

# A novel secure and energy aware LOADng routing protocol for IoT: an application to smart agriculture

Touhami Sana<sup>1,2</sup>, Belghachi Mohamed<sup>1</sup>

<sup>1</sup>Department of Mathematics and Computer Science, Faculty of Exact Sciences, Tahri Mohamed University, Bechar, Algeria

<sup>2</sup>Laboratory of LTIT, Tahri Mohamed University, Bechar, Algeria

## Article Info

### Article history:

Received May 15, 2024

Revised Sep 17, 2024

Accepted Sep 29, 2024

### Keywords:

Energy efficiency

Hello flood attack

Internet of things

LOADng routing protocol

Security

## ABSTRACT

In the burgeoning domain of the internet of things (IoT), efficient and secure communication protocols are crucial for the seamless operation of diverse applications. This paper proposes a novel routing protocol, termed secure and energy aware LOADng (SEA-LOADng), tailored for IoT deployments in the context of smart agriculture. The protocol is designed to address the unique challenges posed by agricultural environments, including limited energy resources and the need for robust security measures. The proposed protocol leverages LOADng, a lightweight and efficient routing protocol suitable for low-power and lossy networks characteristic of IoT deployments. Through innovative energy-aware mechanisms, it optimizes the power usage of IoT devices, thus prolonging their operational lifespan and reducing maintenance overhead. Moreover, stringent security measures are integrated into the protocol to safeguard sensitive data transmitted within the IoT network. To assess the efficacy of the proposed protocol, comprehensive simulations are carried out using realistic smart agriculture scenarios. The results demonstrate significant improvements in energy efficiency compared to LOADng protocol, while maintaining robust security against hello flood attack.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Touhami Sana

Department of Mathematics and Computer Sciences, Faculty of Exact Sciences

Tahri Mohamed University

Kenadsa Street, Bechar, Algeria

Email: touhami.sana@univ-bechar.dz

## 1. INTRODUCTION

The internet of things (IoT) [1] refers to a system of linked devices that gather data, manipulate actuators, and monitor networks. The rapid expansion of the IoT has catalyzed innovation across various domains, ranging from healthcare and transportation to homes cities and factories. Among its myriad applications, smart agriculture stands out as a critical domain where IoT technologies are revolutionizing traditional farming practices [2] as shown in Figure 1. By deploying sensors to manage water consumption, optimize pesticide and fertilizer usage, and collect data on soil and air quality through the use of sophisticated algorithms and machine learning methods, companies are transforming agriculture into a data-driven, precision-oriented industry.

Smart agriculture offers farmers a suite of tools to address the multifaceted challenges they face, enabling remote monitoring and management of agricultural processes. With IoT devices installed across farmlands, farmers can stay connected and make informed decisions from anywhere and at any time [3], [4]. This connectivity not only enhances operational efficiency but also has the potential to reduce production costs and increase productivity by providing instant insights into soil conditions, water availability, and environmental parameters [5], [6].

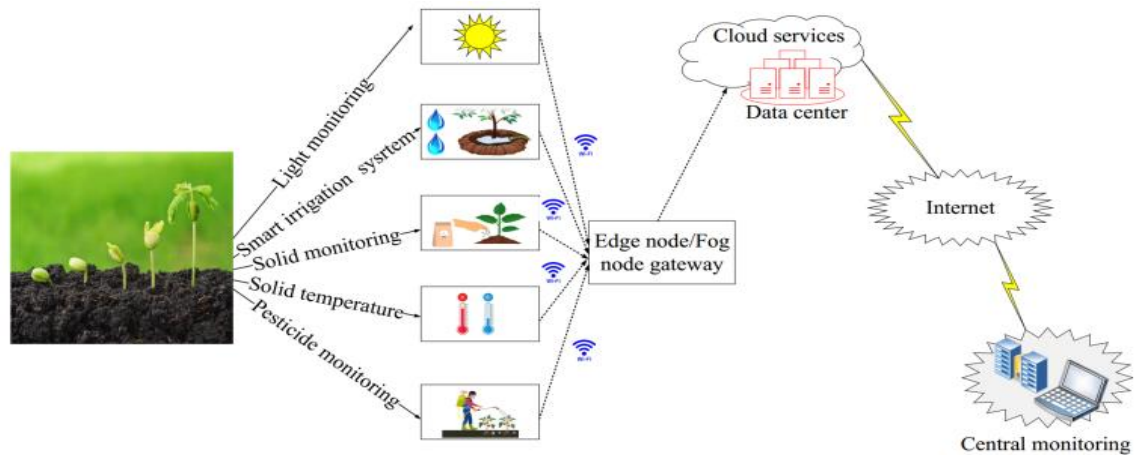


Figure 1. IoT in smart agriculture

However, the broad implementation of IoT in smart farming introduces challenges related to routing and secure data transmission. IoT devices often have resource constraints, including limited computing power, memory, and energy [7]-[9]. Thus, any secure routing method needs to be both lightweight and efficient in order to accommodate these constraints [10]-[12]. The lightweight on-demand ad hoc distance-vector routing protocol next generation (LOADng) is a widely adopted and effective routing protocol specifically designed for 6LoWPAN networks [13].

Recently, numerous studies have been conducted on communication security [14] and energy efficiency [15], [16] in IoT networks separately, achieving both simultaneously remains a challenge [17]-[19] due to their inverse relationship [20], [21]. Robust security mechanisms typically consume significant energy, which is a valuable resource for many IoT nodes.

In response to these challenges, this paper proposes a novel secure and energy-aware LOADng (SEA-LOADng) routing protocol tailored specifically for IoT networks deployed in agricultural settings. SEA-LOADng aims to strike a balance between energy conservation and data security, addressing the unique requirements of smart agriculture. By integrating adaptive routing mechanisms, SEA-LOADng optimizes energy utilization while ensuring reliable communication among IoT devices.

Furthermore, SEA-LOADng incorporates robust security features to protect sensitive agricultural data from hello flood attacks, a common security threat in IoT networks. By leveraging the number of Route REQuests (RREQs) sent by a node, the protocol enhances the security of data transmissions within the IoT network.

The remainder of the paper is organized as follows: Section 2 provides a literature review. Section 3 gives a brief overview of the LOADng routing protocol. Section 4 examines the Hello Flood attack. Section 5 details the proposed approach, while section 6 discusses the results and analysis. Finally, section 7 presents the conclusion.

## 2. RELATED WORKS

Hasseb *et al.* [22] introduced a wireless sensor network (WSN) that utilizes IoT technology framework tailored for smart agriculture. This framework encompasses various design stages. Initially, farming sensors collect pertinent data and identify cluster heads (CH) through a decision function with multiple criteria. Furthermore, the framework employs signal-to-noise ratio (SNR) is used to evaluate signal quality on transmission channels, ensuring reliable and efficient data transfer. Additionally, security measures are put in place to protect data sent from farming sensors to base stations (BS), including the use of recurrence from a linear congruential generator.

Hosseinzadeh *et al.* [14] proposed a secure routing approach based on cluster-tree architecture utilizing the dragonfly algorithm (CTSRD) for IoT networks. Their scheme introduces a lightweight trust mechanism named weighted trust (W-Trust), which operates in a distributed manner. W-Trust employs a penalty coefficient to diminish the trust value associated with malicious nodes, effectively isolating them within the network. Conversely, it enhances the trustworthiness of genuine IoT devices by employing a reward factor. Moreover, CTSRD incorporates a clustering process based on trust termed T-Clustering, where the cluster head nodes (CHs) are chosen from among trustworthy IoT nodes. Subsequently, CTSRD

establishes a routing tree, referred to as DA-Tree, between CHs based on the dragonfly algorithm (DA). To assess the effectiveness of the routing tree, CTSRD presents an innovative fitness function. DA-Tree is created to provide a secure, stable, and optimal routing setup, with the goal of balancing energy consumption and extending network lifespan. The performance of CTSRD is evaluated against existing methods, EEMSR and E-BEENISH, across various metrics including network longevity, energy use, and packet delivery rate.

Jain *et al.* [15] introduces a routing model specifically tailored for agricultural data in IoT-based WSNs, with a focus on enhancing energy and bandwidth efficiency. This model operates through clusters and emphasizes the selection of CH for data aggregation. A new method, the chaos mapping and opposition-centered learning grasshopper optimization algorithm (CO2GA), is used to identify the optimal set of CHs from the agricultural sensor nodes (SN). Clustering is then based on the proximity between the selected CH and SN. Data is gathered by the clusters and sent to their respective CHs, where it is encrypted using the chaos key generated advanced encryption standard with Rivest–Shamir–Adleman (CKAES-RSA) algorithm. The encrypted IoT data is then routed to BS or sink nodes (SN) through an optimal routing path. The paper also proposes an optimal route selection (ORS) strategy using a deep learning (DL) approach, specifically a crossover and mutation-based optimal Multi-Layer Perceptrons (CM-OMLP), which evaluates the effectiveness of the hidden layer concerning energy, bandwidth, trust, delay, and congestion levels.

Sankar *et al.* [16] introduced the energy-aware grid-based data aggregation scheme in routing (EGDAS-RPL) protocol was introduced for IoT networks with the goal of extending network lifespan. The protocol consists of three main processes: forming grids, selecting grid heads (GH), and choosing GH parents. Initially, EGDAS-RPL divides the network into equally sized grids within a square topology. It then uses a probabilistic approach to select the GH node for each grid. Lastly, it applies the expected transmission count (ETX) metric to identify the optimal GH parent for data transmission.

### 3. LOADNG OVERVIEW

The LOADng protocol, also known as Lightweight on-demand ad hoc distance vector routing protocol-next generation, is a reactive routing protocol designed for WSNs. It represents a streamlined version of the ad hoc on-demand routing protocol AODV, which was initially created for use in devices based on IEEE 802.15.4 in 6LoWPANs and LLNs [23]. LOADng can serve as either a layer 3 route-over routing protocol or as a layer 2 mesh-under protocol. Consequently, the algorithm of LOADng stands out for its straightforwardness and minimal storage of data requirements. Therefore, it is considered an excellent and appropriate solution for advanced metering infrastructure (AMI) mesh networks [24], [25]. As it was initially crafted for WSNs and low power and lossy networks (LLNs), adjustments are necessary to align with their particular requirements and constraints.

LOADng specifies four categories of packets [26]:

- Route request (RREQ): Initiated by a router, known as the <originator>, when there is an available data packet for a destination, but no valid route has been established. The RREQ includes the particular destination address.
- Route reply (RREP): Created by a router after receiving and handling a RREQ, integrating the destination address into its routing table.
- Route reply acknowledgement (RREP-ACK): Produced by a LOADng router upon receiving a RREP, Informing the adjacent sender of the RREP that it has been effectively received.
- Route error (RERR): Produced by a router when it detects a broken route to the destination.

LOADng incorporates the fundamental features of AODV, such as generating and sending RREQ packets, as shown in Figure 2, to establish a path to a specific destination.

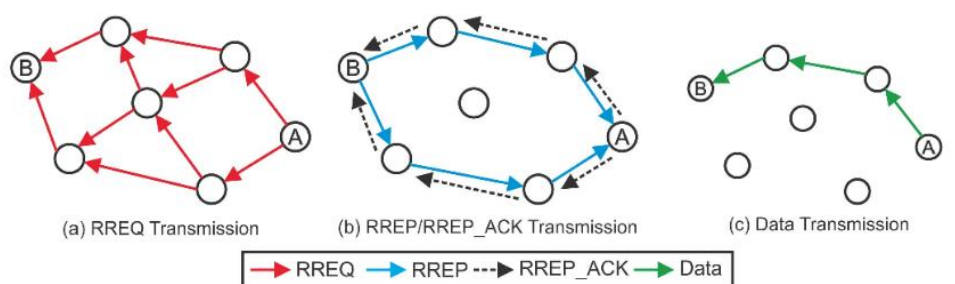


Figure 2. The operation of LOADng and its utilization of control messages

Upon receiving this message, only the designated node (terminator) is able to respond with a RREP, as shown in Figure 2. The RREP is then sent sequentially through each hop to reach the source. When intermediate nodes get the RREP, they send an RREP-ACK to the neighboring node that provided the RREP, confirming the bidirectional nature of the link. If a broken route is detected, an error message may be sent back to the data packet's source. Unlike AODV, LOADng restricts intermediate nodes from generating RREPs, which helps reduce the size of control messages—an important consideration in LLNs.

In LOADng, sequence numbers are not required in messages sent to requesting routers. Furthermore, LOADng does away with Gratuitous RREP. Instead, if an intermediate node has a valid route to the destination, it sends a unicast RREP to the source and notifies the destination through this message. This approach reduces message size, which is in line with the low-power and memory constraints of LLNs.

In contrast, nodes employing the LOADng protocol does not keep a precursor list with the IP addresses of neighboring nodes expected to be the next hop toward each destination, as seen in the AODV protocol. Instead, they concentrate solely on determining the next hop for sending the current packet to its destination. Additionally, unlike AODV, LOADng control messages can incorporate Type-Length-Value (TLV) elements, which allow for the expansion of protocol functionalities.

#### 4. HELLO FLOOD ATTACK

In a HELLO flood attack, an adversarial node takes advantage of its high transmission power to send, record, or repeat HELLO messages, creating a false impression of being a neighbor to multiple nodes in the network. This leads to significant confusion in network routing. This attack exploits protocols that use broadcast Hello messages to announce their presence as shown in Figure 3. By using a transmission range greater than other nodes, the attacker can flood a large area of the network with multiple Hello messages [27]. As a result, other nodes erroneously perceive the attacker as a neighboring node. Consequently, all nodes respond to these erroneous messages, draining their energy and causing network confusion.

In the LOADng protocol, there is a vulnerability where an adversarial node can exploit the network by sending an excessive number of RREQ messages within a short time period. These RREQs are targeted towards a destination node that cannot be reached due to an unavailable address. Since the destination node cannot be reached, the RREQ messages continue to propagate throughout the network without ever receiving a RREP message [28].

This flood of RREQ messages overwhelms the network and has detrimental effects, particularly on the nodes' battery life. As the nodes continuously process and forward these unnecessary RREQ messages, their energy resources are rapidly depleted. This battery depletion significantly impacts the overall functioning and efficiency of the network [28]. By exploiting this vulnerability in the LOADng protocol, a malicious node can disturb the regular functioning of the network, drain the batteries of nodes, and potentially cause network instability or failure.



Figure 3. Hello flood attack

#### 5. PROPOSED METHOD

Many researchers have utilized IoT technology across various fields to monitor environmental data. IoT has been crucial in observing and managing agricultural land, including crops, climate, and water usage. However, agriculture still faces challenges such as energy efficiency, data routing, and security because of the restricted battery life of sensors and the open transmission medium.

LOADng [13] is a routing protocol that facilitates data transfer between nodes and represents a significant advancement in IoT routing. Known for its lightweight design and suitability for resource-

constrained environments, LOADng has been recognized as an effective solution for IoT network routing. However, LOADng is vulnerable to several attacks, including the Hello flood attack, where a malicious node can disrupt the network by sending an excessive number of RREQ messages in a short time. This flood of RREQ messages can overwhelm the network, especially impacting the battery life of the nodes.

The pursuit of enhanced security has driven researchers to explore new methodologies. To address this, we developed SEA-LOADng, a Secure and Energy Aware version of LOADng, to protect agricultural data from Hello flood attacks. We introduce security measures specifically designed to counter these attacks in the agricultural sector. This paper proposes a detection solution based on the number of RREQ messages transmitted by a node.

In LOADng, when a node wants to send data to another node, it sends a RREQ message. A node can send up to three consecutive Hello messages to check if a link is faulty. In such cases, the node is not considered an attacker; it simply wants to verify the link status. Therefore, we assume that a node can transmit a maximum of three RREQ messages within a specific time interval. If a node exceeds this limit, it will be classified as an attacker in our scenario. Algorithm 1 in the paper presents the pseudocode for the attack detection process.

#### Algorithm 1. Identification of Hello Flood Attack

```

Inputs: RREQ_number
Output: Attack Determination (yes or no)
For each node that receives RREQ message do
  If (RREQ_number > 3) then
    The request is discarded
  Else
    The request is accepted
  End If
End For

```

## 6. RESULTS AND DISCUSSION

This research centers on implementing and evaluating our suggested approach using the Cooja simulator, which is built on the Contiki OS tailored for IoT sensor nodes. In our simulations, we utilize the Z1 mote as both server and client nodes. The simulations are conducted for a duration of 15 minutes, and we employ the unit disk graph medium (UDGM) model to replicate distance-based signal loss in the radio medium. To ensure consistency, we manually position 5, 10, 15, 20, 25, and 30 nodes. The deployment of LOADng is implemented through the Contiki rime stack. The parameters used for the simulations are outlined in Table 1 for reference.

To evaluate the effectiveness of our proposed method, we have focused on three key metrics: Received packets, expected transmission count (ETX), and Energy consumption. These metrics have been selected to assess and analyze the performance of our method.

Parameters	Value
Operating system	Contiki 3.0
Simulator	Cooja
Radio model	UDGM: Distance loss
Mote type	Z1 mote
Nodes Number	5,10,15,20,25,30
Couche Mac	CSMA
Couche RDC	Contikimac
Channel check rate	8 Hz
Network stack	Rime
Simulation time	15 minutes

### 6.1. Received packets

Received packets represent the quantity of data packets that have been successfully received within a communication system or network. This metric evaluates the efficiency and reliability of data transmission and reception. The count of received packets offers valuable information regarding the performance of the communication process. By examining the received packets, it becomes possible to assess the reliability of the transmission link, detect any instances of packet loss or interference, and evaluate the overall effectiveness of the system.

Based on the results shown in Figure 4, it can be observed that the SEA-LOADng protocol surpasses LOADng in terms of received packets in all tested scenarios. This comparison indicates that the SEA-

LOADng protocol exhibits superior efficiency and reliability in receiving data packets when compared to the LOADng protocol. The enhanced performance of the SEA-LOADng protocol in receiving packets underscores its potential in improving the overall effectiveness of the communication system or network.

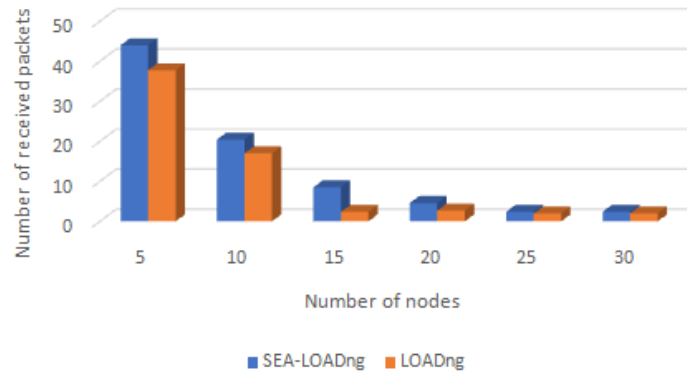


Figure 4. Comparison of number of received packets

## 6.2. ETX

ETX refers to the expected number of transmitted packets required for successful reception, with a focus on seeking higher quality links over a specific timeframe. However, relying solely on ETX is insufficient for assessing network conditions. Therefore, it becomes necessary to incorporate additional metrics to monitor the dynamic nature of both link and node situations. ETX is computed following to (1):

$$ETX = 1 / (DF * DR) \quad (1)$$

where DF stands for forward data delivery and DR stands for reverse data delivery.

Figure 5 presents a comparison of ETX values. The findings demonstrate that the SEA-LOADng protocol outperforms LOADng in terms of expected transmissions (ETX) across all tested scenarios. This indicates that the SEA-LOADng protocol exhibits more efficient and reliable packet transmission behavior in comparison to LOADng. These results suggest that the SEA-LOADng protocol offers advantages in terms of packet transmission reliability and resource utilization over the LOADng protocol.

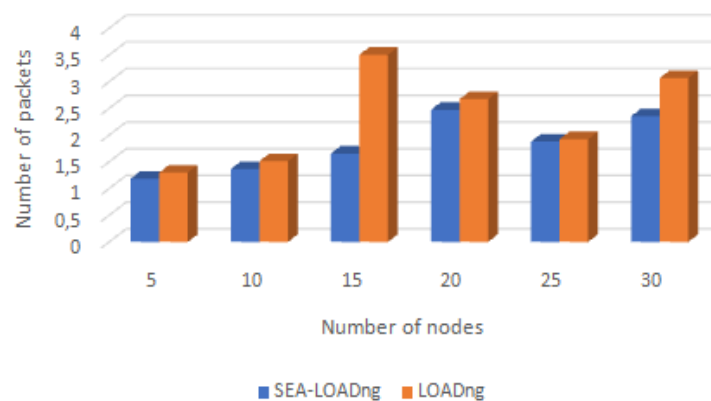


Figure 5. ETX comparison

## 6.3. Energy consumption

The (2) represents the calculation for energy consumption:

$$Energy\ Consumed = Pkt(S) * Tx + Pkt(R) * Rx \quad (2)$$

where Tx represents the energy consumed during transmission and Rx represents the energy consumed during reception. Pkt(S) refers to the number of packets sent, and Pkt(R) denotes the number of packets received.

The results depicted in Figure 6 clearly indicate that the SEA-LOADng protocol consumes less energy than LOADng across all scenarios. This finding highlights the superior energy efficiency of the SEA-LOADng protocol in terms of energy consumption when compared to the LOADng protocol. The SEA-LOADng protocol's ability to minimize energy consumption showcases its potential to enhance the sustainability and longevity of IoT systems, making it an ideal choice for energy-constrained environments.

This study stands out as more efficient than others because it addresses both security and energy efficiency simultaneously, whereas other approaches typically focus on either security or energy efficiency individually.

Moreover, the results presented in Figures 4 to 6 demonstrate that SEA-LOADng outperforms LOADng in terms of received packets, ETX, and energy consumption. These findings highlight the superior efficiency, reliability, and energy conservation of the SEA-LOADng protocol. Its ability to enhance communication reliability and optimize resource usage makes it a valuable protocol for IoT-based smart agriculture systems, ultimately contributing to more effective, sustainable, and efficient farming practices.

The enhanced performance of SEA-LOADng in terms of received packets, ETX, and energy consumption has significant implications for smart agriculture:

- a) Real-time monitoring: Improved packet reception and lower ETX values enable sensors and actuators to reliably communicate real-time data about soil moisture, weather conditions, pest presence, and other critical parameters. This reliability allows farmers to respond quickly to changing conditions.
- b) Resource optimization: Efficient communication protocols reduce the need for retransmissions, conserving battery life and bandwidth. This is especially important in remote or large agricultural fields where power sources are limited, and frequent maintenance is not feasible.
- c) Data-driven decisions: With more reliable data, agricultural practices can become more data-driven. This can lead to optimized water usage, precise application of fertilizers and pesticides, and overall better crop management strategies. Enhanced decision-making improves yields and reduces environmental impact.
- d) Sustainability and longevity: The SEA-LOADng protocol's superior energy efficiency makes it an ideal choice for energy-constrained environments. By minimizing energy consumption, the protocol helps extend the operational life of IoT devices, reducing the need for frequent maintenance or battery replacements. This sustainability is crucial for the long-term viability of IoT deployments in agriculture.

Our study suggests that a secure routing protocol is not associated with poor performance in energy efficiency. The proposed method benefits from both secure and energy-efficient routing compared to other studies that focus on either security or energy efficiency individually, as shown in Table 2.

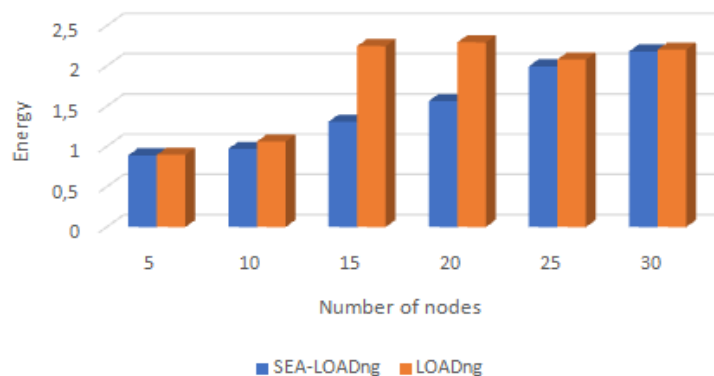


Figure 6. Energy consumption comparison

Table 2. Comparison with other methods

Work	Security	Energy efficiency
[7]	Studied	Not studied
[8]	Not studied	Studied
[9]	Not studied	Studied
Proposed method	Studied	Studied

The proposed method distinguishes itself by integrating both security and energy efficiency. By combining these two aspects, it provides a more balanced and comprehensive solution, addressing the dual challenges of securing IoT networks while optimizing energy consumption. This dual focus makes the proposed method particularly well-suited for applications in smart agriculture, where both secure and efficient operations are essential.

However, further and in-depth studies are necessary to confirm its performance, especially in regard to potential attacks such as denial of service (DoS) or Sybil attacks. Future studies may explore SEA-LOADng's performance under different environmental conditions, with feasible ways of producing scalable, energy-efficient, and secure communication protocols. Recent observations suggest that the increased resilience of SEA-LOADng is directly correlated with its adaptive energy consumption model. Our findings provide conclusive evidence that this phenomenon is associated with protocol design changes, not due to elevated numbers of network retransmissions.

## 7. CONCLUSION AND PERSPECTIVES

SEA-LOADng has demonstrated its potential to revolutionize IoT-based smart agriculture by providing a secure, efficient, and energy-aware routing protocol. Its successful implementation can lead to more sustainable and productive farming practices, contributing to the overall advancement of agricultural technology. Future research and development efforts will continue to refine and expand the capabilities of SEA-LOADng, ensuring its relevance and effectiveness in the evolving landscape of IoT applications. Additionally, efforts will be directed towards finding solutions to other potential attacks in smart agriculture.

## ACKNOWLEDGEMENTS

The authors are grateful to everyone who provided them with their expertise, including professors, doctoral students, and research laboratories of Tahri Mohamed University, Bechar.

## REFERENCES




- [1] S. Li, L. D. Xu, and S. Zhao, "The internet of things : a survey, " *Information Systems Frontiers*, vol. 17, no. 2, pp. 243-259, 2015, doi: 10.1007/s10796-014-9492-7.
- [2] T. A. Khoa, M. M. Man, T. Y. Nguyen, V. Nguyen, and N. H. Nam, "Smart agriculture using IoT multi-sensors: A novel watering management system," *Journal of Sensor and Actuator Networks*, vol. 8, no. 3, 2019, doi: 10.3390/jsan8030045.
- [3] M. Naresh, and P. Munaswamy, "Smart agriculture system using IoT technology," *International Journal of Recent Technology and Engineering*, vol. 7, no. 5, pp. 98–102, 2019.
- [4] B. B. Sinha, and R. Dhanalakshmi, "Recent advancements and challenges of internet of things in smart agriculture: A survey," *Future Generation Computer Systems*, vol. 126, pp. 169–184, 2022, doi: 10.1016/j.future.2021.08.006.
- [5] A. Jain and A. Kumar, "Smart agriculture monitoring system using IoT," *International Journal for Research in Applied Science and Engineering Technology*, vol. 8, no. 7, pp. 366-372, 2022, doi: 10.22214/ijraset.2020.7060.
- [6] S. Ratnaparkhi, S. Khan, C. Arya, S. Khapre, P. Singh, M. Diwakar, and A. Shankar, "Smart agriculture sensors in IoT: A review," *Materials Today*, 2020, doi: 10.1016/j.matpr.2020.11.138.
- [7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
- [8] S. Pal, and Z. Jadidi, "Analysis of security issues and countermeasures for the industrial internet of things," *Applied Sciences*, vol. 11, no. 20, pp. 9393, 2021, doi: 10.3390/app11209393.
- [9] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: a survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017, doi: 10.1016/j.jnca.2017.04.002.
- [10] P. Singh, M. Khari, and S. Vimal, "EESMT: An energy efficient hybrid scheme for securing mobile ad hoc networks using IoT," *Wireless Personal Communications*, vol. 126, no. 3, pp. 2149–2173, 2022, doi: 10.1007/s11277-021-08764-x.
- [11] S. Arora, I. Batra, A. Malik, A. K. Luhach, W. S. Alnumay, and P. Chatterjee, "Seed: Secure and energy efficient data-collection method for IoT network," *Multimedia Tools and Applications*, vol. 82, no. 2, pp. 1–15, 2022, doi: 10.1007/s11042-022-13614-4.
- [12] N. Moussa, E. Nurellari, and A. E. B. E. Alaoui, "A novel energy-efficient and reliable ACO-based routing protocol for WSN-enabled forest fires detection," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 1, pp. 1-17, 2022, doi: 10.1007/s12652-022-03727-x.
- [13] A. Verdieri, Y. Igarashi, T. Lys, C. Lavenu, J. Yi, U. Herberg, H. Satoh, A. Niktash, T. Clausen, and J. Dean, "The lightweight on-demand ad hoc distance-vector routing protocol-next generation (loadng)," *Computer Networks*, vol. 126, pp. 125-140, 2016, doi: 10.1016/J.COMNET.2017.06.025.
- [14] M. Hosseinzadeh, J. Tanveer, A. M. Rahmani, E. Yousefpoor, M. S. Yousefpoor, F. Khan, and A. Haider, "A cluster-tree-based secure routing protocol using dragonfly algorithm (DA) in the internet of things (IoT) for smart agriculture," *Mathematics*, vol. 11, no. 1, pp. 80, 2022, doi: 10.3390/math11010080.
- [15] J. K. Jain, D. Chauhan, and P. Jain, "An energy efficient and bandwidth aware optimal routing for IoT in agriculture," 2021, doi: 10.21203/rs.3.rs-429148/v1.
- [16] S. Sankar, P. Srinivasan, A. K. Luhach, R. Somula, and N. Chilamkurti, "Energy-aware grid-based data aggregation scheme in routing protocol for agricultural internet of things," *Sustainable Computing Informatics and Systems*, vol. 28, pp. 100422, 2020, doi: 10.1016/j.suscom.2020.100422.






- [17] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," *Journal of Network and Computer Applications*, vol. 190, pp. 103118, 2021, doi: 10.1016/j.jnca.2021.103118.
- [18] E. Yousefpoor, H. Barati, and A. Barati, "A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 1917–1942, 2021, doi: 10.1007/s12083-021-01116-3.
- [19] H. Jeong, S. W. Lee, M. H. Malik, E. Yousefpoor, M. S. Yousefpoor, O. H. Ahmed, M. Hosseinzadeh, and A. Mosavi, "SecAODV: A secure healthcare routing scheme based on hybrid cryptography in wireless body sensor networks," *Frontiers in Medicine*, vol. 9, pp. 829055, 2022, doi: 10.3389/fmed.2022.829055.
- [20] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An energy-efficient data aggregation mechanism for IoT secured by blockchain," *IEEE Access*, vol. 10, no. 3, pp. 11404–11419, 2022, doi: 10.1109/ACCESS.2022.3146295.
- [21] S. M. Hussein, J. A. L. Ramos, and A. M. Ashir, "A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks," *Electronics*, vol. 11, no. 17, pp. 2721, 2022, doi: 10.3390/electronics11172721.
- [22] K. Haseeb, I. U. 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. 2081, 2020, doi: 10.3390/s20072081.
- [23] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing, experimental," *RFC Editor*, USA, 2003.
- [24] D. Wang, Z. Tao, J. Zhang, and A. Abouzeid, "RPL based routing for advanced metering infrastructure in smart grid," *IEEE International Conference on Communications (ICC)*, pp. 1-6, 2010, doi: 10.1109/ICCW.2010.5503924.
- [25] J. Tripathi, J. Oliveira, and J. P Vasseur, RFC 6687, "Performance evaluation of routing protocol for low power and lossy networks (RPL)," *RFC Editor*, 2010, doi: 10.17487/RFC6687.
- [26] S. Elyengui, R. Bouhouchi, and T. Ezzedine, "LOADng routing protocol evaluation for bidirectional data flow in ami mesh networks," *International Journal of Emerging Technology and Advanced Engineering*, vol. 5, pp. 37-43, 2015, doi: 10.48550/arXiv.1506.06357.
- [27] S. Choubey, A. Choubey, M. Abhilash, and K. K. Mehta, "Defense mechanisms against hello flood attack in wireless sensor network," *CS Journal*, vol. 3, pp. 1-6, 2010.
- [28] G. Glissa, and A. Meddeb, "A security analysis of LOADng routing protocol," *IEEE/ACS 14th International Conference on Computer Systems and Applications*, pp. 1070-1074, 2017, doi: 10.1109/AICCSA.2017.145.

## BIOGRAPHIES OF AUTHORS



**Mrs. Touhami Sana**    she is a Ph.D. student in Computer Science, specializing in Networks and Distributed Systems, at Tahri Mohammed University (UTMB) in Algeria. She earned her Master's degree in Computer Science, with a focus on Advanced Information Systems, from the same university in 2018. Her research interests are centered around IoT security. She can be reached via email at: [touhami.sana@univ-bechar.dz](mailto:touhami.sana@univ-bechar.dz).



**Mr. Belghachi Mohamed**    he is a distinguished Professor Researcher affiliated with Tahri Mohamed University of Bechar in Algeria. He holds a prominent position as a member of the "Ad-hoc Networks" research team within the STIC (Systems and Information and Communication Technologies) Laboratory at Abou-Bekr Belkaid Tlemcen University. With a profound knowledge and experience in various domains, his expertise spans across wireless sensor networks (WSN), internet of things (IoT), internet of vehicles (IoV), flying Ad-hoc Networks (FANETs), and artificial intelligence (AI). Dr. Belghachi Mohamed's contributions have significantly impacted these fields, further advancing the realms of connectivity, communication, and intelligent systems. He can be contacted at email: [belghachi.mohamed@univ-bechar.dz](mailto:belghachi.mohamed@univ-bechar.dz).