A Secure LOADng Routing Protocol Scheme Based Fuzzy Logic

Touhami Sana*, Belghachi Mohamed
Department of Mathematics and Computer Science, Tahri Mohamed University, Bechar, Algeria
E-mail: touhami.sana@univ-bechar.dz
*Corresponding author

Keywords: LOADng routing protocol, security, the internet of things, hello flood attack, fuzzy logic

Received: April 26, 2024

The Lightweight On-demand Ad hoc Distance-vector Routing Protocol - Next Generation (LOADng) has played a pivotal role in shaping the landscape of the Internet of Things (IoT) and associated standards. It enables sophisticated communication among compact, intelligent, and embedded networking devices. LOADng focuses primarily on establishing secure connections between interconnected objects, ensuring reliable and protected communication. However, it is susceptible to several types of attacks, including Jamming attacks, Blackhole attacks, Hello Flood attacks, and others. This study presents a new protocol Fuzzy-LOADng that utilizes fuzzy logic to identify Hello Flood attack directed at the LOADng routing protocol. To validate the reliability of our proposed method, we assess Fuzzy-LOADng in the presence of a Hello Flood attack. We also compare its detection accuracy with six machine learning algorithms and evaluate its energy overhead compared to to the original LOADng (both under attack and without IDS). The results indicate that Fuzzy-LOADng surpasses the other methods, achieving a 99.98% True Positive Rate, a 0.1% True Negative Rate, and exhibiting low energy consumption.

Povzetek: Predlagana shema za protokol LOADng temelji na uporabi mehke logike za zaznavanje napadov tipa Hello Flood. Metoda Fuzzy-LOADng dosega najboljše rezultate v primerjavi z obstoječimi rešitvami za protokole IoT.

1 Introduction

The term Internet of Things (IoT) [1] refers to a network of interconnected devices designed for data gathering, actuator manipulation, and network monitoring. However, networking these devices poses significant challenges due to their limited resources such as energy, computation, memory, and mobility. These challenges define a specific type of network known as Low-power and Lossy Networks (LLNs) [2, 3]. LLNs are characterized by their limited resources and communication capabilities, presenting hurdles for developing efficient routing solutions, especially for large-scale deployments with numerous nodes [4]. Addressing challenges to enable interoperability between IoT networks, particularly LLN networks, and the internet requires resolving limitations of the IPv4 (Internet Protocol version 4) protocol stack.

To address these issues, the Internet Engineering Task Force (IETF) has introduced IPv6 over Low-power Wireless Personal Area Network (6LoWPAN) as a solution for IoT-based LLNs. 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 [5].

The advent of the LOADng protocol [5] marked a significant stride in the domain of IoT routing. Renowned for its lightweight design and adaptability to resource-constrained environments, LOADng has garnered attention as a viable solution for routing in IoT networks. However, the quest for enhanced security propelled researchers to explore innovative methodologies.

This paper concentrates on the Hello Flood attack, by proposing a new intrusion detection method using fuzzy logic in the LOADng routing protocol [6]. Results obtained using the Cooja simulator in the Contiki OS [7] demonstrate that our method identifies this attack with a remarkably high True Positive Rate (TPR) and an exceptionally low False Positive Rate (FPR).

The rest of this paper is structured as follows: Section 2 presents a literature review. Section 3 provides a brief overview of the LOADng routing protocol, its specifications, and the Hello Flood attack. The proposed approach is detailed in Section 4, followed by the results and discussion in Section 5. Finally, the conclusion is provided in Section 6 alongside some perspectives.

2 Related works

In [8], a solution utilizing geographical information and signal strength was proposed to detect Hello Flood attacks. Each sensor node monitors its surroundings, and upon detecting a transmission signal, the node verifies if the signal strength aligns with the geographical position

of the originator node. This approach was among the first in the field.

In [9], an intrusion detection architecture based on collaborative neighbor monitoring was suggested. Neighboring nodes communicate to identify Jamming, Selective Forwarding, and Hello Flood attacks. Their approach was deployed within the CTP (Collaboration Tree Protocol) framework in the TinyOS environment.

In [10], a strategy to address the Hello Flooding attack was proposed, utilizing client puzzles and signal strength measurements. In this method, nodes are classified as "friends" or "strangers" based on signal power measurements, and requests with abnormal power levels are rejected. Strangers are then required to complete puzzles. However, aside from the computational cost of the puzzles, which are effective only when the number of requests is high, relying solely on received power levels is not a reliable protection measure.

In [11], a neighborhood monitoring-based intrusion detection system was proposed. This system is based on the principle that sensor nodes in close proximity tend to display similar behavior. If a node exhibits behavior significantly different from its neighboring nodes, it is deemed malicious. For optimization, the system uses adaptive filtering with the Alpha-Beta method.

In [12], the Flood attack was examined, and a machine learning-based method for detecting the attack was developed.

In [13], a method called LSFA-IoT is proposed to protect the AODV routing protocol and IoT networks from flooding attacks. This approach is segmented into two primary phases: the initial phase incorporates a physical layer intrusion and attack detection system to identify attacks, while the second phase focuses on detecting incorrect events through APT-RREQ messages.

In [14], an IDS (Intrusion Detection System) called the compression header analyzer intrusion detection system (CHA-IDS) is proposed. This system examines 6LoWPAN compression header data to address individual and combined routing attacks. CHA-IDS is a multi-agent framework created to capture and handle raw data for gathering, analysis, and system actions. It utilizes best-first and greedy stepwise methods along with correlation-based feature selection to pinpoint the most crucial features required for intrusion detection. These features are subsequently tested using six machine learning algorithms to ascertain the optimal classification method for distinguishing between attack and non-attack scenarios. The best classification method is employed to create a rule that is implemented in Tmote Sky.

In [15], a novel framework for intrusion detection in cluster-based wireless sensor networks has been developed. This framework includes multiple protocols functioning at distinct levels. The initial protocol is a specification-based detection system that operates on IDS agents at the lower level. The second protocol is a binary classification detection system that functions at the cluster head (CH) node at the intermediate level. Moreover, each cluster head (CH) utilizes a reputation protocol to evaluate the reliability of its IDS agents. In addition, each cluster head (CH) monitors its neighboring CHs using a specification detection protocol, incorporating a voting mechanism managed at the high-level base station.

Table 1 present a summary of related works discussed in this paper.

Table 1: Summary of related works.

Author	Defense mechanism	Performance metrics	Limitations
[8]	Signal strength and geographical information	Detection rate	Not efficient in many ways. Not energy efficient.
[9]	Neighbors monitoring	FP, FN.	Communication overhead poses a challenge. Did not consider the power consumption rate.
[10]	Signal strength measurements and client puzzles	-	Unable to detect attacks launched by a coordinated group of colluding nodes. Critical parameters like FPR, FNR and energy consumption are not analyzed.
[11]	Neighborhood	Receiver Operating Characteristic, Packet Delivery Ratio, Average End-to-End Delay.	Cannot detect various attacks in WSN. Energy consumption is not analyzed.
[12]	Machine Learning Algorithm	Power Consumption.	Critical parameters like FPR, FNR are not analyzed.
[13]	LSFA-IoT	FPR, FNR, DR, PDR	Energy consumption is not analyzed.
[14]	Compression Header Analyzer Intrusion Detection System	TPR, energy consumption.	Unable to precisely identify the attacker.
[15]	Cluster-based wireless sensor networks	TPR, FPR, efficiency, energy consumption	Only a limited number of detection approaches are deployed extensively in computer networks. Do not take into account the context of obile WSNs

3 Background

In this section we present the background concepts necessary to our work.

3.1 LOADng routing protocol

The Lightweight On-demand Ad hoc Distance-vector Routing Protocol Next Generation, LOADng, functions as a reactive routing protocol tailored for Wireless Sensor Networks (WSN). It stems from the Ad hoc On-Demand Vector routing protocol (AODV) and was initially devised for devices operating on IEEE 802.15.4 within 6LoWPANs and LLNs [16]. This protocol can operate as either a layer 3 route-over routing protocol or a layer 2 mesh-under protocol. LOADng is highly esteemed for its simplicity and minimal memory storage demands. These attributes render it particularly suitable for Advanced Metering Infrastructure (AMI) mesh networks [17, 18]. However, given its initial development for WSNs and LLNs, it necessitates adaptation to align with their specific requirements and limitations.

3.2 LOADng specification

LOADng protocol defines four types of control messages that serve specific purposes [19]:

Route REQuest (RREQ): An originating device generates the RREQ message when it requires sending a data packet to a destination. The RREQ packet lacks a valid route to the ultimate destination but encompasses vital details like the destination address, sequence number, hop count, hop limit, and characteristics of routing metrics.

Route REPly (RREP): A router acting as the destination for the data creates the RREP message upon receiving an RREQ message. This router, designated as the data receiver, forms the RREP message. It resembles the structure of the RREQ message but incorporates an extra field named "ackrequired," signaling the necessity for an acknowledgment message.

Route REPly ACKnowledgement (RREP-ACK): The RREP-ACK message is produced by a LOADng router upon receiving an RREP message with an "ackrequired" field set to true. This message is directed straight to the destination as the routes remain intact.

Route ERRor (RERR): A router generates the RERR message upon detecting that a destination is unreachable. The malfunctioning route is pinpointed through the "errorcode" field, aiding in diagnosing the cause of the route failure.

The LOADng operates through several key steps (see Figure 1) [19]:

- ✓ RREQ Generation: An originating LOADng Router produces RREQ messages aiming to find a route towards a designated destination node.
- ✓ RREQ Forwarding: The RREQ messages are relayed through intermediate nodes listed in the routing table entry. This sequence persists until the RREQs arrive at the destination LOADng Router.
- ✓ RREP Generation: After receiving the RREQ message, the assigned destination generates an RREP message in return. The RREP is transmitted hop-by-hop towards the originator, adhering to the stored reverse route acquired from the Routing Set at intermediary nodes.
- ✓ RREP-ACK: When the "ackrequired" field in the RREP message is set to True, the recipient of the RREQ must dispatch an RREP-ACK message to the sender of the RREP, affirming the successful receipt of the RREP.
- ✓ RERR Management: Upon detecting a malfunctioning route, RERR message is dispatched to the originator of the data packet, notifying it of the route's failure.

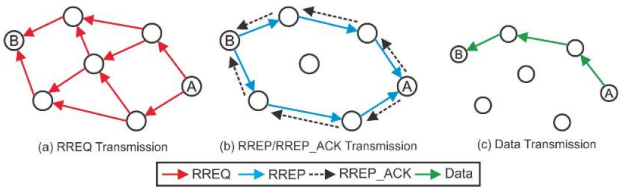

Figure 1: Operation of LOADng and its utilization of control messages.

To facilitate these operations, each node utilizing LOADng routing maintains Information Base, which includes the following details [20]:

- Routing Set: Stores information about the routing processes, such as valid routes and associated metrics.
- Blacklisted Neighbor Set: Keeps track of neighbors that are deemed unresponsive or unreliable for routing purposes.
- Pending Acknowledgment Set: Maintains a record of pending acknowledgments to be sent or received.

By maintaining these sets, nodes can effectively participate in the LOADng routing protocol and facilitate efficient communication within the network.

3.3 Hello Flood attack in LOADng

In a Hello Flood attack, depicted in Figure 2, a malicious node can utilize a high transmission power to transmit, record, or replicate HELLO messages. This action creates a false perception of being a neighbor to numerous nodes within the network, leading to significant ambiguity in network routing. This attack capitalizes on the practice of several protocols that utilize broadcast Hello messages to announce their presence in the network. By employing a transmission range greater than that of other nodes, an attacker can inundate a large area of the network with multiple Hello messages [21], causing other nodes to mistakenly perceive the attacker as their neighbor. Consequently, all nodes respond to these false messages, depleting their energy and leaving the network in a state of confusion.

Figure 2: Hello flood attack.

In the LOADng protocol [19], vulnerability exists whereby a malicious node can manipulate the network by sending an excessive amount of RREQ messages within a brief period. These RREQs are aimed at an unreachable destination node with an unattainable address. As the destination node cannot be accessed, the RREQ messages persistently spread throughout the entire network without ever receiving a RREP message.
This flood of RREQ messages overwhelms the network and has detrimental effects, particularly on the battery life of the nodes. As the nodes continuously process and forward these unnecessary RREQ messages, their energy resources deplete rapidly. This battery depletion can severely impact the overall functioning and efficiency of the network.
By exploiting this vulnerability in the LOADng protocol, an adversary node can disrupt the network's normal operation, drain the nodes' batteries, and potentially cause network instability or failure.

4 Proposed approach

In this section, we introduce security measures that aim to mitigate the Hello Flood attack by utilizing fuzzy logic. The proposed solution outlined in this paper focuses on detecting the Hello Flood attack by utilizing both signal strength and fuzzy logic methods.
The assumption is made that the signal strength of all sensor nodes within a specific radio range is the same.
Every node assesses the signal strength of the received "hello" messages in comparison to the established radio range strength. When the signal strengths match, the sending node is classified as a “comrade”. If the signal strength varies, the sender is classified as an “outsider”.
When a node is designated as an outsider, its authenticity undergoes additional scrutiny through the application of fuzzy logic.
Our proposed approach for intrusion detection involves using fuzzy logic with three metrics: packet count, energy consumption, and RSSI (Received Signal Strength Indicator). Each node is assigned a distinct state at a given time interval based on three fuzzy input parameters.

The input parameters in the fuzzy system are represented by graphs of membership functions. The graphs illustrate how the values on the x-axis of one parameter correspond to the values on the y-axis of the other parameter. Consequently, two values along the y-axis correspond to each point on the x-axis.

Fuzzy logic is a widely used approach in network-related fields. It offers the capability to transform several input variables into a single output [22, 23]. The fuzzy process model, as depicted in Figure 3, comprises four steps [23]. In this research, we utilized the Mamdani model [24], which is widely recognized as the most commonly used method for fuzzy inference.

The four steps of the fuzzy process model are as follows:

Fuzzification: This step involves capturing the designated input variables and determining their membership degrees to assign suitable fuzzy set values.

Fuzzy inference: It allows for the combination of fuzzified input variables and the computation of the fuzzy output.

Aggregation: If the output relies on multiple rules, this step consolidates all values into a single value.

Defuzzification: In this last stage, the fuzzy output is transformed into a precise value according to the preceding step.

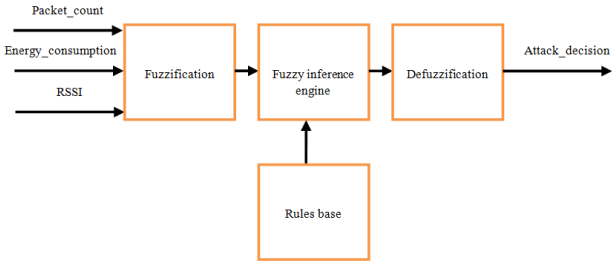

Figure 3: The fuzzy process model of our approach.

The primary objective of this paper is to determine the nature of a node, whether it is trustworthy or malicious. The proposed approach is structured in two stages as described below:

1st Phase: If the signal strength of the transmitting node matches that of the other nodes, the RREQ message is accepted.

2nd Phase: If the signal strength of the transmitting node differs from the others, a fuzzy method utilizing three input parameters is employed. This fuzzy system evaluates whether an attack has occurred or not. If an attack is identified, the RREQ message is rejected. Conversely, if no attack is detected, the RREQ message is accepted.

Algorithm 1 presents the pseudo code for the attack detection process.

Algorithm 1. Detection of Hello flood Attack

Fuzzy Inputs : Packet_count, Energy_consumption, RSSI
Fuzzy Output : Attack Decision (yes or no)
for each node receiving RREQ message **do**
  if (signal strength of node>signal strength of the other nodes) **then**
    Run the fuzzy method
    if (attack has happened) **then**
      Request is discarded
    else
      Request is accepted
    end if
  else
    Request is accepted
  end if
end for

To demonstrate the fuzzy logic composition, we utilize three metrics: Packet_count, Energy_consumption and RSSI (Received Signal Strength Indicator).

✓ Energy_consumption: This metric measures the amount of energy consumed by the nodes.

✓ Packet_count: This metric represents the number of packets transmitted by the node.

✓ RRSI: This metric indicates the strength of the received signal.

In fuzzy logic, variables are represented as linguistic values that range between true and false. These linguistic variables are used to express the degree of dependency among metrics and generate an output [22,23] Figure 4 illustrates the fuzzy graph for the Packet_count parameter, where the membership function is categorized into minimum, normal, and maximum. The maximum specified Packet_count value in this paper is 15. Figure 5 represents the fuzzy graph for the Energy_consumption, with a range from 0 to 255. The energy level is divided into three categories: low, medium, and high. Figure 6 presents the fuzzy chart for the RSSI parameter, which is also categorized as weak, moderate, and strong.

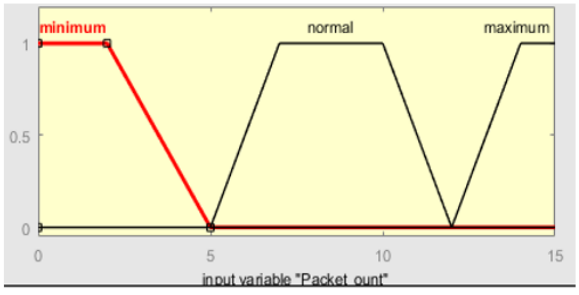

Figure 4: The membership function of Packet_count.

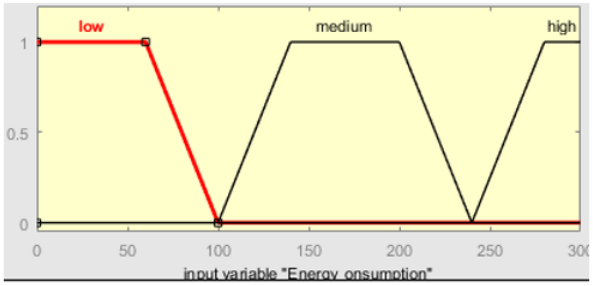

Figure 5: The membership function of Energy_consumption.

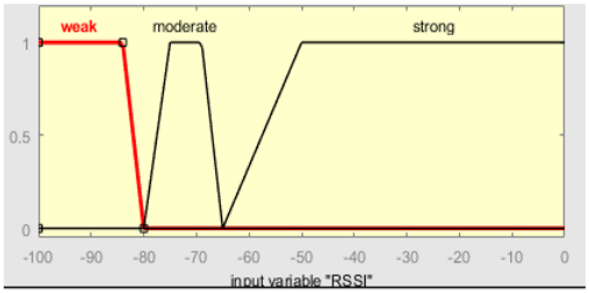

Figure 6: The membership function of RSSI.

Figure 7 illustrates the fuzzy rule base utilized for linking the input-output membership functions. The fuzzy inference system operates according to the IF-THEN rules outlined in Table 2. These rules incorporate specific fuzzy logic operators such as 'AND' or 'OR' to link various linguistic variables.

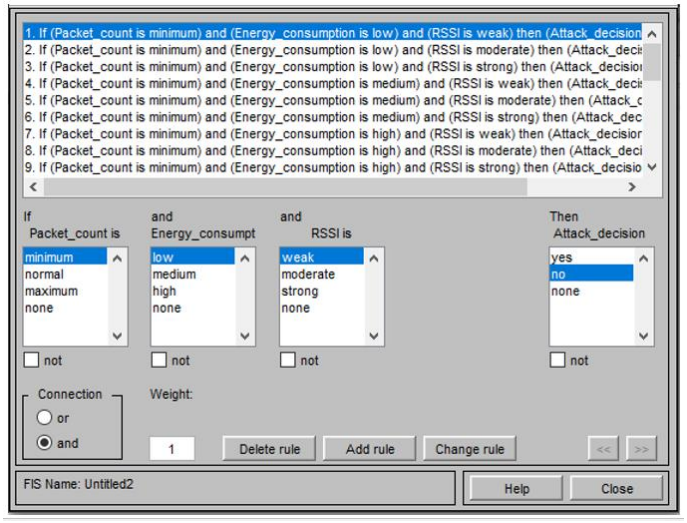

Figure 7: Fuzzy rule base.

Table 2: Fuzzy rules.

Packet_ count	Energy_ consumption	RSSI	Attack_ Decision
Minimum	Low	Weak	No
Minimum	Low	Moderate	No
Minimum	Low	Strong	No
Minimum	Medium	Weak	No
Minimum	Medium	Moderate	No
Minimum	Medium	Strong	No
Minimum	High	Weak	Yes
Minimum	High	Moderate	No
Minimum	High	Strong	No
Normal	Low	Weak	Yes
Normal	Low	Moderate	No
Normal	Low	Strong	No
Normal	Medium	Weak	Yes
Normal	Medium	Moderate	No
Normal	Medium	Strong	No
Normal	High	Weak	Yes
Normal	High	Moderate	Yes
Normal	High	Strong	No
Maximum	Low	Weak	Yes
Maximum	Low	Moderate	No
Maximum	Low	Strong	No
Maximum	Medium	Weak	Yes
Maximum	Medium	Moderate	Yes
Maximum	Medium	Strong	No
Maximum	High	Weak	Yes
Maximum	High	Moderate	Yes
Maximum	High	Strong	Yes

5 Results and discussions

To validate our approach, we implement the Hello Flood attack in Contiki-Cooja [25] to observe how the fuzzy-LOADng protocol detects it. This section first outlines the simulation setup and evaluation metrics, followed by a discussion of the results achieved.

5.1 Simulation setup

The Z1 mote serves as the server, client, and malicious nodes in our setup. Our simulation scenario includes a total of 8 nodes positioned manually to achieve a consistent RSSI value. The topology setup, depicted in Figure 8 below, features node 8 as the malicious node broadcasting the hello message. This malicious node can impersonate a neighbor node to multiple nodes by broadcasting the message with a high RSSI, thereby gaining entry into the network.

To initiate the attack in LOADng, the attacker broadcasts RREQ messages to announce its intent. Our implementation of LOADng utilizes the Contiki Rime stack. Simulations are conducted over a 20-minute period using the Unit Disk Graph Medium (UDGM) model to simulate signal attenuation in the radio medium.

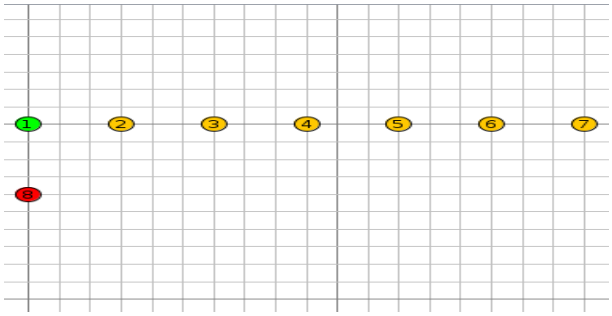

Figure 8: Topology setup.

The simulation parameters are detailed in Table 3.

Table 3: Simulation parameters.

Parameters	Values
Operating system	Contiki 3.0
Simulator	Cooja
Radio model	UDGM: Distance loss
Mote type	Z1 mote
Number of nodes	6 clients, 1 sink
Number of attackers	1
Couche Mac	CSMA
Couche RDC	Contikimac
Channel check rate	8 Hz
Network stack	Rime
Simulation time	20 minutes

5.2 Evaluation metrics

Two sets of evaluation metrics have been developed to validate the effectiveness of the proposed method. The initial set primarily assesses accuracy using metrics like True Positive Rate (TPR) and False Positive Rate (FPR). The second set measures energy consumption.

5.2.1 TPR and FPR

The TPR, also known as the Detection Rate, indicates the IDS's effectiveness in detecting malicious behaviors. Conversely, the FPR indicates the IDS's propensity to incorrectly identify legitimate behaviors as malicious. The formulas for calculating these two metrics are provided in equations 1 and 2:

$$TP_{rate} = \frac{TP}{TP+FN} \quad (1)$$

$$FP_{rate} = \frac{FP}{FP+TN} \quad (2)$$

Where

- True Positive (TP): Indicates correctly detected malicious behaviors, where the IDS accurately raises an alert for a malicious event.
- False Positive (FP): Occurs when the IDS incorrectly raises an alarm for legitimate behavior in the network.
- True Negative (TN): This happens when the IDS correctly identifies a legitimate behavior as normal.
- False Negative (FN): This occurs when the IDS incorrectly identifies a malicious event as normal.

5.2.2 Energy consumption

The effects on resource consumption are assessed using metrics such as energy consumption of the network and power consumption of individual nodes, as outlined in [26]. The equations 3 and 4 are used to compute these metrics:

Energy_usage(mJ) =(19.5mA×transmit+21.8mA×listen+1.8mA×CPU +0.0545×LPM)×3 V/4096×8 (3)

$$\text{Power\_consumption(mW)} = \frac{Energy\_usage(mJ)}{Time\ (s)} \quad (4)$$

The higher the energy and power consumption of the network, the shorter its operational lifetime will be.

5.3 Simulation results and discussion

5.3.1 Detection efficency

To ensure the reliability of our proposed method, we compare our detection accuracy results with six algorithms evaluated in [14], which specifically address the Hello Flood attack and have been assessed using Cooja.

Table 4 compares the performance of various machine learning methods evaluated in [14] with our method regarding TPR and FPR. A summary of the data is as follows:

Table 4: Comparison of TPR and FPR of our method with other methods.

Method	TPR	FPR
J48	99,8	0,12
Logistic	99,9	0,18
MLP	99,6	0,4
Naïve bayes	97,1	3,8
Random forest	99,8	0,12
SVM	96,2	4,4
Proposed method	99,98	0,1

Figures 9 and 10 respectively show the TPR and FPR of our method compared with other methods.

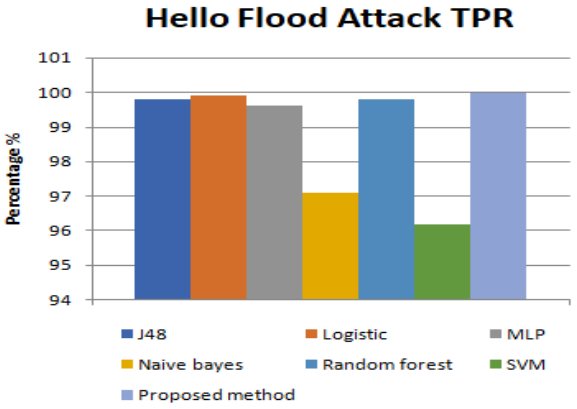

Figure 9: True positive rate.

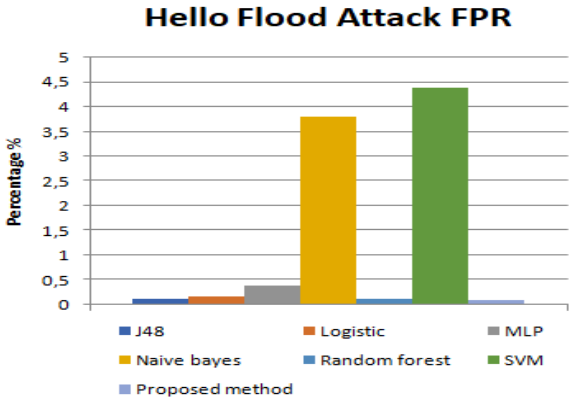

Figure 10: False positive rate.

According to the results shown in Figures 9 and 10, it is evident that the proposed fuzzy-LOADng protocol exhibits the highest TPR (99.98), indicating it correctly identifies positive cases more frequently than other methods. It also has the lowest FPR (0.1), meaning it generates the fewest false alarms compared to other methods. The use of fuzzy logic enables nuanced decision-making, which reduces the likelihood of FP.

5.3.2 Energy efficiency

Evaluating energy consumption is essential for estimating node lifetime, particularly for applications with limited access to a continuous power supply. We conducted a 20-minute simulation in the collect view (where the sink collects environmental data from all other nodes) with and without IDS (LOADng and Fuzzy-LOADng). The energy and power consumption of both LOADng and Fuzzy-LOADng were recorded, as shown in Figure 11.

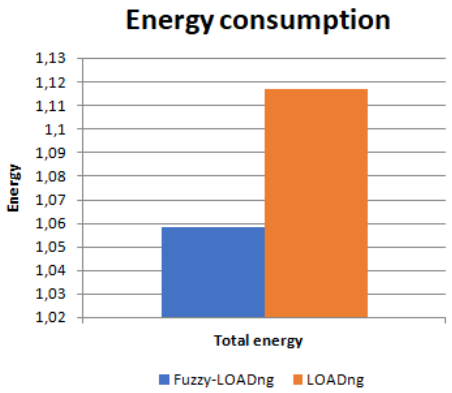

Figure 11: Comparison of energy consumption.

According to the results presented in Figure 11, it is evident that the Fuzzy-LOADng protocol consumes less energy than LOADng. This finding indicates that the Fuzzy-LOADng protocol is more energy-efficient than the LOADng protocol in terms of energy consumption. By demonstrating superior energy efficiency, the Fuzzy LOADng protocol show cases its potential to enhance the sustainability and longevity of IoT systems, making it a favorable choice for energy-constrained environments. This increase is due to the efficient handling of RREQ messages.

6 Conclusion and perspectives

This paper focuses on the security obstacles encountered within the LOADng routing protocol and explores the development of a secure version using fuzzy logic technology, particularly against Hello Flood attacks. Fuzzy logic contributes to improved security measures by enabling flexible and nuanced decision-making in various domains. The proposed protocol was evaluated using the Contiki Cooja simulator. The simulation results and comparison with previous works show that Fuzzy-LOADng detects hello flood attacks with an exceptionally high TPR and an extremely low FPR, and consumed low energy overhead demonstrating its superior performance and security enhancements.

Like any routing protocol, LOADng faces security challenges that need to be addressed to ensure the secure operation of the network. Here are some common security challenges associated with routing protocols:

1. Authentication and Authorization: Unauthorized nodes may attempt to gain access to the network and disrupt the routing process. Ensuring the authenticity and authorization of nodes is crucial to prevent malicious entities from participating in the routing protocol.
2. Confidentiality: Data transmitted between nodes in a WSN should be kept confidential to protect sensitive information from eavesdropping. Encryption techniques, such as symmetric or asymmetric encryption, can be used to ensure the confidentiality of data.
3. Integrity: It is essential to ensure the integrity of the routing protocol messages and data transmitted within the network. Techniques like message authentication codes (MACs) or digital signatures can be employed to verify the integrity of the transmitted data.
4. Availability: Routing protocols should be resilient to attacks that can disrupt the availability of the network. Denial-of-service (DoS) attacks, for example, can overwhelm the network with excessive traffic or exhaust network resources. Implementing mechanisms to detect and mitigate such attacks is important for maintaining network availability.
5. Secure Key Management: LOADng, like other routing protocols, may require the use of cryptographic keys for secure communication. Proper key management practices, including key distribution, key storage, and key revocation, should be in place to ensure the security of the key infrastructure.
6. Localization Attacks: LOADng relies on localized information to make routing decisions. Malicious nodes may provide false or misleading location information, leading to routing disruptions or even targeted attacks. Techniques to verify and validate location information can help mitigate these attacks.

These are just a few examples of the security challenges that routing protocols, including LOADng, may face.

In the future, we plan to enhance the security of this protocol by employing cryptographic methods, authentication techniques, secure key management, artificial intelligence, and other advancements.

Acknowledgement

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] Li, S., Da Xu, L., and Zhao, S., (2015), “The internet of things: a survey”, Information Systems Frontiers, vol. 17, no. 2, pp. 243-259, doi.org/10.1007/s10796-014-9492-7.

[2] Zhao, M., Kumar, A., Chong, P.H.G., and Lu, R., (2017), “A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities”, Peer-to-Peer Networking Applications, vol. 10, no. 5, pp. 1232-1256, doi.org/10.1007/s12083-016-0475 y.

[3] Farzaneh, B., Ahmed, A.K., and Alizadeh, E., (2019), “MC-RPL: A New Routing Approach based on Multi-Criteria RPL for the Internet of Things”, IEEE 9th International Conference on Computer and Knowledge Engineering (ICCKE),

Mashhad, Iran, 24-25 October, pp. 420-425, IEEE, USA, doi.org/10.1109/ICCKE48569.2019.8964675.

[4] Ghaleb, B., AI-Dubai, A., Ekonomou, E., Alsahran, A., Nasser, Y., Mackenzie, L., and Boukerche, A., (2018)., "A survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-power and Lossy Networks: A focus on Core Operations", IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1607-1635, doi.org/10.1109/COMST.2018.2874356.

[5] Verdiere, A., Igarashi, Y., Lys, T., Lavenu, C., Yi, J., Herberg, U., Satoh, H., Niktash, A., Clausen, T., and Dean, J., (2016), "The lightweight on-demand ad hoc distance-vector routing protocol-next generation (loadng)", Computer Networks, vol. 126, pp. 125-140, doi.org/10.1016/J.COMNET.2017.06.025.

[6] Zadeh, L.A, (1976), "A fuzzy-algorithmic approach to the definition of complex or imprecise concepts", International Journal of Man machine studies, vol. 8, no. 3, pp. 249-291, doi.org/10.1016/S0020-7373(76)80001-6.

[7] Dunkels, A., Gronvall, B., and Voigt, T., (2004), "Contiki-a lightweight and flexible operating system for tiny networked sensors", 29th Annual IEEE International Conference on Local Computer Networks, Tampa, FL, USA, 16-18 November, pp.455-462, IEEE, USA, doi.org/10.1109/LCN.2004.38.

[8] Pires, W.R., Figueiredo, T.H., Wonga, H.C., and Loureiro, A., (2004), "Malicious node detection in wireless sensor networks", Parallel and Distributed Processing Symposium, p. 24.

[9] Stetsko, A., Folkman, L., and Matyáš, V., (2010), "Neighbor-based intrusion detection for wireless sensor networks", 6th International Conference on Wireless and Mobile Communications (ICWMC), Valencia, Spain , 20-25 September , pp. 420-425, IEEE, USA, doi.org/10.1109/ICWMC.2010.61.

[10] Singh, V.P., Jain, S., and Singhai, J., (2010), "Hello flood attack and its countermeasures in wireless sensor networks", International Journal of Computer Science, vol. 7, no. 3, pp. 23-27.

[11] Khosravi, H., Azmi, R., and Sharghi, M., (2016), "Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks", International Journal of Future Computer and Communication, vol. 5, no. 2, pp. 99-103, doi.org/10.18178/ijfcc.2016.5.2.452.

[12] Gönen, S., Barişkan, M.A., Karacayilmaz, G., Alhan, B., Yilmaz, E.N., Artuner, H., and Sindiren, E., (2022), "A Novel Approach to Prevention of Hello Flood Attack in IoT Using Machine Learning Algorithm", El-Cezerî Journal of Science and Engineering, vol. 9, no. 4, pp. 1529-1541, doi.org/10.31202/ecjse.1149925.

[13] Zarei, S.M., Fotohi, R., (2021), "Defense Against Flooding Attacks using Probabilistic Thresholds in the Internet of Things Ecosystem", Security and Privacy, doi.org/10.1002/spy2.152.

[14] Napiah, M.N., Idris, M.Y., Ramli, R., And Ahmedy, I., (2018), "Compression Header Analyzer Intrusion Detection System (CHA - IDS) for 6LoWPAN Communication Protocol", IEEE Access, vol. 6, pp. 16623-16638, doi.org/10.1109/ACCESS.2018.2798626.

[15] Sedjelmaci, H., Senouci, S.M., and Feham, M., (2022), "An efficient intrusion detection framework in cluster-based wireless sensor networks", Security and communication networks, vol. 6, no. 10, pp. 1211-1224, doi.org/10.1002/sec.687.

[16] Perkins, C., Belding-Royer, E., and Das, S., RFC 3561, (2003), "Ad hoc On-Demand Distance Vector (AODV) Routing, Experimental", RFC Editor, USA.

[17] Wang, D., Tao, Z., Zhang, J., and Abouzeid, A., (2010), "RPL based routing for advanced metering infrastructure in smart grid", IEEE International Conference on Communications (ICC), Cape Town, South Africa, 23-27 May, pp.1-6, IEEE, USA, doi.org/10.1109/ICCW.2010.5503924.

[18] Tripathi, J., Oliveira, J., and Vasseur, J.P., RFC 6687, (2010), "Performance evaluation of routing protocol for low power and lossy networks (RPL)", RFC Editor, USA, doi.org/10.17487/RFC6687.

[19] Glissa, G., Meddeb, A., (2017), "A security analysis of LOADng routing protocol", IEEE/ACS 14th International Conference on Computer Systems and Applications, Hammamet, Tunisia, 30 October-03 November, pp. 1070-1074, IEEE, USA, doi.org/10.1109/AICCSA.2017.145.

[20] Elyengui, S., Bouhouchi, R., Ezzedine, T., (2015), "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, doi.org/10.48550/arXiv.1506.06357.

[21] Choubey, S., Choubey, A., Abhilash, M., and Mehta, K.K., (2010), "Defense Mechanisms against Hello Flood Attack in Wireless Sensor Network", CS journal, vol.3, pp.1-6.

[22] Nourmohammadi-Khiarak, J., Feizi-Derakhshi, M.R., Razeghi, F., Mazaheri, S., Zamani-Harghalani, Y., and Moosavi-Tayebi, R., (2020), "New hybrid method for feature selection and classification using metaheuristic algorithm in credit risk assessment", Iran Journal of Computer

Science, Springer, vol. 3, pp. 1-11, doi.org/10.1007/s42044-019-00038-x.

[23] Lamaazi, H., and Benamar, N., (2018), "OF-EC: A novel energy consumption aware objective function for RPL based on fuzzy logic", Journal of Network and Computer Applications, vol. 117, pp. 42-58, doi.org/10.1016/j.jnca.2018.05.015.

[24] Kamgueu, P., Nataf, E., and NdieDjotio, T., (2015), "On design and deployment of fuzzy-based metric for routing in low-power and lossy networks", IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops), Clearwater Beach, FL, USA, 26-29 October, pp. 789-795, IEEE, USA, doi.org/10.1109/LCNW.2015.7365929.

[25] Contiki. Available online: http://www.contiki-os.org/ (accessed on 6 May 2016).

[26] Raza, S., Wallgren, L., and Voigt, T., (2013), "SVELTE: Real-time intrusion detection in the Internet of Things", Ad Hoc Networks, vol. 11, pp. 2661–2674.