Evaluating Localization Algorithms in IoT Networks Under Jamming Attacks

Michael Savva*, Iacovos Ioannou*†, and Vasos Vassiliou*†
*Department of Computer Science, University of Cyprus
†CYENS Centre of Excellence, Nicosia, Cyprus

***Abstract*—This research investigates the performance of six localization algorithms in the context of Jamming attacks within Internet of Things (IoT) networks. Building upon our previous work involving the Fuzzy Logic-based Intrusion Detection System (FLIDS) approach, we have extended the framework to incorporate a dedicated localization module to pinpoint the jamming source. The study assesses the effectiveness of these localization techniques by analyzing key metrics, including the Euclidean error distance and algorithm execution time.**

***Keywords*-Internet of Things, Jamming Attacks, Localization, Intrusion Detection, Fuzzy logic, Multilateration**

I. Introduction

The ”Internet of Things” (IoT) concept encompasses a range of tangible entities, such as sensors, machines, actuators, and other apparatus, specifically engineered to gather and transmit data through the Internet. These items are frequently designed with specific functionalities in order to accommodate specific jobs, and they can seamlessly integrate into bigger systems when connected with comparable devices [1].

Furthermore, owing to their profound integration with critical infrastructure networks, IoT devices are susceptible to a multitude of dangers. The vulnerability discussed by Surendar et al. (2016) is mostly attributed to the intrinsic limitations in terms of memory, computational capability, and energy reserves [2]. The compounded challenges arise from the amalgamation of diverse technologies, the inherent heterogeneity within IoT networks, and the decentralized nature of their deployments, thereby accentuating the vulnerabilities and necessitating a robust security framework [2]. It is essential to acknowledge that the unique constraints inherent in IoT environments often preclude the utilization of conventional security mechanisms, thereby exposing IoT devices, networks, and applications to heightened security risks, as highlighted in the work by Lopez et al. [3].

Numerous threats can severely impact the performance and functionality of IoT networks, as discussed in Deogirikar et al.’s work [4]. Among these, the jamming intrusion is the most pervasive and detrimental, as elucidated by Jaitly [5]. The prevalence of wireless technologies has brought forth the issue of jamming attacks in wireless communication as a critical research concern, primarily due to the relative ease with which wireless communication can be disrupted [6]. In the event of a wireless network falling victim to such an attack, its signals are typically inundated with irregular or sophisticated radio jamming signals, rendering legitimate wireless devices incapable of deciphering data packets [7].

ISBN 978-3-903176-63-8 © 2024 IFIP

The ongoing vulnerability of wireless communication to radio jamming attacks persists, attributed to the open nature of wireless channels, the accessibility of launching such attacks, and the limited progress in the development of jamming-resistant wireless networking systems [7].

This paper evaluates the effectiveness of localization techniques under the Jamming attack in IoT networks. This paper uses the detection knowledge of our previous work on the FLIDS [8], [9] approach, adding a localization module in order to map the jammer. This paper examined the effectiveness of localization techniques using the Euclidean error distance and execution time of algorithms. This study uses the Retransmissions and ETX (Expected Transmission Count) network layer metrics in order to locate the jammer at the edge.

Experiments are conducted in various scenarios using TelosB (IEEE 802.15.4/ZigBee) with omnidirectional antenna sensor nodes in Contiki OS and the Cooja simulator tool to assess this strategy.

The novel contribution of this research is the advancement of IoT network defenses against jamming, through the novel integration of a localization module within a Fuzzy Logic-based Intrusion Detection System. This enhancement not only strengthens the security framework but also pioneers the use of network layer metrics like Retransmissions and ETX for pinpointing jammers. Additionally, employing TelosB nodes and the Cooja simulator within Contiki OS for empirical testing brings the study closer to the complexities of real-world IoT scenarios. These efforts collectively elevate the robustness of IoT systems against jamming disruptions. This study presents the following contributions to the field of IoT security:

- A comprehensive evaluation of six localization algorithms’ performance in the presence of jamming attacks, a scenario prevalent in IoT network operations.
- Extension of the FLIDS framework to include a dedicated localization module designed to accurately pinpoint the source of jamming.
- A thorough analysis of algorithmic performance through key metrics such as Euclidean error distance and algorithm execution time, contributing to a nuanced understanding of localization effectiveness.
- Utilization of network layer metrics, specifically Retransmissions and Expected Transmission Count (ETX), to facilitate the jammer localization at the network edge.
- An extensive experimental setup using TelosB nodes within Contiki OS and the Cooja simulator, reflecting practical IoT network conditions and attack scenarios.

The rest of the paper is structured as follows. Section II

provides background information on some jamming localization algorithms. Section III describes the proposed algorithm for jammer localization. The efficiency of the investigated approaches is examined, evaluated, and compared in Section IV. Finally, Section V includes concluding remarks and our future directions.

II. Background and Related Work

Localization algorithms can be classified into two primary categories: Range-based algorithms, as demonstrated in studies like [10]–[14]; and Range-free algorithms, as exemplified in works such as [15], [16].

Range-based algorithms employ precise point-to-point estimation methods, relying on distance or angle measurements for range estimation, as highlighted in [17]. These techniques necessitate the deployment of high-precision and expensive hardware, including directional antennas for distance estimation, as discussed in works such as [18], [19]. In Range-based approaches, distance estimation is accomplished through one of the following methods: Time of Arrival (ToA), Time Difference of Arrival (TDoA), Angle of Arrival (AoA) [20], or Received Signal Strength (RSS) [21].

Range-free algorithms harness the connectivity information between neighbouring nodes, employing specialized protocols that obviate the necessity for radio signal measurements. Instead, this category of algorithms relies on radio communication range to delineate nodes within a specific communication sphere. These algorithms operate on the premise that if two nodes can communicate, the distance between them, with a certain probability, is less than their maximum transmission range, as elucidated in [17].

Several prominent Range-free algorithms, documented in the existing literature, include the Centroid Localization (CL) Algorithm, Approximate Point In Triangulation (APIT), DV-Hop algorithm, and the Amorphous Positioning Algorithm [17]. Conversely, range-free localization strategies are being explored as more cost-effective alternatives when compared to the pricier range-based solutions, as noted in [22].

A. Related Work on Jamming Localization Algorithms

Accurate identification of the source of a jamming attack is paramount to initiate security measures against the interfering node and restore network communication, as emphasized in [23].

In this context, there exist four established jammer localization algorithms: Centroid Localization (CL) [24], Weighted Centroid Localization (WCL) [25], Virtual Force Iterative Localization (VFIL) [26], and Double Circle Localization (DCL) [23]. Moreover, the abovementioned approaches will be evaluated in two different network topologies.

1) Centroid Localization (CL): CL offers a means of jammer localization, functioning independently of the target nodes' cooperation. Specifically, CL leverages the positional data of nearby nodes, defined as those within the transmission range of the target node. When localizing a jammer, these nearby nodes are the ones being jammed. Consequently, in order to gauge the jammer's position, CL compiles the coordinates of all jammed nodes and calculates their average, which serves as the estimated location of the jammer [26].

CL exclusively relies on network node coordinates, making it resilient to uncertainties in radio propagation within the environment. Nevertheless, it displays heightened sensitivity to the arrangement of jammed nodes. For instance, the estimation will exhibit a corresponding bias if the overloaded nodes are concentrated on a particular side of the jammer. Moreover, a greater network density in a uniformly distributed network enhances the likelihood of jammed nodes being uniformly dispersed around the jammer, thereby resulting in more accurate estimations.

Suppose there are N jammed nodes represented as $\{(X_1, Y_1), (X_2, Y_2), \ldots, (X_N, Y_N)\}$.

The jammer's location can be estimated as follows:

$$\left(\widehat{X}_{jammer}, \widehat{Y}_{jammer}\right) = \left(\frac{\Sigma_{i=1}^{N} X_i}{N}, \frac{\Sigma_{i=1}^{N} Y_i}{N}\right) \quad (1)$$

The CL algorithm in article [24] estimates the jammer's position by averaging boundary and jammed node locations. However, CL is sensitive to nodes' position and density. Therefore, the accuracy of the location error depends on the number of affected nodes and their location.

2) Weighted Centroid Localization (WCL): WCL is an improved iteration of CL that determines the target node's position through a weighted average computation. One potential metric for assigning weights is the proximity between the target node and its neighbors, like the distance between the jammer and a jammed node in our context. The rationale is that a jammed node near the jammer should significantly influence the average location estimate more than one situated farther away. In real-world applications, WCL has demonstrated a superior ability to produce more accurate estimations than CL [25].

Through the incorporation of a weighting factor into the centroid approach, the estimation of the jammer's location is formulated as follows:

$$\left(\widehat{X}_{jammer}, \widehat{Y}_{jammer}\right) = \left(\frac{\Sigma_{i=1}^{N} w_i X_i}{\Sigma_{i=1}^{N} w_i}, \frac{\Sigma_{i=1}^{N} w_i Y_i}{\Sigma_{i=1}^{N} w_i}\right) \quad (2)$$

The weight $w_i = \frac{1}{d_i^2}$ where d_i is the distance between the i-th neighboring node and the jammer node. A potential method for obtaining distance information involves measuring the received signal strength (RSS) of incoming radio signals, which exhibits an inverse relationship with distance.

Blumenthal et al. introduced the WCL based on the Link Quality Indicator, and it is a variation algorithm for tracking ZigBee nodes in outdoor settings [25]. WCL offers a rapid and straightforward solution for determining the positions of devices within wireless sensor networks. Additionally, the authors employed Link Quality Indicator (LQI) measurements to estimate the distance between nodes and reference points.

Additionally, Wang et al. [27] proposed an enhanced method known as WCL based on the RSSI variation algorithm to determine node locations by refining the CL algorithm. While the CL technique estimates the jammer's location by averaging the positions of all affected nodes within or near the jamming area, it can introduce significant errors when only a few nodes are influenced by the jamming signal, depending on their locations. To mitigate this issue, WCL calculates the average jamming power received by

boundary nodes and employs it as a weight to minimize location errors.

3) Virtual Force Iterative Localization (VFIL): (VFIL) [26] seeks to enhance CL by refining the estimation process based on the distribution of jammed nodes. In its approach, VFIL initially estimates the transmission range of the jammer. Subsequently, it defines an estimated jammed region in a circular configuration, utilizing CL's estimation as the center and encompassing all jammed nodes, with boundary nodes positioned outside this region.

VFIL then iteratively adjusts the center of the estimated jammed region within the network to cover the maximum number of jammed nodes. It operates on the assumption that when the estimated jammer's location matches the actual position, the estimated jammed region will coincide with the real jammed region.

To bring the estimated location in line with the actual jammer's location, VFIL undergoes multiple iterations employing two virtual forces known as "pull" and "push." In each iteration step, the jammed nodes positioned outside the estimated jammed region exert a pull force, drawing the jammed region towards them. Conversely, unaffected nodes located within the estimated jammed region apply a push force, pushing the jammed region away from them.

Consider (X_0, Y_0) as the estimated jammer's position, (X_i, Y_i) as the position of a jammed node, and (X_j, Y_j) as the location of an affected node. We represent the forces F_i (pull) and F_j (push) as normalized vectors, indicating their directions relative to the estimated jammer's position.

$$\begin{aligned} F^i_{\text{pull}} &= \left[\frac{X_i - \widehat{X}_0}{\sqrt{(X_i - \widehat{X}_0)^2 + (Y_i - \widehat{Y}_0)^2}}, \frac{Y_i - \widehat{Y}_0}{\sqrt{(X_i - \widehat{X}_0)^2 + (Y_i - \widehat{Y}_0)^2}} \right], \\ F^j_{\text{push}} &= \left[\frac{\widehat{X}_0 - X_j}{\sqrt{(\widehat{X}_0 - X_j)^2 + (\widehat{Y}_0 - Y_j)^2}}, \frac{\widehat{Y}_0 - Y_j}{\sqrt{(\widehat{X}_0 - X_j)^2 + (\widehat{Y}_0 - Y_j)^2}} \right] \end{aligned} \tag{3}$$

Liu et al. [26] choose a threshold of 100 iterations as the stop point during the adjustment of virtual force.

4) Double Circle Localization (DCL): DCL [23] relies on the fundamental concepts of the Maximum Inscribed Circle (MIC) and the Minimum Bounding Circle (MBC). In this framework, the MBC represents the smallest circles that can be inscribed, whereas the MIC corresponds to the largest circle that can be inscribed within the convex hull formed by a collection of jammed nodes. Utilizing the DCL method enhances the accuracy of identifying the jammer's position [28], providing a more robust confidence level.

DCL determine the final values for both the Minimum Bounding Circle (MBC) and Maximum Inscribed Circle (MIC) by calculating their respective average values, as described in the following equations:

$$\begin{aligned} (X_{MBC}, Y_{MBC}) &= \left(\frac{X_{mbc} + X'_{mbc}}{2}, \frac{Y_{mbc} + Y'_{mbc}}{2} \right), \\ (X_{MIC}, Y_{MIC}) &= \left(\frac{X_{mic} + X'_{mic}}{2}, \frac{Y_{mic} + Y'_{mic}}{2} \right) \end{aligned} \tag{4}$$

Ultimately, obtain the outcome by applying the following equation:

$$\begin{aligned} (\widehat{X}_{\text{jammer}}, \widehat{Y}_{\text{jammer}}) = (&w_1 X_{MBC} + w_2 Y_{MIC}, \\ &w_1 Y_{MBC} + w_2 X_{MIC}) \end{aligned} \tag{5}$$

Where (X_{mbc}, Y_{mbc}) and (X_{mic}, Y_{mic}) are the circle centers of MBC and MIC, the values for the w can be obtained by either an empirical approach under the condition of $w_1 + w_2 = 1$.

In the paper [23], Cheng et al. proposed a jammer localization algorithm named DCL. The proposed approach DCL is compared with three existing algorithms, CL, WCL, and VFIL [26], and makes a comprehensive comparison through simulation and experiments. Moreover, the researchers perform experiments in isotropy jammer scenarios and change the direction of the jammer's antenna to imitate the anisotropy jammer scenario.

5) Particle Swarm Optimization (PSO): In their study, Pang et al. [22] introduced a novel approach for pinpointing the origin of an attacker through the utilization of the PSO. This PSO algorithm was applied to determine the minimum covering circle encompassing the jammed positions, which served as an estimate of the jammer's location. The researchers conducted simulations using Matlab and assessed their method's performance by comparing the estimated jammer location's Euclidean distance to the actual jammer location within the network.

6) Antenna Identification and Localization: The authors in [29] introduce an enhanced method called Antenna Identification and Localization of the Jammer (AIJL) to address the challenges of locating jammers in unconventional environments. This technique takes into consideration both jammed nodes and boundary nodes when determining the jammer's position. Their approach can be divided into two main steps. First, they compute the convex hulls of the jammed nodes and the boundary nodes. Second, within these convex hulls, they calculate the circumcircles of the clusters formed by these nodes. To determine the circumcircle, they select three nodes: the first two are the farthest two points within the convex hull, and the third node is the farthest from the midpoint of the previous two points. This process results in circumcircles for both the jammed nodes and the boundary nodes. The estimated jammer location is then determined as the orthocenter of these two circumcircles.

7) Monotone chain algorithm: Alikh and Rajabzadeh [30] presented a novel approach for detecting and localizing jamming attacks within wireless sensor networks. Their method employs a lightweight security mechanism and falls under the range-free localization category, utilizing the Monotone Chain algorithm (MC). Simulations were conducted using Matlab. However, it's worth noting that the authors did not specify the type or characteristics of the jammer in their study.

In contrast to the methodologies examined in the literature review, our methodology was evaluated within a simulation environment that closely emulates real-world conditions. Specifically, we employed the Contiki 3.1 operating system in conjunction with the Cooja Simulation tool. On the other hand, other approaches were tested using the Matlab software inside a predetermined experimental configuration. Our methodology primarily centered on utilizing measurements

derived from the network layer to facilitate the localization process. This study examined six unique network topologies, three of which were based on a grid structure. This topology is characterized by its structured layout, where nodes are evenly spaced in a grid pattern. The predictable and orderly arrangement allows for systematic assessment of the localization algorithms. It provides a controlled environment to observe the effects of jamming with minimal external variability, facilitating clear comparisons of algorithm performance under uniform conditions. At the same time, the remaining three were randomized, considering the influence of the sink's position. Contrasting with the grid arrangement, the random topology features nodes distributed in a non-uniform manner, mimicking more realistic and chaotic deployment scenarios often encountered in urban and rural IoT settings. This topology tests the robustness and adaptability of the localization algorithms in handling irregular node distributions and the complexities introduced by environmental unpredictability and node density variations. Furthermore, we manipulated the placement of the jammer in order to comprehend its impact. Significantly, our approach facilitated instantaneous identification and precise localization of geographical positions.

III. Modified Multilateration Localization Algorithm with Weights (MMLAW)

This section describes the new proposed MMLAW algorithm using multilateration and estimating distance using two network layer metrics, retransmissions, and ETX. The proposed MMLAW methodology performs the localization strategy more accurately and faster than other approaches CL [24], SC, DCL [23], and VFIL [26]. Moreover, this paper successfully identifies the position of the four different jammers. To identify them, we use the following metrics as weights in the algorithm: i) the packet Retransmissions and ii) ETX.

Detection Module The first step of our solution is to use the FLIDS [8], [9] approach to detect the jammer. FLIDS is a lightweight Fuzzy logic-based intrusion detection system to detect jamming attacks in IoT and WSN networks accurately. FLIDS uses network and Mac layer input metrics, indicating a jamming index as output. FLIDS uses the metrics of retransmissions and ETX to detect different types of jammers in the Routing Protocol for Low-Power and Lossy Networks (RPL). In this work, we examine the detection methodology, where we split the network into one-minute duration portions to perform real-time and more accurate results. Another improvement of the previous work is to perform normalization of the input values before feeding the FLIDS. This improvement helps the solution to adjust automatically to changes in the environment or behavior of the jammer. A more detailed analysis of the approach is examined in our previous work [8], [9].

Localization Module Our solution's second step is accurately locating the jammer after the detection module alarm. In this module, the algorithm predicts a jammer position and gives us the jammer's predicted (x,y) coordinates. We evaluated our approach based on two metrics: first, we calculated the error using the Euclidean distance, and second, we calculated the Execution time algorithm to evaluate the performance.

The proposed MMLAW method employs geometric calculations through multilateration, which relies on jammed nodes' x and y coordinates and the distances between the jammer and these nodes. This study introduces an innovative distance calculation method, leveraging the most suitable metric identified in our prior research [8], [9], where retransmissions are the best metric. Incorporating a detection metric into the weight of the examination algorithm can boost localization accuracy. Traditional algorithms like WCL use signal strength, notably RSSI, as their weight determinant. However, this can be influenced by multi-path propagation, shadowing, and interference. Detection metrics, on the other hand, provide a richer data source to enhance localization. They also offer insights into current network conditions and the environment. Integrating these metrics makes the proposed algorithm more adaptive to real-time network situations. In the following paragraph, we explain why we selected the Retransmissions as a weight to our proposed algorithm:

1) **Simplicity**: Retransmissions are easily measured and directly signify link quality.
2) **Network Quality Indicator**: Retransmissions reflect network link quality, pointing to interference, congestion, or weak signals.
3) **Metric Reliability**: Retransmissions have proven the most reliable after testing metrics like ETX or PDPT using brute force investigation.
4) **ETX Limitations**: ETX accounts for packet loss in both directions, possibly obscuring specific link quality.
5) **PDPT Limitations**: Being probabilistic, PDPT can fluctuate, whereas retransmissions offer more stability.

Multilateration is a widely used approach to determine the location of a target. This method requires a minimum of three anchor nodes to perform 2-D space localization. The equations representing multilateration are expressed as follows [31], [32]:

$$\begin{cases} (x-x_1)^2+(y-y_1)^2=d_1^2 \\ (x-x_2)^2+(y-y_2)^2=d_2^2 \\ \vdots\vdots\vdots \\ (x-x_N)^2+(y-y_N)^2=d_N^2 \end{cases} \tag{6}$$

Where: (x, y) is the coordinates of the unknown nodes in this case, the coordinates of the jammer, $(x_1, y_1), (x_2, y_2)...(x_N, y_N)$ are the coordinates of the N anchor and d is the distance between the anchor nodes. Then, this non-linear system of equations must be solved using suitable methods to obtain the unknowns x and y.

The Distance calculation in case of retransmissions is based on the following quotation:

$$d = w * \frac{1}{r^2}$$

w = weight to adjust the value, r = the normalized value of retransmissions The retransmissions are inversely proportional to the distance. The higher value of retransmissions indicates that the node is near the jammer. The parameter 'w' serves as a weight for value adjustment. To optimize this value, we conducted simulations from 0 to 20. Our analysis determined

that the optimal weight for achieving the best results is 10. The Distance calculation in the case of ETX is based on the following quotation:

$$d = w * r$$

w = weight to adjust the value, r = the normalized value of ETX The ETX is proportional to the distance value. The lower value of ETX indicates that the node is near the jammer. The parameter 'w' serves as a weight for value adjustment. To optimize this value, we conducted simulations from 0 to 30. Our analysis determined that the optimal weight for achieving the best results is 20.

Our approach utilizes the above information related to multirateration, and we have concluded the implementation of the Alg. 1 that utilizes the Retransmissions or ETX as distance.

Algorithm 1: Proposed Localization Algorithm - MMLAW

Require: Jammer_affected_nodes
Ensure: Estimated position (x_result, y_result) and error

position_change $\leftarrow 0$
$N \leftarrow$ length(Jammer_affected_nodes)
if $N > 2$ **then**
  Initialize arrays: $x[1 \dots N]$, $y[1 \dots N]$, $d[1 \dots N]$
  for $i = 1$ to N **do**
    $x[i] \leftarrow$ Jammer_affected_nodes$[i][1]$
    $y[i] \leftarrow$ Jammer_affected_nodes$[i][2]$
    $d[i] \leftarrow$ result_d
  end for
  Initialize matrices: $A[1 \dots N-1, 1 \dots 2]$, $B[1 \dots N-1]$
  for $i = 1$ to $N-1$ **do**
    $A[i,1] \leftarrow 2 \times (x[i+1] - x[1])$
    $A[i,2] \leftarrow 2 \times (y[i+1] - y[1])$
    $B[i] \leftarrow d[1]^2 - d[i+1]^2 - x[1]^2 - y[1]^2 + x[i+1]^2 + y[i+1]^2$
  end for
  result $\leftarrow$ linear system solver of A and B
end if

IV. Performance Evaluation

In this section, we describe the findings of our research. We compare our Proposed Localization Algorithm - MMLAW, with the competitive approaches found in the open literature and shown in Section II-A.

A. Discussion of Results

In this section, we provide a comprehensive analysis of the performance of our proposed MMLAW technique relative to existing algorithms, utilizing two key metrics: Euclidean Distance Error in meters and Execution Time in seconds. We first calculate the Euclidean Distance Error between the actual jammer position and our predictive estimates. Our findings reveal that our proposed MMLAW technique exhibits significantly lower distance errors when compared to the Centroid, Double Circle, Single Circle [1], and VFIL. Fig. 1 examines the Euclidean distance errors associated with several jamming approaches in a randomly generated topology. The evaluated approaches encompass MMLAW - Retransmissions, MMLAW - ETX, Centroid, Single Circle, Double Circle, and VFIL. These methods were tested against Deceptive, Constant, Random, and Reactive jammers. The key findings indicate that for the Random Placement Topology, the proposed MMLAW with Retransmissions algorithm is consistently superior, irrespective of the type of Jammer. MMLAW with ETX is better than the Centroid for the Constant and Random Jammers and worse for the Deceptive and Reactive Jammers.

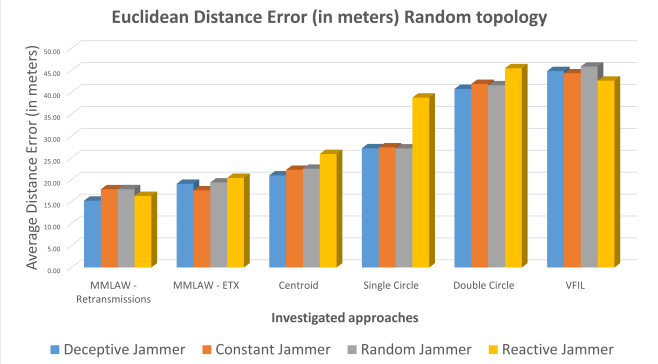

Fig. 1: Euclidean Distance Error (in meters) Random topology

Fig. 2 examines and compares the distance estimation errors in Euclidean distance across multiple methods in a 5x5 grid topology while considering alternative jamming models. Again, it was found that the MMLAW variants exhibited the lowest error rates, whereas VFIL demonstrated the greatest error rates. The MMLAW - ETX exhibited the lowest error rate, measuring 6.51 meters among the several constant jammers considered. With random jammers, the MMLAW - Retransmissions and ETX algorithms exhibited comparable performance, with errors of approximately 6.35 meters. Compared to MMLAW - ETX, MMLAW - Retransmissions had a slightly superior performance of 8.61 meters as opposed to 8.86 meters against reactive jammers. In general, the MMLAW - ETX consistently exhibited the fewest errors, hence suggesting its robustness. On the other hand, it was shown that VFIL frequently displayed the most significant faults, indicating possible weaknesses within a grid system.

[1]The **Single Circles Localization** (SCL) or **Single Differential Circles Localization** (SDCL) approach introduced by us, employs a geometric method to determine the position of a jammer within a network. This algorithm processes datasets containing positions of nodes, distinguishing between *jammed* and *boundary* nodes based on their connectivity status. It utilizes the concept of *minimum bounding circles* (MBC), which are calculated separately for both jammed and boundary nodes using Welzl's algorithm. Welzl's algorithm efficiently finds the smallest enclosing circle for a set of points. The differential component of SDCL is realized by computing two MBCs: one for boundary nodes ($MBC_{boundary}$) and another for jammed nodes (MBC_{jammed}). The estimated position of the jammer is then derived by analyzing the geometric differences between these two circles, specifically their centers and radii. This approach allows for refined estimation by accounting for variations in node distribution affected by the jamming signal, thereby enhancing localization accuracy in environments where traditional methods might be compromised by noise and signal distortion.

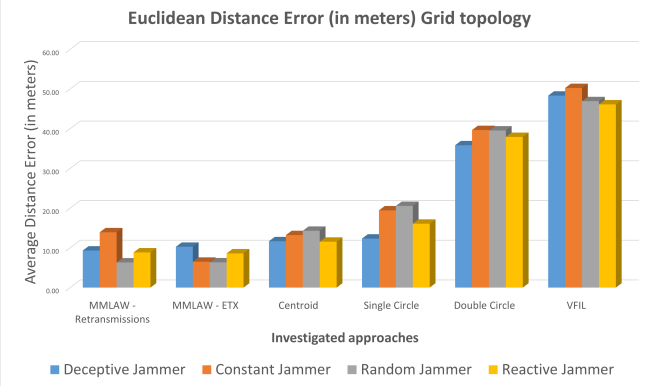

Fig. 2: Euclidean Distance Error (in meters) Grid topology

Fig. 3 presents the performance evaluation in terms of the execution time. Among the strategies employed, the Centroid method had the highest efficiency level, with a processing time of about 0.33 milliseconds, except for the minor efficiency decrease to 12.19 ms under the influence of the Constant Jammer. In summary, Centroid consistently showed the lowest execution times among all jammers, while VFIL frequently exhibited the highest execution times. The effectiveness of alternative tactics shows variability depending on the type of jammer, underscoring the need to take into account the specific jamming scenario when choosing an approach.

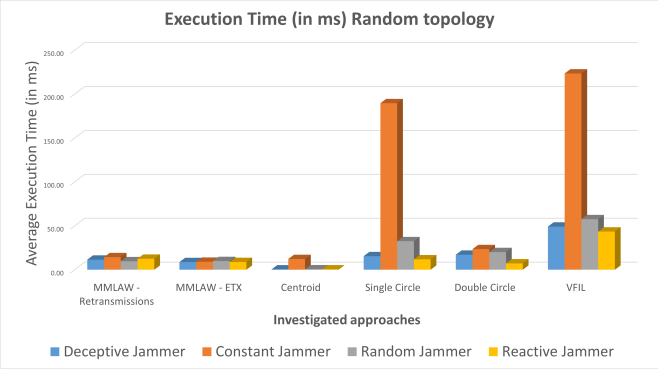

Fig. 3: Execution Time (in ms) Random topology

Fig. 4 comprehensively analyzes execution durations for different jamming types and strategies inside a grid layout. The CL is the fastest, VFIL is the slowest, while the two proposed algorithms are the second and third best (and overall better than Single Circle, Double Circle, and VFIL). The MMLAW - retransmissions and ETX values exhibited variability depending on the presence of a jammer, but the timings for single and double circles fell within the mid-range.

The key observations from the analysis include:

- **MMLAW - ETX** and **MMLAW - Retransmissions** generally exhibited the lowest error rates, with the former especially resilient in grid topologies.
- **Centroid** consistently emerged as the most time-efficient across all jammer types and topologies. Nevertheless, the proposed methodologies exhibit only a marginal deviation from the centroid time.
- **VFIL** displayed longer processing times and high error rates, highlighting potential weaknesses in real-time scenarios.
- **Single Circle** maintained a stable mid-range error performance across different jammers.

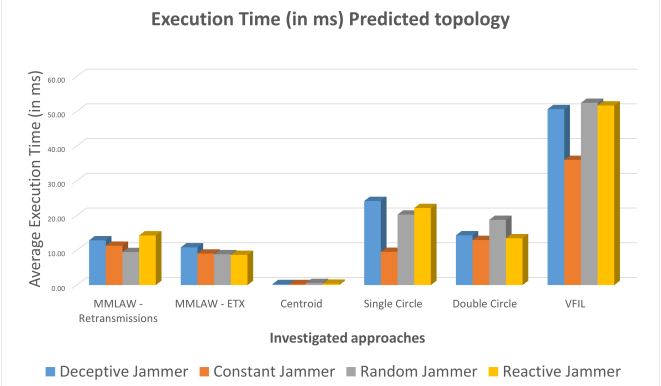

Fig. 4: Execution Time (in ms) Grid topology

In summary, it is evident that both Centroid and the Proposed MMLAW methods provide exceptional speed, although the MMLAW - Retransmissions with the MMLAW - ETX exhibit superior accuracy. However, it is crucial to underscore the significance of customizing jamming strategies according to unique situations and forms of interference in order to achieve ideal outcomes. The persistent difficulties encountered with VFIL indicate a necessity for its continued improvement or careful implementation.

V. Final Conclusions and Future Work

This paper introduces an innovative approach for detecting jammers in IoT environments. We conducted extensive simulations within the Contiki OS and Cooja Simulation tool, exploring diverse scenarios in the context of the RPL network protocol. To begin with, we employed Fuzzy logic algorithms to carry out the detection phase. We leveraged a Modified Multilateration Localization Algorithm with Weights (MMLAW) for the Localization phase, incorporating distance estimation through the network layer metrics. We perform local detection and localization at the edge. Our evaluation of this novel technique demonstrates its ability to accurately pinpoint jammers while maintaining a remarkably efficient execution time.

Acknowledgement

This work has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 739578, the ADROIT6G project of the SNS-JU under Grant Agreement No. 101095363, and the Government of the Republic of Cyprus through the Deputy Ministry of Research, Innovation and Digital Policy.

References

[1] D. Hendricks, "The Trouble with the Internet of Things," *London Datastore. Greater London Authority. Retrieved*, vol. 10, 2015.

[2] M. Surendar and A. Umamakeswari, "InDReS: An Intrusion Detection and Response System for Internet of Things with 6LoWPAN," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1903–1908, IEEE, 2016.

[3] M. López, A. Peinado, and A. Ortiz, "An extensive validation of a sir epidemic model to study the propagation of jamming attacks against iot wireless networks," *Computer Networks*, vol. 165, p. 106945, 2019.

[4] J. Deogirikar and A. Vidhate, "Security Attacks in IoT: A Survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 32–37, IEEE, 2017.

[5] S. Jaitly, H. Malhotra, and B. Bhushan, "Security Vulnerabilities and Countermeasures Against Jamming Attacks in Wireless Sensor Networks: A Survey," in *Computer, Communications and Electronics (Comptelix), 2017 International Conference on*, pp. 559–564, IEEE, 2017.

[6] K. Grover, A. Lim, and Q. Yang, "Jamming and Anti-Jamming Techniques in Wireless Networks: a Survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[7] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *arXiv preprint arXiv:2101.00292*, 2021.

[8] M. Savva, I. Ioannou, and V. Vassiliou, "Fuzzy-logic based ids for detecting jamming attacks in wireless mesh iot networks," in *2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet)*, pp. 54–63, 2022.

[9] M. Savva, I. Ioannou, and V. Vassiliou, "Performance evaluation of a fuzzy logic-based ids (flids) technique for the detection of different types of jamming attacks in iot networks," in *2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet)*, pp. 93–100, 2023.

[10] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free Localization Schemes for Large Scale Sensor Networks," in *Proceedings of the 9th annual international conference on Mobile computing and networking*, pp. 81–95, 2003.

[11] W. Dargie and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*. John Wiley & Sons, 2010.

[12] A. Kumar, N. Chand, V. Kumar, and V. Kumar, "Range Free Localization Schemes for Wireless Sensor Networks," *International journal of Computer Networks & Communications*, vol. 3, no. 6, p. 115, 2011.

[13] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks*. John Wiley & Sons, 2007.

[14] S.-Y. Kim and O.-H. Kwon, "Location Estimation Based on Edge Weights in Wireless Sensor Networks," *The Journal of Korean Institute of Communications and Information Sciences*, vol. 30, no. 10A, pp. 938–948, 2005.

[15] C.-Y. Chong and S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, 2003.

[16] X.-Y. Li, P.-J. Wan, and O. Frieder, "Coverage in Wireless ad hoc Sensor Networks," *IEEE Transactions on computers*, vol. 52, no. 6, pp. 753–763, 2003.

[17] A. Ademuwagun, V. Fabio, *et al.*, "Reach Centroid Localization Algorithm," *Wireless Sensor Network*, vol. 9, no. 02, p. 87, 2017.

[18] R. Nagpal, H. Shrobe, and J. Bachrach, "Organizing a Global Coordinate System from Local Information on an ad hoc Sensor Network," in *Information processing in sensor networks*, pp. 333–348, Springer, 2003.

[19] L. Lazos and R. Poovendran, "SeRLoc: Secure Range-independent Localization for Wireless Sensor Networks," in *Proceedings of the 3rd ACM workshop on Wireless security*, pp. 21–30, 2004.

[20] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 32–43, 2000.

[21] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost Outdoor Localization for Very Small Devices," *IEEE personal communications*, vol. 7, no. 5, pp. 28–34, 2000.

[22] L. Pang, X. Chen, Z. Xue, and R. Khatoun, "A Novel Range-free Jammer Localization Solution in Wireless Network by Using PSO Algorithm," in *International Conference of Pioneering Computer Scientists, Engineers and Educators*, pp. 198–211, Springer, 2017.

[23] T. Cheng, P. Li, and S. Zhu, "An Algorithm for Jammer Localization in Wireless Sensor Networks," in *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, pp. 724–731, IEEE, 2012.

[24] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S. V. Krishnamurthy, "Lightweight jammer localization in wireless networks: System design and implementation," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pp. 1–6, IEEE, 2009.

[25] J. Blumenthal, R. Grossmann, F. Golatowski, and D. Timmermann, "Weighted centroid localization in zigbee-based sensor networks," in *2007 IEEE international symposium on intelligent signal processing*, pp. 1–6, IEEE, 2007.

[26] H. Liu, X. Wenyuan, Y. Chen, and Z. Liu, "Localizing Jammers in Wireless Networks," in *2009 IEEE International Conference on Pervasive Computing and Communications*, pp. 1–6, IEEE, 2009.

[27] Z.-m. Wang and Y. Zheng, "The Study of the Weighted Centroid Localization Algorithm Based on RSSI," in *2014 International Conference on Wireless Communication and Sensor Network*, pp. 276–279, IEEE, 2014.

[28] H. Inchana and S. K. BJ, "Double circle localization for the detection of jamming attack in wireless sensor network," in *2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, pp. 1–5, IEEE, 2022.

[29] J. Fan, T. Liang, T. Wang, and J. Liu, "Identification and Localization of the Jammer in Wireless Sensor Networks," *The Computer Journal*, vol. 62, no. 10, pp. 1515–1527, 2019.

[30] N. Alikh and A. Rajabzadeh, "Using a lightweight security mechanism to detect and localize jamming attack in wireless sensor networks," *Optik*, vol. 271, p. 170099, 2022.

[31] H. Shi, "A new weighted centroid localization algorithm based on rssi," in *2012 IEEE International Conference on Information and Automation*, pp. 137–141, IEEE, 2012.

[32] J. Du, *Indoor localization techniques for wireless sensor networks*. PhD thesis, université de Nantes, 2018.