Sensor-Assisted Monte Carlo Segmentation with Robustness Boost for WSN and IOT

Dr. A. Avani

Assistant Professor, Department of CSE, Anu Bose Institute of Technology, Paloncha, India

avanialla@gmail.com

ABSTRACT:

Knowing where the geo-location sensor data was gathered from is crucial for scattered sensor systems, particularly in instances involving mobile sensors, which are often encountered in wireless sensor networks or the Internet of Things. With the exception of a radio, which is already present on sensor nodes, range-free Monte Carlo localization-based techniques are relatively energy efficient. However, the incorporation of motion sensor data based dead reckoning considerably enhances location estimations' accuracy and provides resilience against erroneous or hostile network actors. In this paper, we offer a robust sensor-assisted Monte Carlo localization method (RESA-MCL). We demonstrate the efficiency of RESA-MCL in terms of general localization accuracy as well as resilience against malicious assaults or malfunctioning nodes. We offer three attack scenarios based on malicious anchor nodes to assess and contrast our strategy against previous approaches. RESA-performance MCL's are assessed using these attack models, and our method outperforms other methods in conditions of both extremely low and high anchor node density, obtaining a localization error of 0.5 with an anchor density of 0.33. Overall, RESA-MCL does a better job than similar techniques at lower anchor density, reducing localization errors by up to 48%, and is much more resistant to attacks while requiring only a little more computing work.

I INTRODUCTION:

In the modern world, a growing number of Internet of Things (IoT) devices with various types of sensors, as well as Wireless Sensor Networks (WSN), are being deployed to cover a wide range of scenarios, from connected devices [9] to decentralised volunteer measures for evaluating air quality [2], [17], industrial uses [10], and wildlife monitoring [16]. Knowing where the data was recorded is crucial for understanding the

results. Since many applications depend on mobile sensors, sensor nodes must be able to detect their positions dynamically. For instance, in the case of a WSN with fixed nodes, the installation sites of each sensor may be documented. Utilizing the Geographic Information System is the most popular strategy for doing this (GPS). However, using GPS has a variety of drawbacks The sensors are expensive and use a lot of electricity. They also depend on being able to receive satellite signals, which makes it hard to operate indoors and also causes accuracy problems in certain outdoor settings. A solution to the first two issues is to only equip a limited number of nodes with GPS sensors. These nodes then serve as "seed" or "anchor" nodes, assisting other nodes with their own localization. The use of permanent anchors with predetermined positions is another popular strategy, in addition to the use of mobile anchor nodes equipped with GPS sensors. There are several localization algorithms. The two primary categories of them are range-based and range-free techniques. In range-based techniques, unknown nodes (nodes that are not anchor nodes and are trying to find themselves) must actively calculate their distance from anchor nodes or the angle at which they are receiving radio signals.

In these methods, typical measures include Angle of Arrival (AoA) [4], Time of Arrival (ToA) [21], Time Difference of Arrival (TDoA) [22], and Reception Signal Strength (RSS) [20] are all related terms. A common way to calculate the difference between an unknown node and an anchor node is to use RSS in conjunction with the proper propagation model. This method is predicated on the idea that the RSS drops proportionately as transmitter distance increases. However, several restrictions must be taken into account. For instance, in TDoA-based solutions, extremely accurate clock synchronisation among both nodes must be ensured; in AoA-based solutions, it's critical to take into account multipath, NLoS situations, and array configuration; and in Archive solutions, radio noise levels, multipathing, and experimental error can affect the results [21]. Range-based techniques, in general, generally need extra, specialised hardware, clock synchronisation, and greater power consumption to allow the active measurements that must be carried out by unidentified nodes. In some situations, the limitations of each type of measurement may also make it harder to get

a good idea of where something is. Research into range-free solutions, which are often based on connection alone, is performed in order to decrease complexity, hardware dependence, and energy expenses. These methods are simpler to build and require less money to distribute since active assessments from the unknown nodes are not necessary. The Monte Carlo Localization (MCL) algorithm, which Hu and Evans modified in 2004 [8] for positioning in mobile WSNs, is a well-known typical method in this area. Contrary to methods intended for partly or entirely static networks, MCL allows all nodes to move at will throughout time and takes advantage of the mobility to enhance the performance of localisation. In MCL, a collection of weighted samples (particles) is used to represent the probability distribution of each node's present location. A Bayesian filtering method eliminates impossible samples that are beyond the communication range of anchor nodes. The average of all remaining data after filtering serves as the projected node's position. MCL is appropriate for both mobile and stationary applications and needs no extra hardware. However, when communication between unknown nodes and anchor nodes only sometimes happens, MCL's performance soon deteriorates. As a result, while using MCL, ensuring a high anchor node density is crucial.

The security issues of customization have not been taken into account by any of the techniques so far. These techniques may not be as effective as they were in their studies if there are malevolent nodes in the network that report inaccurate positions. Even in the absence of malevolent nodes, a malfunctioning portion of the anchor nodes might cause performance deterioration or even the collapse of the whole system. For instance, in initiatives where connector nodes are statically distributed in the environment, if one or more of the anchor nodes are down, normal nodes nearby will not be able to get the data needed for clustering, such as RSS, TDoA, etc., which will result in a localization failure. ultimately result in localization failure. Furthermore, anchor node faults must be taken into account while developing the localization algorithms in order to make the suggested methodologies more appropriate for real-world circumstances.

In this work, we propose Corrosion resistance Enhanced Sensor Assisted Monte Carlo Localization (RESA-MCL), which helps improve the machine translation

scheme's resiliency against inaccurate information being streamed live by malicious anchor nodes while also achieving a higher localization accuracy compared to earlier schemes. In order to do this, RESA-MCL continually uses dead reckoning, as explained by Hartung et al. [7], as opposed to the previous SA-MCL method, which only did so when out of anchor range. A unique particle subsetting approach used by RESA-MCL reduces the impact that malicious anchor nodes may have on the position estimation while detecting malicious anchor nodes using motion-based plausibility checks. We carefully examine RESAMCL's functionality under several attack scenarios with up to 90% of malevolent anchor nodes and use data-driven parameter selection to guide our analysis.

The following is a summary of our paper's contributions:

(1) We suggest the RESA-MCL scheme, which, in highly flexible low anchor density situations, outperforms comparable describes a process with reduced computational complexity and also includes robustness augmentation to mitigate attacks and achieves higher localization accuracy (up to 48% lower error than comparable recent approach).

(2) Particular attack models are created for cases involving malicious or broken anchor nodes.

(3) Under three distinct assault scenarios, RESA-MCL and prior techniques are assessed and contrasted.

(4) RESA-performance MCL's in all attack models is significantly improved by robustness upgrades compared to methods without them.

(5) To confirm the advantageous characteristics of the method, such as minimal localization error at low anchor density and resilience to assaults, a thorough experimental assessment, including ablation trials, is employed.

(6) To facilitate future assessment and comparison with other methods, an improved version of the original MCL [8] emulator is given. This version includes representations of SA-MCL [7] and RESA-MCL.

II RELATED WORKS:

In recent years, a number of localization methods for WSNs and the IoT have been proposed. The most important component in relation to our work is the consideration of security considerations during localization. As a result, we provide summaries of comparable research divided into four categories: range-based, distance, AI-based, and access control techniques.

RANGE-BASED APPROACHES:

Numerous range-based localization strategies have been put forward, as was mentioned in section I. An RSS-based Localization Using Uncertain Data Mapping (LUDM) for WSN was suggested by Luo et al. [12]. The suggested technique performs better than existing options in terms of the absolute mean localization error, according to simulation findings. At the corners of the experiment area, the four anchor nodes are fixed statically. Also, when the RSS attenuation model is used to increase generalization in uncharted localization contexts, the accuracy of localization may drop by a lot.

A Time of Flight (ToF)-based localization technique for asynchronous WSN was suggested by Wang et al. in 2019 [18]. The simulation results show that the suggested method is better at figuring out where something is than traditional methods. However, the anchor nodes are once again statically distributed throughout the network, and localization is dependent on a central server. This server has to have enough processing power to estimate clock skews and carry out the localization procedure. If there are server problems, this might become a single point of failure for the whole localization process. The same authors suggested a different time-based joint synchronization and localization solution for asynchronous WSN in 2020 [19]. This approach makes use of TDoA. The localization processes are also launched by a centralized server. Simulation results show that this new strategy is better in situations where anchor placements are only partially known.

Its centralized design, however, creates a single point of failure.
A weighted approach for localization in 3D WSN based on RSS/AOA data was developed by Ding et al. in 2021 and given the name ENWLS [4]. It is based on error variance and measurement noise weighted least squares. When there are more than three anchor nodes in the scenario,

simulation findings demonstrate that ENWLS works better than other hybrid RSS/AOA localization algorithms currently in use. This suggests that in the event of anchor node failure, ENWLS is unreliable. Additionally, NLoS and multipath effects are not taken into account. Range-based techniques measure the distances between unknown nodes and anchor nodes in an effort to improve localization accuracy. However, they often need specialized gear or precise clock synchronization to carry out such tests.

Such systems may be hampered by multi-patching or other environmental factors as well. They are thus more difficult to use and more costly.

RANGE-FREE APPROACHES:

This is a typical range-free localization technique. It is described in Section I and needs no extra hardware. More crucially, MCL permits arbitrary movement over time for any network node, including anchors. Using a particle filter, node mobility is used to further improve localization accuracy. One of the prominent characteristics of MCL-based systems is strong mobility assistance.

Several range-free methods inspired by MCL have been proposed to improve localization accuracy and sampling effectiveness [15], [25]. These answers, however, are unable to resolve the original MCL algorithm. Low-cost 9-axis Inertial Measurement Unit (IMU) sensors use dead reckoning to bridge times without being connected to anchor nodes. Using the Differential Evolution optimization approach, Qin and Zhu [15] modified MCL to increase localization accuracy when there were few anchor nodes (MCL-DE). The MCL-DE chooses the sample weight as the objective function for optimization and uses the differential evolution method to get valid samples for location prediction in place of the conventional sample filtering and resampling procedures. The researchers discovered that MCL-DE had improved localization precision. The costs of computing and communication for the proposed plan, on the other hand, are not looked into, and security is not taken into account.

There are other range-free localization techniques that are not MCL-based. DV-Hop-based range-free algorithms are one popular subset of such methods. DV-Hop (CCDV-Hop) and Distributed Connectivity based DV-Hop (DCDV-Hop) are based on

the DV-Hop family of localization algorithms, while Gui et al. [6] developed a decentralised, range-free solution based on these approaches in 2020. However, the simulation results are only given for small and small-sized networks of up to 30 nodes, and malicious or dysfunctional anchor nodes are not taken into account. It was also only tested with extremely high counts of anchor nodes (50 percent of unknown nodes in the small network of 6 unknown nodes and 33.3% in the standard-sized network of 9 data instances) and high communication ranges in comparison to the small simulation areas (20 m in a 40 x 40 m2 or 60 x 60 m2 area), permitting each reporter node to cover a significant portion of the experimental site. The authors don't give a metric of anchor node density.

AI-BASED APPROACHES:

Researchers have combined artificial intelligence (AI) methods with range-based and range-free localization algorithms to provide fresh indoor and outdoor localization solutions. ConFi, the first indoor Wi-Fi localization technique based on a Convolutional Neural Network (CNN), was proposed by Chen et al. in 2017 [3]. It creates a time-frequency matrix that serves as the feature for localisation using Channel State Information (CSI). The authors carried out extensive trials to choose the CNN's parameters, and they also demonstrated that ConFi works better than the alternatives. However, a large number of samples are necessary to train the CNN. ConFi must be trained with a fresh dataset from the new environment in order to be used in that environment, which is not similar to the present one.

For both indoor and outdoor velodromes, Gharghan et al. [5] suggested an adaptive neural fuzzy inference system to calculate the separation between a moving bicycle (i.e., player) and a stationary coordinator node (i.e., coach). The suggested technique beats existing cutting-edge systems in terms of mean absolute error, according to simulation data. The complexity of the fuzzy inference system has a significant impact on how long the offline phase of the Adaptive Neural Fuzzy Inference System (ANFIS) training takes.

Also, the current method requires that the localization coordinates be taught to two ANFIS systems separately, which adds to the cost of training. researchers have also suggested methods that utilise AI techniques based on Wi-Fi fingerprints, such as HybLoc [1], which is a hybrid indoor

localization system for both room-level and latitude-longitude predictions. These methods are in addition to utilising CSI and RSS to train the neutral model. According to the findings of the simulation, HybLoc performs more accurately and precisely. Since the hardware requirements for the sensor nodes to have a quick response time in the prediction phase are not given, it is important to figure out if HybLoc is useful in real life.

Without re-training the model, HybLoc is also inapplicable for localization in a novel context, such as a building that is not included in the dataset, without re-training the model.
An indoor neural network-based localization method for WSNs that is specifically made to pinpoint the location of an Alzheimer's patient was suggested by Munadhil et al. [14]. Regarding the anchor nodes, they make use of RSS. The suggested strategy performs better than other earlier strategies in terms of mean absolute error, according to simulation data. To capture RSS samples, set up the network connection, and provide power for the experiment, the patient's mobile node has to be linked to a laptop. For the majority of real-world cases, this functional specification is unworkable. Additionally, the technique cannot easily be applied to other locations or mobile situations because of the static anchor nodes and the offline training process.
These AI-based methods are often computationally costly and typically only useful in the particular contexts for which they were taught. Additionally, each anchor node in these strategies is placed in a fixed location. They also fail to take into account the security ramifications of malevolent or defective anchor nodes, which might cause problems in real-world systems. In the end, it is important to recognise the system complexity and significant offline training costs of these AI models. Nevertheless, more general and light

SECURITY-AWARE APPROACHES:

Addressing security issues with localization is another important study area, in addition to enhancing localization accuracy, sampling effectiveness, and dealing with transitory connection loss. There are several suggested localization methods that consider security. A lightweight, secure ToA-based localization technique for WSNs was presented by Xie et al. in [21], taking advantage of the noise characteristics brought on by external distance assaults. This strategy primarily tries to ward off

impersonator assaults initiated by outside attackers.

With regard to range-based localization strategies, Liu et al. introduced the Malicious Node Detection algorithm based on Clustering and Consistency Evaluation (MNDC) as well as an improved secure localization variant known as EMDC [11]. They use density-based spatial clustering to find the strange node clusters. The next step is to find malicious nodes that compromise the networks using a sequential probability ratio test. The results of the simulations reveal that in terms of detection accuracy and efficiency, the suggested algorithms perform better than other cutting-edge plans. The sequential probability ratio test and the clustering algorithm's added processing burden are not explained, however. Furthermore, because there is no mechanism in place, malevolent anchor nodes cannot regain their reputations. It has more deployment demands than range-free schemes since it is a Span scheme.

A secure APIT-based range-free technique to find Sybil nodes within the network was suggested by Yuan et al. [24]. Sybil-free APIT (SF-APIT) is assessed with relatively large connectivity ranges (60 m in a 300 x 300 m2 area), but with a low percentage of anchor nodes compared to unknown nodes (10%). Low localization mistakes are achieved under these circumstances. However, since SF-APIT only works with traditional networks, malevolent anchor nodes that don't engage in Sybil attacks are not taken into account. There is no anchor density metric according to Hu and Evans' definition [8].

Existing security-aware approaches frequently concentrate on network structure-based attacks (such as wormhole or Sybil attacks), have high computational requirements, assume static networks, or make significant assumptions (such as the reliability of anchor nodes) that may not hold true in practical situations. When anchor or unknown nodes are believed to behave maliciously, it is common practise to either not provide a precise attack model for the behaviour of malicious nodes or to just identify such nodes and not provide instructions on how to proceed after that.

We suggest RESA-MCL, which combines the benefits of range-free methods, such as low cost and simplicity of deployment, with the improved resilience against assaults of secure localization techniques while still being extremely light. with regard to calculation. Because our system is completely decentralised, there is no single

point of failure and only the nodes themselves are needed for infrastructure. It is possible to identify malfunctioning or malicious anchor nodes and reduce their negative impact on localization precision.

We establish three distinct attack models for anchor nodes and compare our suggested technique to earlier ones in similar circumstances. Since RESA-MCL is built on MCL, it fully supports both unknown and anchor node mobility. Because there is no offline training phase or reliance on any location-specific data, RESAMCL may be utilised in any context and is not location-dependent. Less than 5% of the anchor nodes in our system are unknown, and our method works effectively with short communication distances (50 m in a 500 x 500 m2 region).

Overall, RESA-MCL may be installed with a minimum amount of hardware. Similar to SA-MCL, it makes use of sensor data from inexpensive and low-powered 9-axis Inertial Measurement Unit (IMU) sensors to improve detection performance and enable the identification of errant or malicious anchor nodes. The real authority parameters were measured presented by Hartung et al. [7] apply to RESA-MCL as well because it primarily consists of computationally cheap improvements to SA-MCL. This shows that RESA-deployment MCL's on low power devices IRIS sensor nodes [13] based on an 8 bit microcontroller and XBee (2.4 GHz 802.15.4) radio is feasible.

III LOCALIZATION SCHEME:

The SA-MCL scheme that was presented by Hartung et al. [7] serves as the foundation for RESA-MCL, to which a range of enhancements have been applied. These changes improve its overall accuracy and make it more resilient in networks where some nodes are broken or are being used for bad purposes.

The MCL [8] methodology serves as the foundation for SA-MCL. In what comes next, we'll briefly go over these methods again and then go into more detail about the changes made to RESA-MCL. The sign that is used at the beginning The MCL algorithm [8] may be broken down into two distinct parts. The first step The first phase consists of network connections, while the second phase is the implementation of an The location estimate process makes use of a particle filter. The essential information is required to bring the location information up-to-date. Compiled at a stage of the process of communication through a

network. Here, Anchor nodes are responsible for transmitting their positions. Nodes that are unidentified You will get this information straight from an anchor node, and then you will broadcast it again while noting that it is a rebroadcast. Nodes that are in receipt of Regardless of the kind of broadcast, the received location data should be stored. node IDs. This data is used by the nodes at predetermined times.

The particle filter itself is composed of two distinct stages: the prediction stage, and the filtering stage. At the beginning, N particles are generated by each unknown node. These dots in two-dimensional space, known as particles, stand in for potential locations of the unknown node. They are dispersed in a haphazard manner over the region of potential places. A close approximation of the probability distribution of possible node sites may be found in these particles. During the step when the prediction is made, each particle is moved to a new position within the radius that corresponds to the node's maximum speed. This method assures that, if no observations are made to restrict the distribution, its uncertainty will expand over time in line with the movement of the node. This is the case even if the distribution is observed. During the filter stage, the resampled particle is compared to the broadcasts that were received from the anchor nodes, and the retransmissions of those broadcasts that were sent two hops further are forwarded. If the particle is not located within the radio range of any of the anchor nodes, from which transmissions are received, or within the ring between one and two radio ranges in the case of 2-hop retransmissions, then the particle is discarded and a new particle is sampled in its place, which restarts the process.

Listing 1 provides a more in-depth explanation of the algorithm because the initial description of the algorithm leaves some room for interpretation. It does this by following the actual code given in the simulator made available by the authors, which includes additional information such as a relaxed acceptance criterion for particles during the filter step.

During the resembling process, the 'attempts' parameter indicates how many iterations, and thus how much time, should be spent searching for a group of particles that satisfy the range MCL requirements. The value of the 'attempts' parameter is set to 10000 when the algorithm is executed for the very first time; however, for future executions, the value is changed to 200. In addition, during

the execution of the more comprehensive initialization procedure, the while loop is executed via first completely deleting relaxed samples and then, if required, retaining them a second time. In the sake of clear communication.

The first version of the MCL algorithm makes use of a meet Condition function and does not include the extra particle sub-setting that was included in RESA-MCL.

By adding the 'enable Subset' argument to MCL and meet Condition, we eliminate the possibility of having two slightly distinct versions of the pseudo code. The "enable Subset" argument is always set to "false" in the MCL and meet Condition languages when it comes to the traditional MCL method. The meet Condition function analyses a given sample to determine whether or not it satisfies the filter criterion in its whole, just to a limited extent, or not at all. In the event where sufficient samples are located to completely satisfy the tight range criterion, the relaxed requirement is not applied. If this is not the case, the range is increased by meters, and particles that satisfy this more flexible requirement are also considered acceptable.

The resample In Radius(p,r) method produces a random, new point around the supplied point p that is still contained within the boundaries of the experimental region. The point must be located within the specified radius r and must be located within that radius. The choose(S,N) function takes as input a set S and an integer more than or equal to N. It then picks at most N members at random from the set S, but it never returns more than |S| elements.

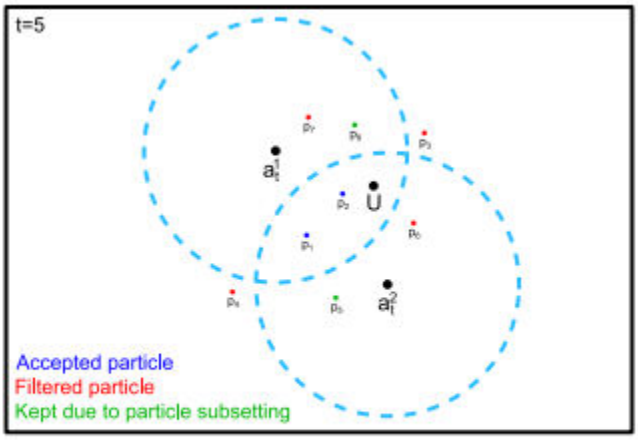

FIGURE 1. Example illustrating the particle subsetting process (S.III-D2) with two anchors, one unknown node U and $k \in \{1, 2, \ldots, 8\}$, $t = 5$, $j \in \{1, 2\}$.

IV EVALUATION:

EXPERIMENTAL SETUP:

The MCL and SA-MCL evaluations both make use of a Java-based simulator that was first designed for the MCL assessment and utilised for that evaluation. These evaluations make use of an enhanced and

improved version of that simulator. Code Ocean makes both the source code and the results of simulations open to the public. Our version of the simulator is one of such simulators. 1 This simulator is used to guarantee that the results of other MCL-based algorithms, such as SA-MCL, which often utilise the same code base as well, may be compared to those produced by this simulator.

Each experiment is carried out using a total of 300 nodes. At the beginning of each run, initial locations are decided upon in a completely arbitrary manner. 10 of these are used in some capacity as anchor nodes, unless otherwise noted. The radio communication range inside the experimental area is 50 metres, while the area itself is 500 square metres. The simulations are conducted for a total of a thousand steps, with each step signifying an interval of time equal to one second and one iteration of the localization process. Every one of these runs is carried out a further ten times with a new random seed. As explained by Yoon et al. [23], nodes move according to a modified version of the random waypoint movement model. Within this model, a maximum route segment endurance requirement and a least movement control of VMin are enforced in order to avoid movement from degrading to low average speeds.

To be more specific, the movement speeds are chosen at random from a range that extends from 10 m s1 to 20 m s1, and there is a restriction of no more than five time steps allowed for each section of the course. In order to take into account the impact that noisy sensors have on the assessment of our scheme and to make a fair comparison to SA-MCL, an error of 20% is added to both the speed and the direction that is perceived. In range-free localization techniques, RSS or connection quality between nodes is not addressed beyond the need of basic connectivity. This is because basic connectivity is all that is necessary.

Anchor density is defined by Hu and Evans [8] as the average number of anchor nodes that are located at a distance of one hop to unknown nodes. It is not feasible to offer a stable anchor density using this definition because of the mobility of the nodes and the randomization that occurs at the beginning. We conducted ten separate experiments, each consisting of 1000 steps, and found that the specified experimental settings resulted in an average anchor density of 0.327, with a standard deviation of 0.054. Error in

localization is expressed in all numbers as the radio range divided by the error in metres. This is the standard metric for range-free techniques.

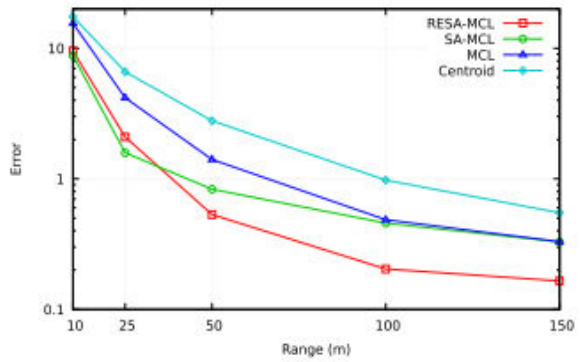

FIGURE 2. Comparison at different communication ranges without attack.

The findings presented in Section IV-C led to the conclusion that the particle subsetting parameters should be set to s = 3,s = 4 (which is equal to s = 12,s = 16) for all trials with the exception of those in which those values were expressly varied. This reduces the effect of malicious nodes while not having much of an effect on the performance of localization when there aren't any attacks. Evaluation is done on the performance of four range-free localization algorithms, namely Centroid, MCL, SA-MCL, and RESA-MCL, under the conditions of three distinct assault scenarios. In what follows, we will conduct an analysis of the findings of our tests.

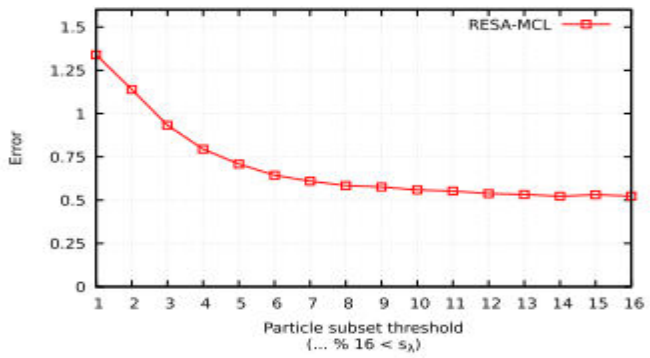

FIGURE 3. Evaluation of particle subset sizes without attacks and $s_\phi = 16$.

Within this section, we establish the settings that work well for the particle subsetting procedure described in Section III-D2. Figure 3 illustrates how well RESA-MCL performs in a case when there are no assaults, using a threshold value of 16, and varying values for the s parameter (threshold). In a scenario in which s = s = 16, there is no subsetting of the particles, but in a scenario in which s = 1, just one particle in every 16 is impacted by an anchor node. It is possible to demonstrate that, for s 8

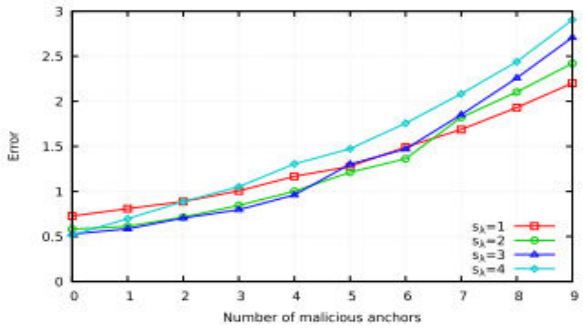

FIGURE 4. Evaluation of particle subset sizes under fixed position attack with $s_\phi = 4$.

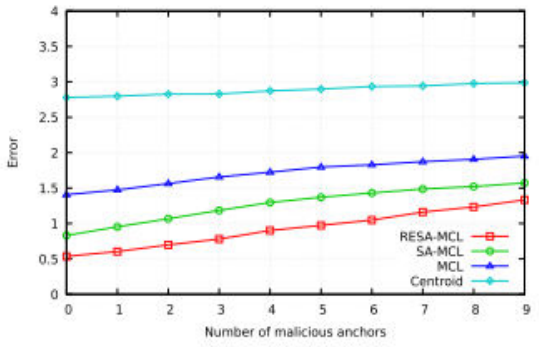

FIGURE 5. Biased position attack.

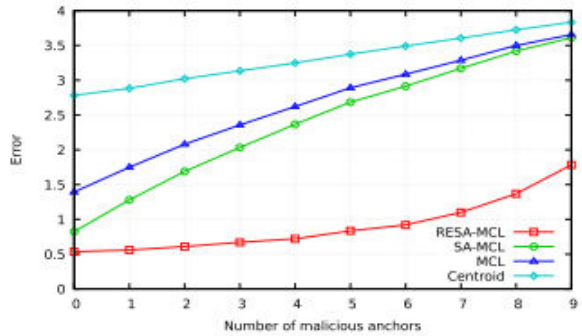

FIGURE 6. Random position attack.

Error in localization rises precipitously as s decreases, but as s reaches 12 or above, the performance of localization is only marginally impacted by particle subsetting.

As can be seen in Figure 4, a more limited particle subsetting renders RESA-MCL more resistant to assaults. This assessment will focus on the fixed position assault since it was determined to be the most successful attack in Section IV-D3, which prompted this decision. Because of the findings shown in Picture 3, as well as in order to make the figure easier to read, we have divided both s and s by 4, and we have shown the results for s ranging from 1 to 4, since these are the tradeoff points that are most important.

According to Section IV-B, the least subsetting performs the best in the case when there are no assaults, while the performance of s = 3 is practically identical to that of the least subsetting. In situations in which 10% to 40% of the anchor nodes are malicious, s = 3 works the best, but more aggressive subsetting is more successful in situations in which 50% or more of the anchor nodes are malicious. We conclude that a network in which the majority of the nodes are malicious is a less common scenario, thus we settle on s = 3 as a suitable trade-off between resilience and the precision of localization in networks that are not under assault. Therefore, s = 3 will be the starting point for all subsequent tests.

V CONCLUSION AND FUTURE WORKS:

We present RESA-MCL, a novel MCL-based, range-free, security-aware localization algorithm for wireless sensor networks (WSNs) and the Internet of Things (IoT) that strongly outperforms comparable approaches both in safe situations and under attack by malicious anchor nodes. This work is part of our ongoing research on wireless

sensor networks. Without any attacks, it outperforms a recent solution that is comparable to it by 48%, achieving a reduced localization error at anchor densities that are comparable. Three different approaches are used by RESA-MCL in order to strengthen its resistance to malicious anchor nodes and improve the accuracy of general localization. Both very sparse networks with a small number of anchor nodes and extremely dense networks with a large number of anchor nodes lead to improvements in the accuracy of the localization process. Additional contributions include the invention of three distinct attack models against localization techniques in wireless sensor networks (WSNs) and the internet of things (IoT). These models are based on the premise that certain anchor nodes are either malicious or dysfunctional. We assess the earlier techniques, Centroid, MCL, and SA-MCL, under these assault scenarios and find that all three of them are significantly impacted by the attacks. In contrast, we show that RESA-MCL is resistant to assaults using all three types of attack models and show that its localization error only rises minimally even when there are 30% malicious anchor nodes present in the most effective kind of attack model, which is the fixed position attack model.

In addition, we present a very comprehensive reformalization of the original MCL technique via the use of pseudocode and propose the concept of 2-hop plausibility testing, which has the potential to boost the network's resistance against malevolent unknown nodes. This reformulation incorporates implementation details that were previously only available in the simulation created by the original author. We also give researchers a version of the simulator that works better and has fewer bugs so that it will be easier for them to use MCL-based methods in the future. We have optimised and improved the simulation software that was originally given so that future research can compare these different methods more easily by Hu and Evans [8] and Hartung et al. [7] and then make it accessible on CodeOcean. [8] (see Section IV).

In the future, we want to examine other attack models, such as mixed attack methods, malevolent unknown nodes, as well as the efficacy of modified versions of the functionality of the 2-hop plausibility check. In addition to this, we want to look at methods to improve the efficiency of

verifying implausible location data while also lowering the number of false positives. In addition, we want to confirm the outcomes of our simulations by testing our technique in a testbed that replicates the actual world. One other strategy for improving the accuracy of the localization that we want to investigate is making the technique topology-aware, which will enable it to remove inaccessible terrain from the positions of the particles.

REFERENCE:

[1] B. A. Akram, A. H. Akbar, and O. Shafiq, ‘‘HybLoc: Hybrid indoor Wi-Fi localization using soft clustering-based random decision forest ensembles,’’ IEEE Access, vol. 6, pp. 38251–38272, 2018.

[2] N. Castell, F. R. Dauge, P. Schneider, M. Vogt, U. Lerner, B. Fishbain, D. Broday, and A. Bartonova, ‘‘Can commercial low-cost sensor platforms contribute to air quality monitoring and exposure estimates?’’ Environ. Int., vol. 99, pp. 293–302, Feb. 2017.

[3] H. Chen, Y. Zhang, W. Li, X. Tao, and P. Zhang, ‘‘ConFi: Convolutional neural networks based indoor Wi-Fi localization using channel state information,’’ IEEE Access, vol. 5, pp. 18066–18074, 2017.

[4] W. Ding, S. Chang, and J. Li, ‘‘A novel weighted localization method in wireless sensor networks based on hybrid RSS/AoA measurements,’’ IEEE Access, vol. 9, pp. 150677–150685, 2021.

[5] S. K. Gharghan, R. Nordin, A. M. Jawad, H. M. Jawad, and M. Ismail, ‘‘Adaptive neural fuzzy inference system for accurate localization of wireless sensor network in outdoor and indoor cycling applications,’’ IEEE Access, vol. 6, pp. 38475–38489, 2018.

[6] L. Gui, F. Xiao, Y. Zhou, F. Shu, and T. Val, ‘‘Connectivity based DV-Hop localization for Internet of Things,’’ IEEE Trans. Veh. Technol., vol. 69, no. 8, pp. 8949–8958, Aug. 2020.

[7] S. Hartung, A. Bochem, A. Zdziarstek, and D. Hogrefe, ‘‘Applied sensorassisted Monte Carlo localization for mobile wireless sensor networks,’’ in Proc. Int. Conf. Embedded Wireless Syst. Netw. (EWSN), Graz, Austria, Feb. 2016, pp. 181–192.

[8] L. Hu and D. Evans, ‘‘Localization for mobile sensor networks,’’ in Proc. 10th

Annu. Int. Conf. Mobile Comput. Netw., Phildadelphia, PA, USA, 2004, pp. 45–57.

[9] A. Kanev, A. Nasteka, C. Bessonova, D. Nevmerzhitsky, A. Silaev, A. Efremov, and K. Nikiforova, ‘‘Anomaly detection in wireless sensor network of the ‘smart home’ system,’’ in Proc. 20th Conf. Open Innov. Assoc. (FRUCT), Apr. 2017, pp. 118–124.

[10] M. Liu, K. Yang, N. Zhao, Y. Chen, H. Song, and F. Gong, ‘‘Intelligent signal classification in industrial distributed wireless sensor networks based industrial Internet of Things,’’ IEEE Trans. Ind. Informat., vol. 17, no. 7, pp. 4946–4956, Jul. 2021.

[11] X. Liu, S. Su, F. Han, Y. Liu, and Z. Pan, ‘‘A range-based secure localization algorithm for wireless sensor networks,’’ IEEE Sensors J., vol. 19, no. 2, pp. 785–796, Jan. 2019.

[12] Q. Luo, Y. Peng, J. Li, and X. Peng, ‘‘RSSI-based localization through uncertain data mapping for wireless sensor networks,’’ IEEE Sensors J., vol. 16, no. 9, pp. 3155–3162, May 2016.

[13] MEMSIC. (2010). IRIS OEM Datasheet. Accessed: Jan. 22, 2022. [Online]. Available: http://static6.arrow.com/aropdfconversion/8f126c9f83e22fabed80e2c01b513ad4960db1ea/6020-0123-02_a_iris_ oem_edition-t.pdf

[14] Z. Munadhil, S. K. Gharghan, A. H. Mutlag, A. Al-Naji, and J. Chahl, ‘‘Neural network-based Alzheimer’s patient localization for wireless sensor network in an indoor environment,’’ IEEE Access, vol. 8, pp. 150527–150538, 2020.

[15] M. Qin and R. Zhu, ‘‘A Monte Carlo localization method based on differential evolution optimization applied into economic forecasting in mobile wireless sensor networks,’’ EURASIP J. Wireless Commun. Netw., vol. 2018, no. 1, pp. 1–9, 2018.

[16] P. Sommer, J. Liu, K. Zhao, B. Kusy, R. Jurdak, A. McKeown, and D. Westcott, ‘‘Information bang for the energy buck: Towards energyand mobility-aware tracking,’’ in Proc. Int. Conf. Embedded Wireless Syst. Netw. Junction, KS, USA: Junction Publishing, 2016, pp. 193–204.

[17] L. Tõnisson, J. Voigtländer, M. Weger, D. Assmann, R. Käthner, B. Heinold, and A. Macke, ‘‘Knowledge transfer with citizen science: LuftLeipzig case study,’’

Sustainability, vol. 13, no. 14, p. 7855, Jan. 2021.

[18] T. Wang, H. Ding, H. Xiong, and L. Zheng, ‘‘A compensated multi-anchors TOF-based localization algorithm for asynchronous wireless sensor networks,’’ IEEE Access, vol. 7, pp. 64162–64176, 2019.

[19] T. Wang, H. Xiong, H. Ding, and L. Zheng, ‘‘TDOA-based joint synchronization and localization algorithm for asynchronous wireless sensor networks,’’ IEEE Trans. Commun., vol. 68, no. 5, pp. 3107–3124, 2020.

[20] Y. I. Wu, H. Wang, and X. Zheng, ‘‘WSN localization using RSS in threedimensional space—A geometric method with closed-form solution,’’ IEEE Sensors J., vol. 16, no. 11, pp. 4397–4404, Mar. 2016.

[21] N. Xie, Y. Chen, Z. Li, and D. O. Wu, ‘‘Lightweight secure localization approach in wireless sensor networks,’’ IEEE Trans. Commun., vol. 69, no. 10, pp. 6879–6893, Jul. 2021.

[22] J. Yin, Q. Wan, S. Yang, and K. C. Ho, ‘‘A simple and accurate TDOA-AOA localization method using two stations,’’ IEEE Signal Process. Lett., vol. 23, no. 1, pp. 144–148, Jan. 2016.

[23] J. Yoon, M. Liu, and B. Noble, ‘‘Random waypoint considered harmful,’’ in Proc. 22nd Annu. Joint Conf. IEEE Comput. Commun. Societies, vol. 2, Mar./Apr. 2003, pp. 1312–1321.

[24] Y. Yuan, L. Huo, Z. Wang, and D. Hogrefe, ‘‘Secure APIT localization scheme against sybil attacks in distributed wireless sensor networks,’’ IEEE Access, vol. 6, pp. 27629–27636, 2018.

[25] Y. Zhang, L. Cui, and S. Chai, ‘‘Energy-efficient localization for mobile sensor networks based on RSS and historical information,’’ in Proc. 27th Chin. Control Decis. Conf. (CCDC), May 2015, pp. 5246–5251.

Author Details:

Dr. A. Avani obtained M. Tech degree from JNTU, Hyderabad, India. She is at present working as professor in Department of CSE of Anu Bose Institute of Technology, Paloncha, Telangana, India. Her area of interest is Data mining.