A secure and energy saving protocol for wireless sensor networks

Aso Ahmed Majeed[1], Baban Ahmed Mahmood[2], Ahmed Chalak Shakir[3]
[1]Department of Parasitology, College of Veterinary Medicine, University of Kirkuk, Iraq
[2,3]Network Department, College of Computer Science and Information Technology, University of Kirkuk, Iraq

Article Info

Article history:

Received Jan 10, 2021
Revised Apr 26, 2021
Accepted Oct 4, 2021

Keywords:

Attack
Cryptography
Heterogenous WSN
Key management
Security

ABSTRACT

The research domain for wireless sensor networks (WSN) has been extensively conducted due to innovative technologies and research directions that have come up addressing the usability of WSN under various schemes. This domain permits dependable tracking of a diversity of environments for both military and civil applications. The key management mechanism is a primary protocol for keeping the privacy and confidentiality of the data transmitted among different sensor nodes in WSNs. Since node's size is small; they are intrinsically limited by inadequate resources such as battery life-time and memory capacity. The proposed secure and energy saving protocol (SESP) for wireless sensor networks) has a significant impact on the overall network life-time and energy dissipation. To encrypt sent messsages, the SESP uses the public-key cryptography's concept. It depends on sensor nodes' identities (IDs) to prevent the messages repeated; making security goals-authentication, confidentiality, integrity, availability, and freshness to be achieved. Finally, simulation results show that the proposed approach produced better energy consumption and network life-time compared to LEACH protocol; sensors are dead after 900 rounds in the proposed SESP protocol. While, in the low-energy adaptive clustering hierarchy (LEACH) scheme, the sensors are dead after 750 rounds.

Corresponding Author:

Baban Ahmed Mahmood
Department of Network
University of Kirkuk, Kirkuk, Iraq
Email: baban.mahmoodjaf@gmail.com

1. INTRODUCTION

Recently, the wireless sensor network (WSN) has been considered as a new processing technology. The WSN consists of hundreds of compact and tiny sensor nodes and has a wide range of applications such as home automation, traffic control, flood, tsunami, or earthquake detection, microclimates and monitoring for hazardous gases, and structural health monitoring. Also in terrain scanning, intelligent guiding, imaging, and battlefield surveillance, which are mean to enable monitoring and tracking of movements of vehicles and the presence of enemy forces. Commercial applications include inventory control, vehicle tracking and detection, and monitoring congestion and prevention of road accidents. Health applications include medical monitoring, behavior monitoring, elderly assistance, measurement of blood parameters, remote monitoring of physiological data, and wearable computing. Agriculture applications encompass humidity and temperature measurement, automatic control over water sprinklers, and precision agriculture. Also applications in smart furniture and space exploration, sound, and vibration [1], [2].

Since sensor nodes' sizes are small, the nodes are constraint with resources like energy, storage, processing capabilities, and available bandwidth [3], [4]. These nodes are distributed in environments which cannot be monitored or controlled with traditional networks especially, in military application. Moreover, the link in the network should be secure and strongly by encryption to put hacker's and intruders at bay [5]-[7]. Also, the encryption and decryption are done by the mathematics equation which is acceptable for the tiny nodes [8]. In WSN a data gathering causing high conservation of energy. In general, saving energy is done by eliminating redundant data in transmission which leads to reducing the number of exchanged messages among the nodes in the network [9].

Encryption is an effective method to protect data. While its techniques convert plaintext content into unreadable ciphertext [10], [11]. Here, In the network, a sent message is encrypted by the sender’s private key and receiver’s public-key. On the receiver side, a message is decrypted by the receiver's private key. On the other hand, in symmetric key cryptography, senders and receivers use the same shared key to encrypt and to decrypt messages. This means that both sender and receiver need a secure channel to exchange the shared or secret key between them. Furthermore, the hash function is another type of encryption that produces a fixed number of bits and this process is known as a message digest [5].

This paper proposes an efficient protocol called SESP which uses the public-key cryptography’s concept by depending on IDs to ensure a secure link between nodes. This leads to an increase in battery and network life-time. The sensors are vulnerable to various attacks because of their tiny and resource constraint which can not be uploaded by complex encryption methods. Consequently, the securing link between participating nodes and their energy conservation are challenging issues.

The rest of the paper is organized in the following order; section 2, we sum up several different algorithms given recently in the literature, section 3, the radio energy dissipation model is presented and its merits and demerits are shown, section 4, a comprehensive explanation of the proposed SESP protocol is presented, sections 5 and 6, security goal analysis and attacks' analysis are described respectively, section 7 concludes the paper.

2. RELATED WORK

WSNs comprise many sensor nodes (l) that can gather data and communicate wirelessly. Additionally, most WSNs include two other components, which are the cluster head (CH) and the base station (BS) [12]. The key management plays an essential role to solve issues such as authentication and authorization which are critical [1].

Zhu *et al*. [13] reckon that a scalable and distributed protocol is described that allows a shared key to be established by each pair of nodes. Moreover, two different protocol s, namely, threshold secret sharing and probabilistic key sharing are the basis of a protocol designed. The shared key is used for authentication between the two nodes. Furthermore, each node in this protocol should obtain its neighbors' identity (ID) to calculate the shared key. The node is loaded with a small fraction of the keys from the pool before deployment. Also, after distribution by using a probabilistic protocol (public and deterministic) that allows each pair of nodes, with a certain probability, to share one or more keys. Finally, every pair of nodes connected directly via one or more keys in their key sets, and in case of no shared key, the nodes connect indirectly through an intermediate node. The protocol guarantees connectivity, and because the message is repeated, the adversary can get the key and attacks the network by exhausting the energy of the sensor. Finally, the network will be hacked.

Huang *et al*. [12] improve the low-energy adaptive clustering hierarchy (LEACH) protocol by using hybrid nodes. The network encompasses of WSNs and a distributed fiber sensor link, which is positioned at the middle of the sensor field. The last one needs a steady and comparatively higher power supply. The authors isolate the network into two areas wherein the sensors have restricted energy. Moreover, there is no communication between the two areas. The node's life-time in this protocol is better than the LEACH protocol, but they did not talk about message encryption which makes the network insecure and vulnerable to attacks.

Heinzelman *et al*. [14] produce LEACH protocol, the nodes in the network are homogenous and each node can gather data and send it to the base station. After distribution, the sensors select themselves to become cluster head at a threshold, after which they distribute their status to the other nodes inside the network. The other nodes choose the CH sensor depending on minimal communication energy. Eventually, in LEACH, periodically, a group of nodes is selected as a cluster-based to guarantee that energy load is distributed evenly among the nodes of the different groups. This protocol needs message authentication to prevent the network from malicious nodes.

Rasul *et al*. [15] propose a key distribution scheme wherein random key pre-distribution is used such that better security and performance are achieved for a heterogeneous sensor network (HSN). On the other hand, a homogeneous network produces both high computation and communication overhead in addition to higher storage. The authors use a key pool, a small number of keys, to generate random keys. Key chains, that are made using a one way hash function, make a key pool. For each sensor node, a small number of generation keys that are randomly selected is assigned.

3. RADIO ENERGY DISSIPATION MODEL

The model in Figure 1 for the radio hardware energy distraction where the energy is dissipated by the transmitter to operate the power amplifier and the radio electronics [16]. Also, the energy is dissipated by the receiver to run the radio electronics as depicted in Figure 1.

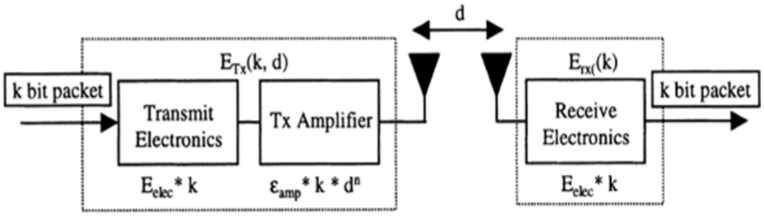


Figure 1. Radio energy dissipation model

In this scheme, based on the distance between the transmitter and receiver, the channel models multipath fading (d4 power loss) and free space (d2 power loss) were used. Sensors spend energy to transmit and receive k bits packet (length of message) to a distance *d* as described as shown in:

$$\begin{aligned} E_T &= E_{Tx\text{-}elec}(l)+E_{Tx\text{-}amp}(l,d) \\ &= lE_{elec}+l\epsilon_{fs}\,kd^2 \qquad d<Do \\ &= lE_{elec}+l\epsilon_{mp}\,kd^4 \qquad d\geq Do \end{aligned} \tag{1}$$

This loss can be inverted using power control when the power amplifier is properly configured. When the distance is lower than a predefined threshold, the free space model is considered; otherwise, the multipath model is utilized [16]. The energy of the electronics, E_{elec}, depends on different factors such as modulation, filtering, digital coding, and spreading of the signal. On the other hand, the energy of the amplifier, $\epsilon_{fs}*d^2$ or $\epsilon_{mp}*d^4$, depends on a sufficient bit-error-rate and the distance between the transmitter and receiver. The parameters for the energy of the communication are E_{elec}=50 nJ/bit,$\in_{fs}$=10 pJ/bit/m^2, $\in_{mp}$=0.0013pJ/bit/m4. However, the data aggregation energy is E_{DA}=5 nJ/bit/signal and the threshold distance value Do is given as shown in [16]:

$$Do = \sqrt{\frac{E_{fs}}{E_{amp}}} \tag{2}$$

The proposed SESP protocol uses the radio energy dissipation model because it uses less energy than the LEACH protocol.

4. PROPOSED SESP PROTOCOL

This paper proposes a MAC formula for key management that is designed for hierarchical WSNs. each cluster head (CH) and sensor (L) has their IDs in hierarchical WSN. Besides, only the CH can communicate with base station (BS), the L sensors can communicate with CH, and L sensors cannot communicate with each other's [17].

In the network, the CHs have high power, large memory capacity, and great process capability. However, the L sensors are normal (restricted energy and memory size) [5], [18]. The distribution area is (100 x 100) m^2, number of CHs are two with 100 L sensors which are scattered randomly in the uncontrolled area [19], [20], the circles are L sensors, pink rectangles are CHs sensors and the green star is BS as shown in Figure 2. There are no power restrictions for the BS, high storage capacity, and larger communication [5], [18], while the power consumption has to be highly reserved for the scattered nodes to keep the life-time of the network as long as possible and position in a safe area. The L sensors' costs are cheaper than CH and that is due we use two CHs, and in case of increases in the CHs, the cost will increase. Moreover, when using large areas, we can increase the number of CHs and BS.

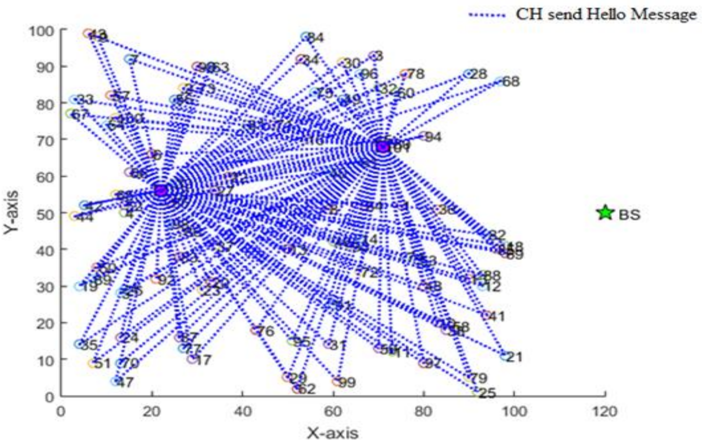


Figure 2. CHs send hello message

4.1. Network setup

4.1.1. Pre-distribution phase

In this part, the initialization and authentication start including the equations needed for communication taking into consideration the following assumptions:

- The network area is 100 x 100 m^2.
- CH directly links with BS and it has the IDs of all Ls and BS.
- L sensors have the CHs IDs which are two and L nodes are 100.
- BS exchanges the messages with L sensors via CH and vice versa.
- L sensors' initial energy is 0.5J.

4.1.2. Distribution phase

After random deployment, each CH broadcasts a hello message as shown in Figure 2 and Figure 3 where ID$_{CH}$ is the identification of the cluster head, || is an append operation, ⊕ is an XOR operation, K∈G is an integer number that starts with one and increased by one in each round to prevent message redundancy, and *i* is the sensor number.

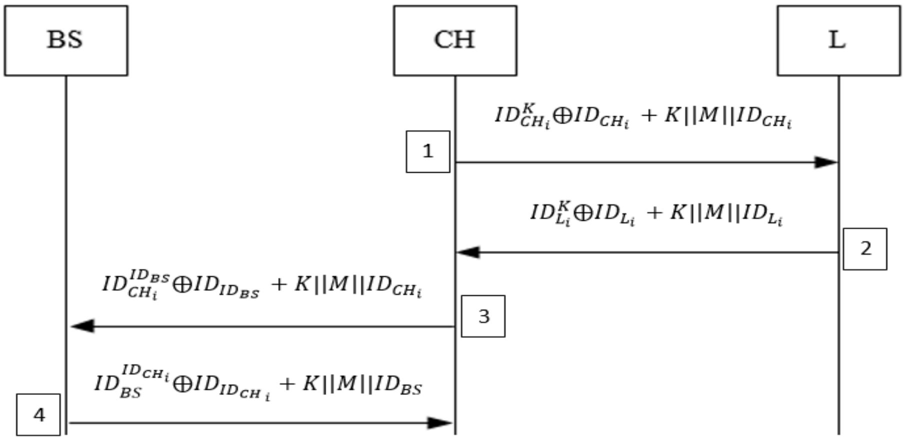

BS
CH
L
1
$ID_{CH_i}^{K} \oplus ID_{CH_i} + K||M||ID_{CH_i}$
2
$ID_{L_i}^{K} \oplus ID_{L_i} + K||M||ID_{L_i}$
3
$ID_{CH_i}^{ID_{BS}} \oplus ID_{ID_{BS}} + K||M||ID_{CH_i}$
4
$ID_{BS}^{ID_{CH_i}} \oplus ID_{ID_{CH_i}} + K||M||ID_{BS}$

Figure 3. The SESP protocol

In step 2, each L receives more than one message from different CHs and chooses the strongest CH's signal after decrypting the message according to Figure 4 [21]. Moreover, the L sensor sends an encrypted message to selected CH consists of its ID as shown in Figure 4. The dotted green line represents near Ls to CH spends energy according to (1) when *d<D0* and the dotted orange line considers the far Ls from CH which spends energy according to (1) when *d>=D0*.Figure 4. The SESP protocol.

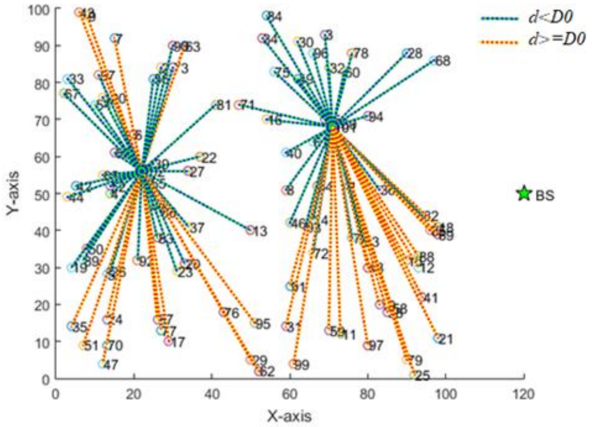


Figure 4. L sensors select the near CH

In step 3, each CH decrypts the Ls message and identifies the legal node via preloaded ID, then creates its cluster and joins the BS as shown Figure 5. In step 4, the BS sends an acknowledgment to each CH according to Figure 6 and leads to complete the network. Moreover, the message is encrypted and decrypted using a protocol shown in Figure 7. In the proposed SESP protocol, nodes select their respective CHs according to the signal ratio from the node that announces itself as CH. Data aggregation is executed by CH, thus CH nodes consume relatively much more energy than member nodes. Calculation of energy dissipated is performed based on distance.

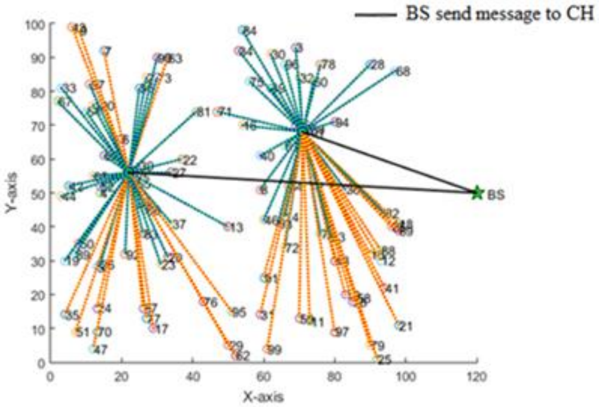


Figure 5. CHs send a message to BS

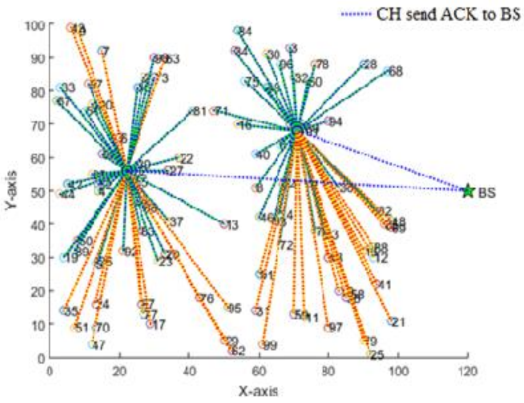
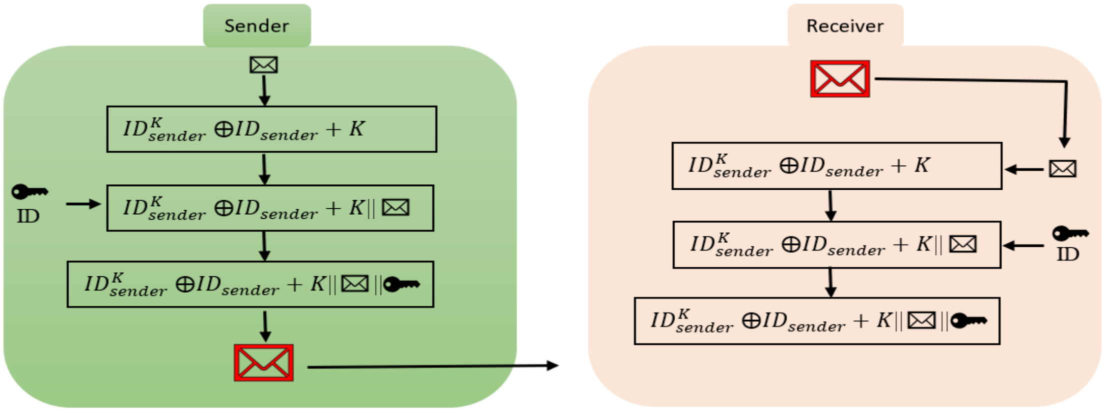


Figure 6. The proposed network



Sender
$ID^K_{sender} \oplus ID_{sender} + K$
ID
$ID^K_{sender} \oplus ID_{sender} + K ||$ ✉
$ID^K_{sender} \oplus ID_{sender} + K ||$ ✉ $||$ 🔑
Receiver
$ID^K_{sender} \oplus ID_{sender} + K$
$ID^K_{sender} \oplus ID_{sender} + K ||$ ✉
ID
$ID^K_{sender} \oplus ID_{sender} + K ||$ ✉ $||$ 🔑

Figure 7. Message encryption and decryption

5. SECURITY GOALS ANALYSIS

The security goals' analysis is the main part of the proposed SESP protocol as given as shown in:

- Authentication: each node in the proposed SESP protocol has a unique key (ID). The sender encrypts its message by its ID in a formula. Besides, the receiver authenticates the received message by the ID of the sender.
- Confidentiality: messages in the proposed protocol is encrypted via an equation: the ID of each sensor remains secret from the enemy by embedding it in the formula. Moreover, it is not repeated.
- Integrity: the proposed SESP protocol protects the received messages from alteration and modification by using an embedded ID in the formula described above in the proposed protocol.
- Availability: the network in the proposed SESP protocol is survived until the nodes spend their energy. Further, the messages are updated in each round.
- Freshness: this goal is achieved because first, the messages exchanged are fresh, and second, the resending of old data is avoided using a counter in the formula.
- Resilience: if an attacker compromises the CHs, then he/she can hack the network. Besides, if the attacker compromises Ls, he/she can hack only this cluster.

Besides, Table 1 shows the comparison between the proposed SESP protocol and the protocols presented in the literature in terms of security goals according to reference [22].

Table 1. Comparison according to security goal

Requirements	Proposed SESP Protocol	Protocol [23]	Protocol [24]	Protocol [25]
Authentication	✓	✓	✓	✓
Confidentiality	✓	×	×	×
Integrity	✓	✓	×	×
Scalability	✓	×	✓	✓
Resilience	×	×	×	×
Cryptographic mechanism	✓	✓	✓	✓

6. ATTACKS ANALYSIS

The proposed SESP method is effective versus different attacks as explained as shown in:

- Eavesdrops attack: the proposed SESP protocol is resistant to this attack because the attacker catches the signals. However, he/she cannot determine what the message includes because the message's contents are a stream bit of numbers, which makes the message non-understandable.
- Sybil attack: this does not influence the network of the proposed SESP protocol because the nodes' IDs are embedded in a formula.
- Sinkhole attack: the nodes in the proposed SESP protocol decrypt the messages according to the formula supplied in pre-distribution. Therefore, the attacker's messages will be canceled.
- Wormhole attack: the attacker work to make a tunnel and change the network route. The attacker doesn't affect our network unless he/she gains the formula.
- Hello flood attack: the proposed SESP protocol is resistant to this attack because the nodes in the proposed SESP protocol have the BS's ID which is embedded in a formula, and recognize the illegitimate BS.
- Clone attack: the intruder can attack and hack the network of the proposed SESP protocol.

Table 2 shows the comparison between the proposed SESP protocol and other protocols presented in the related work in terms of security goals according to this reference [15]. Furthermore, Figure 8 shows the life-time of the sensors. We can see that the proposed SESP protocol is satisfied in terms of the death and life of sensors. The sensor is dead after 750 rounds in the LEACH protocol. while, in the proposed SESP protocol, the sensors are dead after 900 rounds; due to the use of the model in section (3 radio energy dissipation model). Further, Figure 9 shows the total dissipated energy for all the sensors to propose SESP protocol is better than LEACH protocol. due to the use of the model in section (3 radio energy dissipation model). Finally, the simulation of the proposed SESP protocol that was done by MATLAB R2015a shows that the proposed SESP protocol is better than LEACH.

Table 2. Comparison according to attack in WSN.

Protocol Attack	Protocol [26]	Protocol [27]	Proposed SESP protocol
Eavesdropping	×	×	✓
Hello flood	×	✓	✓
Worm-hole	✓	✓	✓
Sinkhole	✓	✓	✓
Sybil	✓	×	✓
Clone attack	×	×	×

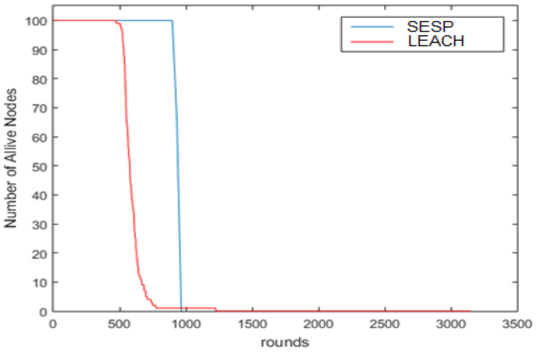


Figure 8. Number of nodes alive in proposed SESP protocol vs LEACH in round

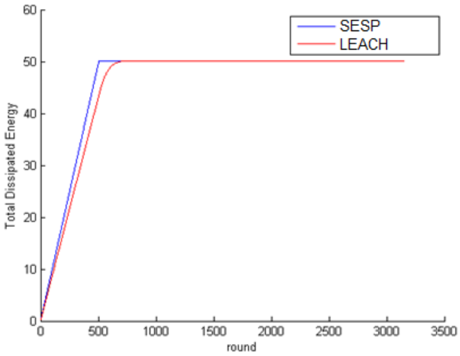


Figure 9. Total dissipated energy of proposed SESP protocol vs LEACH in round

7. CONCLUSION

The proposed SESP protocol is based on a hierarchical network. Nodes in the network establish a secure link through a protocol constructed based on public-key cryptography principles wherein, the ID is considered as a public-key and the formula as a private key. The message in the proposed SESP protocol is encrypted and never repeated in the network (i.e., no other sensor sends a message that was sent by other sensors). İn each round, there are new messages different from the messages either in the previous and/or the next round. That makes the proposed SESP protocol attain security goals like authentication, confidentiality, integrity, availability, and freshness. Moreover, the proposed SESP protocol is resistant to various attacks mentioned above in the attack analysis. Finally, the simulation produced better energy consumption, dissipated energy, network life-time, and better security goals compared to the leach.

REFERENCES

[1] R. Priyadarshi, B. Gupta and A. Anurag, "Deployment techniques in wireless sensor networks: a survey, classification, challenges and future research issues," *The Journal of Supercomputing*, Springer, vol. 76, pp. 1-41, 2020, doi: 10.1007/s11227-020-03166-5.

[2] B. A. Mahmood and D. Manivannan, "Position based and hybrid routing protocols for mobile ad hoc networks: a survey," *Wireless personal communications*, vol. 83, no. 2, pp. 1009-1033, 2015, doi: 10.1007/s11277-015-2437-8.

[3] L. Tawalbeh, S. Hashish and H. Tawalbeh, "Quality of service requirements and challenges in generic WSN infrastructures," *Procedia Computer Science*, vol. 109, pp. 1116-1121, 2017, doi: 10.1016/j.procs.2017.05.441.

[4] E. H. Putra, R. Hidayat, Widyawan and I. W. Mustika, "Energy-Efficient Routing Based on Dynamic Programming for Wireless Multimedia Sensor Networks (WMSNs)," *International Journal of Electronics and Telecommunications*, vol. 63, no. 3, pp. 279-283, 2017, doi: 10.1515/eletel-2017-0037.

[5] A. A. Majeed, "Cluster forming based on spatial information using HMAC in WSN," *Tikrit Journal of Pure Science*, vol. 22, no. 6, pp. 131-139, 2017.

[6] B. A. Mahmood and D. Manivannan, "GRB: Greedy Routing Protocol with Backtracking for Mobile Ad-Hoc Networks," in *IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*, 2015.

[7] B. Mahmood, A. Ibrahim and D. Manivannan, "Sariadne: A secure source routing protocol to prevent hidden-channel attacks," in *IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob),* 2016, doi: 10.1109/WiMOB.2016.7763267.

[8] A. A. Majeed, K. A. Ameen, A. C. Shakir and Y. Alyeksyeyenkov, "The Enhanced Data Sequence Method for ECC Cryptosystem," *Applied Mathematical Sciences*, vol. 8, no. 112, pp. 5553-5564, 2014.

[9] K. N. S. Kumar and Shivashankar, "A review on security and privacy issues in wireless sensor networks," *in 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT),* 2017, doi: 10.1109/RTEICT.2017.8256945 .

[10] H. R. Zagi and A. T. Maolood, "A Novel Serpent Algorithm Improvement By The Key Schedule Increase Security," *Tikrit Journal of Pure Science*, vol. 6, pp. 114-125, 2020, doi: 10.25130/j.v25i6.1078.

[11] B. A. Mahmood and D. Manivanann, "Hybrid on-demand greedy routing protocol with backtracking for mobile ad-hoc networks," *International Journal of Pervasive Computing and Communications,* vol. 16, no. 1, pp. 24-52, 2020.

[12] J-Y Huang, I-E Liao and H-W Tang, "A forward authentication key management scheme for heterogeneous sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, no. 1, p. 296704, 2011.

[13] S. Zhu, S. Xu, S. Setia and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach," *11th IEEE International Conference on Network Protocols, 2003. Proceedings.*, 2003, pp. 326-335, doi: 10.1109/ICNP.2003.1249782.

[14] 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*, 2000, doi: 10.1109/HICSS.2000.926982.

[15] K. Rasul, N. Nuerie and A. K. Pathan, "An Enhanced Tree-Based Key Management Scheme for Secure Communication in Wireless Sensor Network," in *IEEE 12th International Conference on High Performance Computing and Communications (HPCC),* 2010, doi: 10.1109/HPCC.2010.14.

[16] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," in *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660-670, Oct. 2002, doi: 10.1109/TWC.2002.804190.

[17] D. N. Ravikiran and C. G. Dethe, "Improvements In Routing Algorithms to Enhance Lifetime of Wireless Sensor Networks," *International Journal of Computer Networks & Communications (IJCNC*), vol. 10, no. 2, pp. 23-32, 2018, doi: 10.5121/ijcnc.2018.10203.

[18] J. Sumathi and R. L. Velusamy, "A review on distributed cluster based routing approaches in mobile wireless sensor networks*," J Ambient Intell Human Comput.*, vol. 12, pp. 835-849, 2021, doi: 10.1007/s12652-020-02088-7.

[19] J. Shen, A. Wang, C. Wang, P. C. K. Hung and C. Lai, "An Efficient Centroid-Based Routing Protocol for Energy Management in WSN-Assisted IoT," in *IEEE Access*, vol. 5, pp. 18469-18479, 2017, doi:10.1109/ACCESS.2017.2749606.

[20] S. G. Susila and J. Arputhavijayaselvi, "Innovative Energy Resourceful Merged Layer Technique (MLT) of Node Deployment to Enhance the Lifetime of Wireless Sensor Networks," *Egyptian Informatics Journal*, vol. 16, no. 1, pp. 23-28, 2015, doi: 10.1016/j.eij.2014.11.002.

[21] K. Haseeb, I. Ud Din, A. Almogren and N. Islam, "An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture," *Sensors*, vol. 20, no. 7, pp. 1-14, 2020, doi: 10.3390/s20072081.

[22] O. Cheikhrouhou, A. Koubâa, M. Boujelben and M. Abid, "A lightweight user authentication scheme for Wireless Sensor Networks," in *ACS/IEEE International Conference on Computer Systems and Applications-AICCSA*, 2010.

[23] Z. Benenson, F. Gärtner and D. Kesdogan, "User Authentication in Sensor Networks," *Computer Science Connects*, vol. 2, pp. 385-389, 2004.

[24] C. Jiang, B. Li and H. Xu, "An Efficient Scheme for User Authentication in Wireless Sensor Networks," in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*, 2007.

[25] H. Tseng, R. Jan and W. Yang, "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks," in *IEEE GLOBECOM 2007-IEEE Global Telecommunications Conference*, 2007.

[26] S. Hussain, F. Kausar and A. Massood, "An efficient key distribution scheme for heterogeneous sensor networks," in *international conference on Wireless communications and mobile computing,* ACM, August 2007.

[27] B. Maala, H. Bettahar and A. Bouabdallah, "TLA: A Tow Level Architecture for Key Management in Wireless Sensor Networks," in *Second International Conference on Sensor Technologies and Applications*, 2008.

BIOGRAPHIES OF AUTHORS

Aso Ahmed Majeed is currently an instructor at University of Kirkuk Kirkuk, Iraq. He received a B.Sc. in software engineering from Technical College, Kirkuk, Iraq in 2004 and M.Sc. in Computer Engineering from Cankaya University, Ankara, Turkey in 2015. He published his research in the following areas: computer networks, security in wireless sensors network, and AI.

Baban Ahmed Mahmood is currently the chairman of Networks Department at University of Kirkuk, Kirkuk, Iraq. He received a B.Sc., degree in Computer and Software engineering from University of Al-Mustansryah, Iraq, in 2003 and a M.Sc., degree in Computer Science from University of Sulaimaniya, Iraq, in 2009. He received a PhD degree in Computer Science from University of Kentucky, Lexington, Kentucky, USA 2016. He worked in the program of some international conferences. He reviewed many papers for several prestigious journals and conferences. He published his research work in the following areas: routing in ad hoc networks, security of source routing protocols in MANET, and security of health records via cloud.

Ahmed Chalak Shakir is currently the dean of the College of computer science and information technology, University of Kirkuk, Iraq. He received a B.Sc, degree in Computer and Software Engineering from University of Al-Mustansryah, Iraq, in 2001. In 2002 he got a High Diploma degree in software engineering from Iraqi commission for computers & informatics/ Institute for post graduate studies in informatics, Bagdad, Iraq, and a M.Sc., degree in Computer Science from University of Sulaimaniya, Iraq, in 2007. He also received a PhD degree in Computer Engineering, Harbin institude of technology, china in 2013. He published his research work in the following areas: information and network security.