoT security [10, 11].

[12] allows discovering the correlations among sustainable development goals and information and communications technologies. In [13], the author presents the security threats in mobile edge computing of IoT and proposes a physical layer authentication method which exploits channel state information to mitigate threats via detecting spoofing attacks in wireless networks.

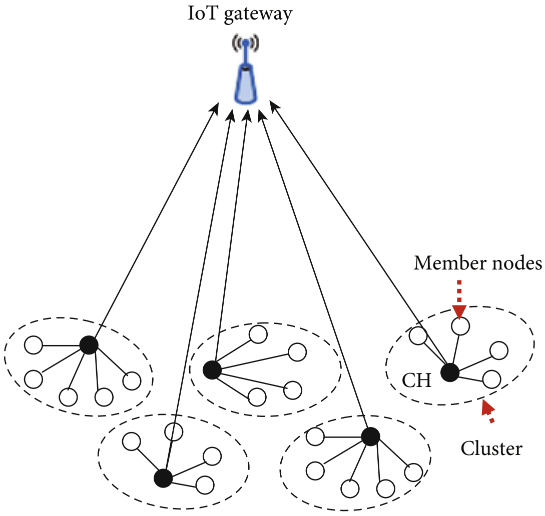

Figure 1: Cluster-based organization for WSNs.

In [14], the protocol KMMR presents three operations. At the beginning, it deals with light local processes orchestrated in ascending and descending levels. Second, it limits the impact of compromised nodes to local links only. Third, KMMR adds and revokes efficient secure nodes. ECC is an ondemand routing network protocol which is specially design for wireless sensor network and ad hoc [15, 16].

In [17, 18], the proposed protocol makes it possible to distribute the computation between the CH and the different members of the cluster. The CH requests these members nodes to calculate well-defined tasks. This operation saves energy and computation at the level of CH. However, the energy will be equal between the different nodes of the zone to oversee, which allows an extension of the life of the network. [19] uses the paralleling technique which makes it possible to accelerate the computation of scalar multiplications. This technique helps to make the work of the CH lightweight.

Currently, there are several challenges related to the development of WSN which is being researched with different technologies and various security-based studies. The authors conducted also their research on factors such as constraints, threats and actions to be taken, vulnerabilities, and security requirements. Based on the situation mentioned above, we have classified the different studies proposed according to the security strategies that were described in each study. These studies can be presented in two essential categories. Studies [20, 21] are related to threats, and adopting proactive security measures helps prevent these attacks more effectively such as constraints and vulnerabilities in WSN networks, and other studies [22, 23] show security requirements, such as how to take countermeasures and the solutions adopted.

Several methods of key management are presented in [24–33], including a random key predistribution method

[34, 35], a block-based encryption [36], and an authentication framework [37]. Each sensor node shares a key with its neighbors and a key with the base station [38]. The base station detects malicious cluster head nodes through authentication. In [39, 40], the authors proposed a security mechanism that permits to identify the malicious nodes through a query processing. This technique provides essential security properties such as confidentiality, integrity, freshness, and data authentication [41–47].

3. The Proposed Protocol: CoopECC

Currently, the IoT is a global network where each entity has a unique address and is connected to the Internet. Any IoT device, including sensors and actuators, can be controlled by mobile phones; so, it will be possible to send data and receive commands. The IoT opens the way to a multitude of applications based on the interconnection between the physical world and cloud computing systems. However, before the large deployment of IoT applications, a number of challenges need to be resolved.

One of these challenges that IoT faces is security and privacy issues. In fact, lack of security increases the risk of users' personal information leakage, while the data is being collected and transmitted through the IoT devices.

Therefore, we propose in this paper a lightweight cryptographic protocol based on collaborative cryptographic mechanism. Our contribution aims to lighten the cryptographic task of the cluster head (CH) by distributing it among cluster members. This technique permits to prolong the network life. More precisely, we leverage the parallelization of scalar multiplications to distribute ECC operations between cluster members.

3.1. CoopECC Description. The ECC algorithm brings together a set of cryptographic techniques which use one or more properties of elliptic curves or more generally of an abelian variety. The use of this technique makes it possible to improve the existing cryptographic primitives, for example, by reducing the size of the cryptographic keys or to construct new cryptographic primitives which were not previously known. ECC is a collection of techniques that ensure data security between nodes while consuming less resource. This makes it possible to attract the attention of researchers more and more.

The advantage of ECC over other cryptography algorithms, e.g., RSA and AES [40], is to have secure communication with a short key size. An experiment was done by Gura et al. [48] that showed by a test with ECC, and only 160 bits are used compared to other asymmetric cryptography algorithms as RSA uses a 1024 bit key. Therefore, the short size of the ECC key enables fast computation, memory saving, and energy.

Our goal is to distribute tasks and simplify the cryptographic operations computation between the CH and its cluster members. More precisely, the proposed CoopECC protocol has the following characteristics:

(i) Task distribution: this method permits to lighten the load of the CH. The CH distributes the main program among the members. This permits to execute the program faster

(ii) Task parallelization: task parallelization allows procedures or threads to be executed by cluster members in parallel

(iii) A lightweight computation: the proposed CoopECCconsumes less computation and energy power than the original ECC, and therefore, it fits the limited resources of IoT devices

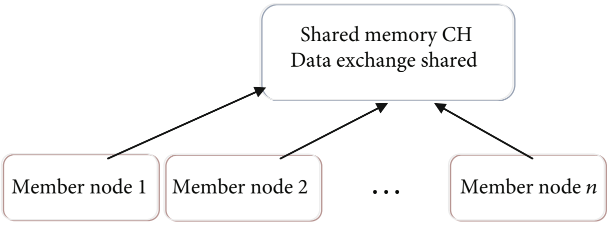

FIGURE 2: Data exchange between CH and cluster members.

To provide parallel computation, we propose to share the memory of the CH between the different cluster member nodes. This shared memory will serve as a communication buffer between CH and its members, and therefore contains the exchanged data, as shown in Figure 2.

All cluster member nodes participate in parallel computations and can perform necessary data updates. This is a reliable and scalable configuration based on the available cluster members. Therefore, the operation of the system will greatly improve its performance.

Depending on the type of the used memory, the time management mechanism to be implemented may be different. The use of shared memory architecture allows easier cooperation between cluster members and therefore faster completion of their tasks. Figure 3 shows that n1 detects the memory block containing, writing, uploading, and reading data exchange X which is momentarily occupied by n2, and it is imperative that n1 will wait for n2 to terminate its current operation as illustrated in equation (1).

$$E : y2 + a1xy + a3y = x3 + a2x2 + a4x + a6. \tag{1}$$

We propose a security algorithm in wireless communication deployed for IoT. We consider cluster-based network topology where a CH is responsible to collect, encrypt, and forward data to the destination. To ensure the security that preserve the confidentiality of data in particular, the ECC algorithm has been used initiated by a CH. As the sensor nodes are resource constraints including, energy, memory, and computation, the scaler multiplications of ECC (the more computational tasks) are done by a set of member nodes in parallels in a cluster provided by the CH.

The technical contribution of the paper is to perform multiplication calculations more efficiently, and the following approach is proposed:

The objective is to calculate $k * G$, where G is a known fixed number and k is the input. The bits of k are divided into n equal parts. Each part is given to different nodes in a

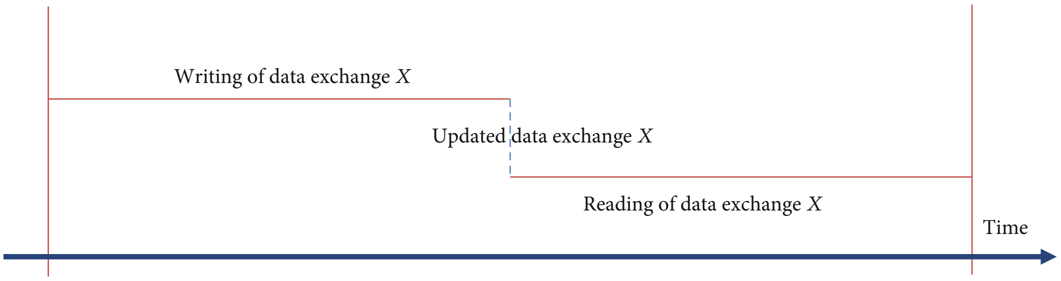

Figure 3: Synchronization of data access.

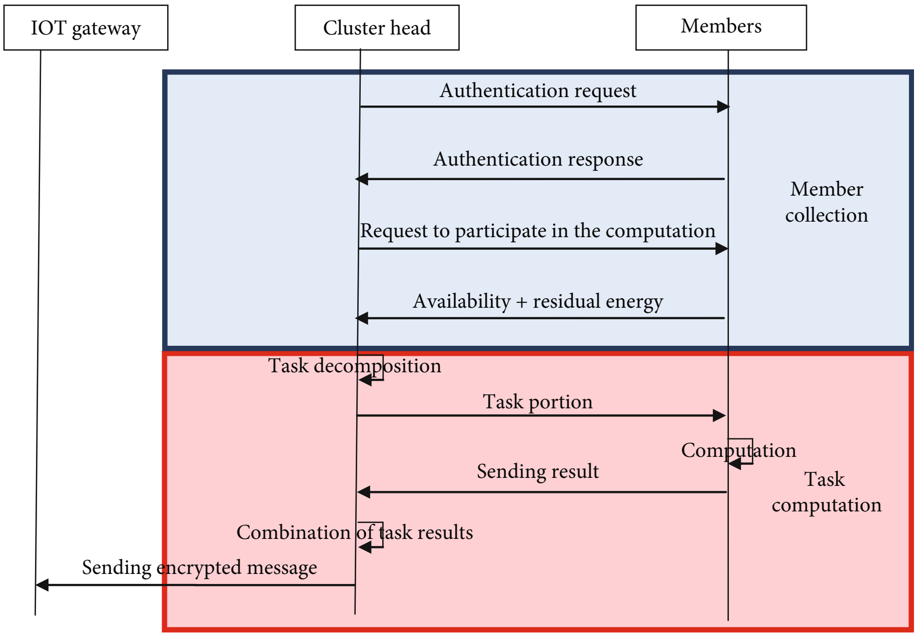

Figure 4: Cooperative cryptographic computation.

cluster. Each of these nodes multiplies its part of k by G and returns the result to CH. The latter collects all the results after appropriate bit shifts to obtain $k * G$.

$$K = \sum_{i=0}^{l-1} \left(K_i 2^{\mathrm{i}}\right). \tag{2}$$

The CH decomposes the integer k into n segments S_i of length $b = \lceil l/n \rceil$:

$$S_i = \sum_{j=ib}^{ib+b-1} \left(K_j 2^j\right). \tag{3}$$

G is a generator point and does not change during the life of the network. $K * G$ will be broken down as follows ($G_i = 2^{ib} G$ is possible):

$$\begin{cases} Q_0 = S_0 G \\ \mathrm{Q}_1 = \mathrm{S}_1 2^{\mathrm{b}} \mathrm{G} \\ \ldots\ldots \ldots \; \ldots \; \ldots \\ Q_{n-1} = S_{n-1} 2^{b(n-1)} G \end{cases} . \tag{4}$$

Using equation (3), each member computations Q_i and transmits the result to the CH. The latter combines them to have the final result.

$$Q_0 = S_0 G + S_1 2^b G + S_2 2^{2b} G \cdots .S_{(n-1)} 2^{(n-1)} G. \tag{5}$$

3.2. CoopECC Operations. The CH receives data revealing a critical event from one of these member nodes. At this time, the CH must inform the BS to take the necessary precautions for all the nodes of the network. The other available members of the same cluster are asked to participate in the cryptographic computation to speed up the encryption procedure. The description of different steps is shown in Figure 4 and given below:

(1) First, the CH authenticates the cluster member

(2) Then, the CH requests the participation of each member node which has enough residual energy for parallel computation

Table 1: Telosb sensor technical specifications.

μController	8 MHZ MSP 430 16-bits MCU
Radio antenna	CC2420 (802.15.4/Zigbee)
Flash memory	48 Ko
RAM	10 Ko

(3) Then, the CH member receives the task necessary to use parallel computing and accelerate the encryption of sensitive data

(4) Member nodes quickly perform parallel computations while viewing data in CH shared memory

(5) Each member node has done what is requested, and it transmits the result of the computation to the CH. The latter combines the results obtained to obtain the final result which can be used to encrypt or sign the message to be sent. The CH aggregates the data and sends it to the IoT Gateway

4. Performance and Evaluation of CoopECC

In order to evaluate the performance of our CoopECC protocol, we implemented it on Telosb sensors, which are designed by Crossbow Technology for research purposes. The technical characteristics of Telosb sensors are presented in Table 1.

The development of the CoopECC protocol was carried out by the NesC (*C* for network and embedded system) language [49] and development language Tinyos [50]. In Table 2, we present the computation time in ms of our parallelism protocol. The gain expressed as a percentage, and it is calculated according to equation (6).

$$\frac{\text{Time}_{\text{ECC}} - \text{Time}_{\text{CoopECC}}}{\text{Time}_{\text{ECC}}}. \quad (6)$$

The gain obtained using the parallelism technique is shown in Table 2 and Figure 5.

Figure 5 shows the computation time of ECC and CoopECC. More precisely, the computation time decreases progressively when more member nodes participate in the parallel computation.

We can notice a significant drop in acceleration as soon as we use more than 45 nodes. The cluster head needs additional time, called overcost, to coordinate radio communications, combine the results received, and calculate the final result.

We used scalar computation up to 60 nodes managed by a single CH in a single cluster. Compared to ECC, gain starts when a cluster contains more than 10 member nodes, and we have obtained a maximum gain of 60% when the number of members reaches 45 nodes. Each node performs the requested computation in minimum time and with very low power consumption. Every time, the number of nodes participating in the computation increases, and there will be an improvement in the life of the network. This implies that the CoopECC protocol presents a better design and a good functioning which allows it to properly manage its cluster composed of CHs and these members.

Table 2: The gain in terms of time (ms) of our parallelism protocol.

Number of nodes in a cluster	ECC	CoopECC	Gain
0	130	190	-46%
5	130	160	-23%
10	130	135	-4%
15	130	115	12%
20	130	98	25%
25	130	80	38%
30	130	70	46%
35	130	60	54%
40	130	55	58%
45	130	52	60%
50	130	52	60%
55	130	55	58%
60	130	58	55%

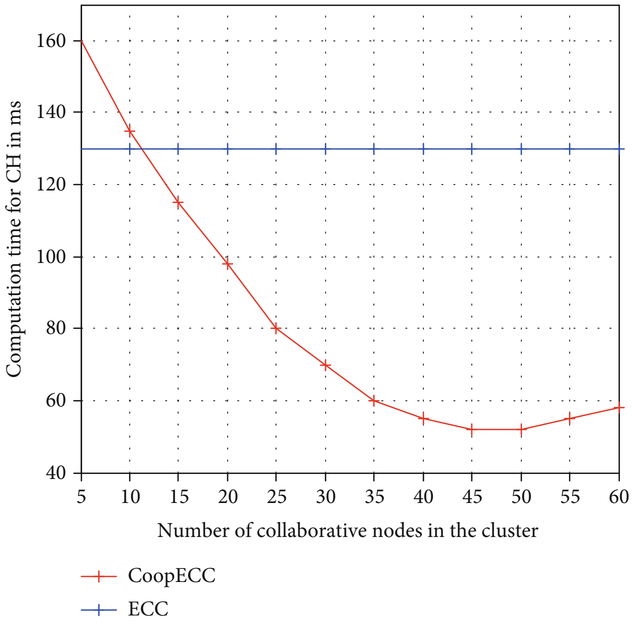

Figure 5: Computation time for CoopECC protocol.

We define the computation time with *p* nodes as Tp, and we evaluate the performance of our method with its speed as Sp which is defined in equation (7), and results are cited in Table 3 and presented in Figure 6.

$$S_{\text{p}} = T_1/T_{\text{p}}. \quad (7)$$

Figure 6 shows that the curve is ascending when it exceeds 10 nodes. This acceleration allows to get results quickly without consuming high energy. Each time the number of nodes increases, the more gains we obtain. The role of the CH is to break down the tasks to simplify the processing by the members.

Table 3: Speed of the proposed protocol CoopECC.

Number of nodes	5	10	15	20	25	30	35	40	45	50	55	60
CoopECC	1.43	2.7	3.9	5.1	5.8	6	6.1	6.2	6.25	6.25	6.1	5.9

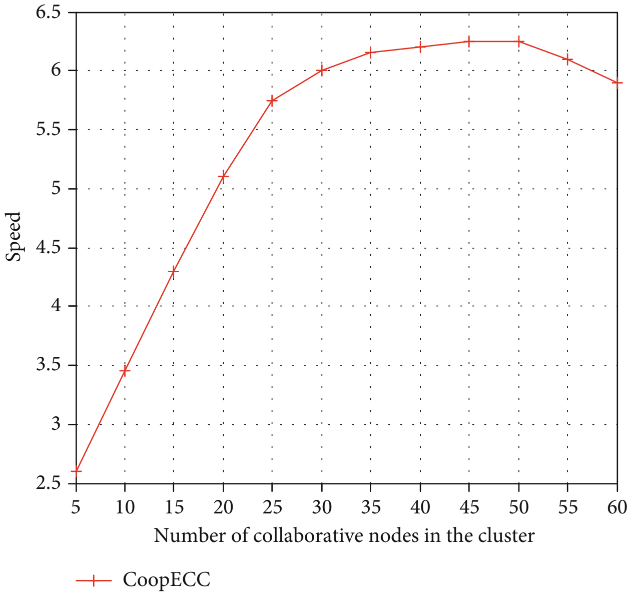

Figure 6: Speed of CoopECC protocol.

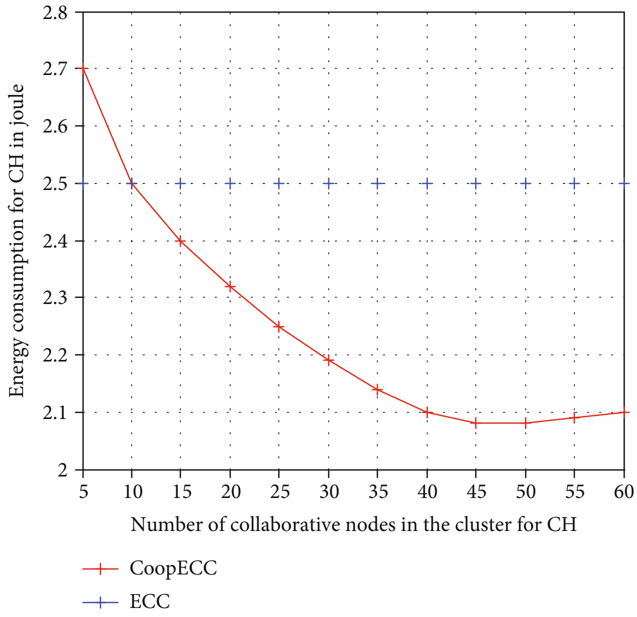

Figure 7: Energy consumption of CoopECC protocol.

The time saved during the calculation reduces energy consumption. A CH can only manage 45 member nodes per cluster, between 45 and 50 nodes, and we see stability. After 50 nodes, there is a drop in the level of scalar computation.

According to Figure 7, the number of nodes is less than 10, a higher energy consumption for the CoopECC protocol,

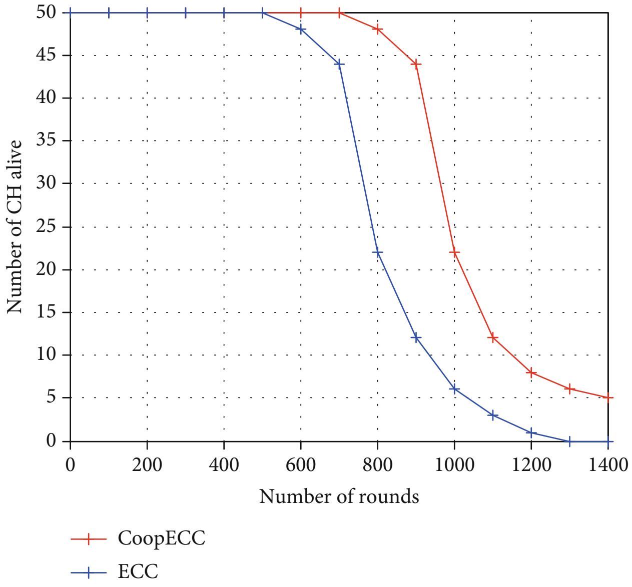

Figure 8: Lifetime of CoopECC protocol.

and this is due to message transmission. Starting from 10 nodes participating in the computation task, the energy consumption of the CoopECC protocol is reduced compared to the ECC algorithm. In ECC, each time a node is elected as CH, it consumes energy, which might leads to its energy depletion and, therefore, a risk of having a limited lifetime of the network.

A very important energy gain when the computation is distributed between a CH and its members. CoopECC offers low energy consumption, good acceleration, and long network lifetime.

Figure 8 illustrates the lifetime of the CoopECC protocol compared to the number of live nodes per round. The first nodes start dying for CoopECC at the 700 rounds, while in the ECC, the first nodes start dying at the 500 rounds. At the end of the simulation, the number of living nodes reaches 1400 rounds for CoopECC and 1200 for ECC. Consequently, CoopECC allows extending the lifetime of the network compared to ECC by maximizing the lifetime of CHs.

5. Conclusion

Cryptography is a widely used solution to secure communication between IoT devices. Our proposed CoopECC protocol is well suited to resource constrained devices. Indeed, CoopECC permits to speed up the cryptographic operations computation based on parallelism concept. More precisely, a computation task is distributed among cluster members to offload the CH. To prove the efficiency and robustness of our approach, we set up a simulation using the TOSSIM simulator. The performance evaluation results have proven the efficiency of our protocol. More precisely, results show that CoopECC offers an interesting gain in terms of energy consumption, good acceleration, computation time, and an extension of network's lifespan. The proposed CoopECC fits the requirement of real-time applications, where the network needs to report an urgent event to the base station, for example, the detection of a natural disaster in environmental monitoring application.

As future work, we plan to work on cryptographic solution for cognitive IoT and using federated learning technique.

Data Availability

The data used to support the findings of the manuscript are available within the article.

Conflicts of Interest

The author(s) declare(s) that they have no conflicts of interest.

Acknowledgments

Dr. Omar Cheikhrouhou thanks the Taif University for its support under the project Taif University Researchers supporting project number (TURSP-2020/55), Taif University, Taif, Saudi Arabia.

References

[1] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987.

[2] J. Yu, E. Lee, S. Oh, Y. Seo, and Y. Kim, "A survey on security requirements for WSNs: focusing on the characteristics related to security," *IEEE Access*, vol. 8, pp. 45304–45324, 2020.

[3] R. L. 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.

[4] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *In Proceedings of the 9th ACM conference on Computer and communications security*, pp. 41–47, Washington, DC, USA, 2002.

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, pp. 10–19, Maui, HI, USA, 2000.

[6] O. Younis and S. Fahmy, "HEED: a hybrid, energy-efficient, distributed clustering approach for adhoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, pp. 66–379, 2004.

[7] A. Ghosal, S. Halder, S. Sur, A. Dan, and S. DasBit, "Ensuring basic security and preventing replay attack in a query processing application. Domain in WSN," in *International Conference on Computational Science and Its Applications*, pp. 321–335, Springer, 2010.

[8] U. Prathap, P. D. Shenoy, and K. Venugopal, "CMNTS: catching malicious nodes with trust support in wireless sensor networks," in *2016 IEEE Region 10 Symposium (TENSYMP)*, pp. 77–82, Bali, Indonesia, 2016.

[9] A. Guermazi, A. Belghith, and M. Abid, "KDSR: a scalable key distribution protocol to secure multi-hop routing in large-scale wireless sensor," in *Networks Sensor Technology: Concepts, Methodologies, Tools, and Applications*, pp. 301–320, IGI Global, 2020.

[10] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," in *The Proceedings of the 10th ACM conference on Computer and communications security*, pp. 62–72, Washington, DC, USA, 2003.

[11] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit cpus," in *Cryptographic Hardware and Embedded Systems - CHES 2004*, M. Joye and J.-J. Quisquater, Eds., pp. 119–132, Springer, 2004.

[12] K. Demestichas, "Survey on security threats in agricultural IoT and smart farming," *Sensors*, vol. 20, no. 22, p. 6458, 2020.

[13] V. Hayashi and W. Ruggiero, "Non-invasive challenge response authentication for voice transactions with smart home behavior," *Sensors*, vol. 20, no. 22, p. 6563, 2020.

[14] A. Guermazi, A. Belguith, M. Abid, and S. Gannouni, "KMMR: an efficient and scalable key management protocol to secure multi-hop communication in large scale wireless sensor network," *KSII Transactions of Internet and Information Systems*, vol. 11, no. 2, 2017.

[15] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for Internet of Things (IoT)," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440–3450, 2020.

[16] R. B. Uriarte and R. DeNicola, "Blockchain-based decentralized cloud/fog solutions: challenges, opportunities, and standards," *IEEE Communications Standards Magazine*, vol. 2, no. 3, pp. 22–28, 2018.

[17] A. Praveena and S. Smys, "Efficient cryptographic approach for data security in wireless sensor networks using MES VU," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1–6, Coimbatore, India, 2016.

[18] W. Jerbi, A. Guermazi, and H. Trabelsi, "Crypto-ECC: a rapid secure protocol for large-scale wireless sensor networks deployed in internet of things," in *International Conference on Dependability and Complex Systems*, pp. 293–303, Springer, 2020.

[19] W. Jerbi, A. Guermazi, and H. Trabelsi, "A secure routing protocol in heterogeneous networks for internet of things," in *2020 International Wireless Communications and Mobile Computing (IWCMC),*, pp. 571–576, Limassol, Cyprus, 2020.

[20] W. Jerbi, A. Guermazi, and H. Trabelsi, "A novel secure routing protocol of generation and management cryptographic keys for wireless sensor networks deployed in internet of things," *International Journal of High Performance Computing and Networking*, vol. 16, no. 2/3, pp. 87–94, 2020.

[21] M. Aloqaily, I. al Ridhawi, H. B. Salameh, and Y. Jararweh, "Data and service management in densely crowded environments: challenges, opportunities, and recent developments," *IEEE Communications Magazine*, vol. 57, no. 4, pp. 81–87, 2019.

[22] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the internet of things," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–5, Sakaka, Saudi Arabia, 2019.

[23] F. Kiani, "A novel channel allocation method for time synchronization in Wireless Sensor networks," *International Journal of Numerical Modelling: Electronic Networks*, vol. 29, no. 5, pp. 805–816, 2016.

[24] O. Cheikhrouhou, "Secure group communication in wireless sensor networks: a survey," *Journal of Network and Computer Applications*, vol. 61, pp. 115–132, 2016.

[25] W. Jerbi, A. Guermazi, and H. Trabelsi, "Design and deployment of a security protocol to provide authentication services for connected objects," in *Proceedings of the 10th Euro-American Conference on Telematics and Information Systems*, pp. 1–6, Aveiro, Portugal, 2020.

[26] O. Cheikhrouhou, A. Koubâa, G. Dini, H. Alzaid, and M. Abid, "LNT: a logical neighbor tree secure group communication scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1419–1444, 2012.

[27] A. Mnif, O. Cheikhrouhou, and M. B. Jemaa, "An ID-based user authentication scheme for wireless sensor networks using ECC," in *ICM 2011 Proceeding*, pp. 1–9, Hammamet, Tunisia, 2011.

[28] M. Boujelben, O. Cheikhrouhou, H. Youssef, and M. Abid, "A pairing identity based key management protocol for heterogeneous wireless sensor networks," in *2009 International Conference on Network and Service Security*, pp. 1–5, Paris, France, 2009.

[29] O. Cheikhrouhou, A. Koubâa, G. Dini, and M. Abid, "RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 15, no. 8, pp. 783–797, 2011.

[30] M. Boujelben, O. Cheikhrouhou, M. Abid, and H. Youssef, "Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks," in *2009 Third International Conference on Sensor Technologies and Applications*, pp. 442–448, Athens, Greece, 2009.

[31] O. Cheikhrouhou and A. Koubâa, "Blockloc: Secure localization in the internet of things using blockchain," *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, 2019, pp. 629–634, Tangier, Morocco, 2019.

[32] W. Jerbi, A. Guermazi, and H. Trabelsi, "High coverage of connected nodes routing protocol for multi-hop wireless sensor network," in *Euro-American Conference on Telematics and Information Systems, EATIS 2018*, pp. 1–5, Fortaleza, Brazil, 2018.

[33] W. Jerbi, A. Guermazi, and H. Trabelsi, "A novel energy consumption approach to extend the lifetime for wireless sensor network," *International Journal of High Performance Computing and Networking*, vol. 16, no. 2/3, pp. 121–160, 2020.

[34] G. Santhi and R. Sowmiya, "A survey on various attacks and countermeasures in wireless sensor networks," *International Journal of Computer Applications*, vol. 159, no. 7, pp. 7–11, 2017.

[35] A. Alharbi, "Security issues in wireless sensor networks," *Indian Journal of Science and Technology*, vol. 10, no. 24, pp. 1–5, 2017.

[36] V. Ekong and U. Ekong, "A survey of security vulnerabilities in wire-less sensor networks," *Nigerian Journal of Technology*, vol. 35, no. 2, pp. 392–397, 2016.

[37] M. Ruta, F. Scioscia, S. Ieva, G. Capurso, and E. Di Sciascio, "Semantic blockchain to improve scalability in the internet of things," *Open Journal of Internet Of Things*, vol. 3, no. 1, pp. 46–61, 2017.

[38] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internetof things: challenges and solutions," 2016, http://arxiv.org/abs/1608.05187.

[39] T. Hardjono and N. Smith, "Cloud-based commissioning of constrained devices using permissioned blockchains," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pp. 29–36, Xi'an China, 2016.

[40] S. Agwa, E. Yahya, and Y. Ismail, "Power efficient AES corefor IoT constrained devices implemented in 130nm CMOS," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–4, Baltimore, MD, 2017.

[41] J. Daemen and V. Rijmen, *The block cipher Rijndael, Smart Card research and Applications, LNCS 1820*, Springer, 2000.

[42] W. Jerbi, A. Guermazi, and H. Trabelsi, "Orphan node connected management in multi-hop clustering-based routing protocols for wireless sensor Networks," *International Journal of Interdisciplinary Telecommunications and Networking*, vol. 11, no. 4, pp. 1–16, 2019.

[43] W. Jerbi, A. Guermazi, and H. Trabelsi, "A clustering protocol for maximum coverage in large-scale wireless sensor networks," *International Journal of Business Data Communications and Networking*, vol. 11, no. 2, pp. 1–21, 2015.

[44] W. Jerbi, A. Guermazi, and H. Trabelsi, "O-LEACH of routing protocol for wireless sensor networks," in *2016 13th International Conference on Computer Graphics, Imaging and Visualization (CGiV)*, pp. 399–404, Beni Mellal, Morocco, 2016.

[45] W. Jerbi, A. Guermazi, and H. Trabelsi, "A novel clustering algorithm for coverage a large scale in WSN," http://arxiv.org/abs/1605.03079.

[46] W. Jerbi, A. Guermazi, and H. Trabelsi, "A routing protocol orphan-leach to join orphan nodes in wireless sensor network," in *Computer Science & Information Technology*, pp. 135–147, Chennai, India, 2016.

[47] W. Jerbi, H. Trabelsi, and A. Guermazi, "Equilibrate and minimize the energy consumption in a cluster for routing protocols in wireless sensor Network," *International Journal of Wireless Networks and Broadband Technologies*, vol. 5, no. 1, pp. 46–58, 2016.

[48] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, 2013.

[49] D. Gay, P. Levis, R. Von Behren, M. Welsh, E. Brewer, and D. Culler, "The nesc language : a holistic approach to networked embedded systems," *Acm Sigplan Notices*, vol. 38, 2003.

[50] P. Levis, S. Madden, J. Polastre et al., "Tinyos : an operating system for sensor networks," in *Ambient intelligence*, pp. 115–148, Springer, 2005.