Research on Collaborative Positioning Algorithm of Wireless Sensor Network Security Under Strong Topology Relation

Yuanyi Dang

School of Automation, Shenyang Institute of Engineering, Shenyang 110136, Liaoning, China
E-mail: MikeDang1981@163.com

Received 09 September 2024; Accepted 19 November 2024

Abstract

In the monitoring area, nodes collaboratively collect various types of critical information about the target object, including temperature, humidity, and stress, and relay this data to users. This study evaluates a scenario with 100 summary points and a communication radius of 20 meters, progressively increasing the number of attack nodes from 0 to 4. Despite the effectiveness of existing security positioning algorithms in mitigating attacks, their substantial network resource consumption remains a challenge. This paper introduces a novel security positioning method designed to tolerate three distinct types of attacks. This approach identifies attack nodes by examining the physical attributes of each node. Analysis indicates that the average positioning error for the witch attack algorithm increases sharply as the number of virtual nodes rises, reaching approximately 80% when four attack nodes are present. Over 1,000 rounds of network observation, node survival rates were documented, starting with an initial pool of 100 nodes. Comparative results reveal that the key-out algorithm begins to experience node failures around the 600th round, with complete node depletion by the 700th round. The MPRP-RSSI algorithm, on the other hand, starts showing

Journal of Cyber Security and Mobility, Vol. 14_1, 25–46.
doi: 10.13052/jcsm2245-1439.1412

failures around the 900th round. By contrast, the proposed algorithm exhibits enhanced robustness, maintaining node stability throughout the entire monitoring period. The enhanced RSSI-based positioning algorithm, which is resilient against replication attacks, applies constraints on communication ranges and enforces unique messaging protocols to regulate node interactions, effectively reducing replication threats.

Keywords: Receive signal strength indication, strong topology, replication attack, wireless sensor, secure positioning.

1 Introduction

In the realm of industrial wireless sensor networks (IWSNs), time synchronization algorithms are primarily categorized into centralized and distributed approaches [1, 2]. Centralized algorithms rely on a central clock source to synchronize the network, while distributed algorithms facilitate synchronization without requiring a central clock, treating all nodes equally [3]. In distributed systems, synchronization is achieved through iterative processes, wherein each node aligns with a virtual clock to ensure relative synchronization across the network. A prominent example of a distributed synchronization protocol is the average consistency time synchronization protocol. In this protocol, each node maintains a virtual clock and periodically broadcasts synchronization messages that contain information about the clock's slope and deviation [4, 5]. Nodes align their virtual clocks by processing synchronization messages received from neighbouring nodes and comparing any detected deviations, progressively achieving a unified clock value across the network. While this method encourages consistency, it can experience slower convergence rates and lower precision compared to centralized synchronization methods. An alternative approach is the maximum consistency time synchronization protocol. Unlike the average consistency protocol, this method adjusts a node's virtual clock by matching it to the clock of a neighboring node with the steepest slope, rather than computing an average value [6]. This strategy allows the network's virtual clocks to quickly synchronize to the value of the node with the maximum slope, potentially enhancing synchronization speed. Cluster-based time synchronization protocols, like the Cluster Consistency Time Synchronization (CCTS) protocol, provide scalable solutions for extensive networks by organizing the network into clusters. Each cluster has a designated leader node, while the remaining nodes act as subordinates.

In contrast to distributed algorithms, centralized algorithms require a source node. During synchronization, subordinate nodes take steps to align their clocks with their superordinate node until the entire network is synchronized, ultimately ensuring synchronization between all ordinary nodes and the source node [7]. The classical centralized synchronization protocols are categorized based on interactions between sender and receiver or solely among receivers [8]. A prominent example is the reference broadcast synchronization protocol, wherein reference nodes broadcast messages. Neighbouring nodes A and B exchange clock information upon receiving these messages, allowing them to determine the time difference and adjust their clocks accordingly to achieve synchronization. In industrial wireless sensor networks, time synchronization algorithms primarily fall into two categories: centralized and distributed approaches [9]. The distributed algorithm does not need the clock source nodes, and all nodes are equal. Each node is synchronized to a virtual clock through distributed iteration to realize the relative synchronization of the whole network. The classical synchronization protocol in the distributed algorithm, such as the average consistency time synchronization protocol, each node maintains a virtual clock, and the node periodically broadcasts the synchronization message, which includes information such as the slope and deviation of the virtual clock [10]. The node adjusts its own virtual clock by receiving the synchronous message of the neighbor node and comparing the deviation of the virtual clock of each neighbor node. Finally, the virtual clock of the entire network node will converge to a logical value. Maximum consistency time synchronization protocol and the average consistency time synchronization protocol, the difference is that the node in updating its virtual clock, not take average operation, but when the neighbor node virtual clock has greater slope, the local node directly update its virtual clock directly to the neighbor node virtual clock [11]. The node possessing the highest clock slope across the network is referred to as the maximum node. With continuous iterations, the virtual clocks of all nodes in the network are adjusted to align with the virtual clock of this maximum node. Additionally, there exists a cluster-based consistency time synchronization protocol. Its fundamental concept involves dividing the network into multiple clusters, within which each cluster designates a cluster node to serve as the leader, while the remaining nodes function as subordinate nodes [12]. The CCTS synchronization protocol consists of two main components: inter-cluster synchronization, which handles synchronization between nodes in different clusters, and intra-cluster synchronization, which manages synchronization between cluster nodes and their subordinate nodes. The

synchronization process relies on the average consistency synchronization method, making it particularly suited for large-scale wireless sensor networks and accelerating the convergence rate of synchronization. While distributed protocols within existing networks offer scalability and robustness, they often exhibit slower convergence rates and reduced synchronization accuracy compared to centralized networks, and their algorithms tend to be relatively complex [13].

2 Overview of Secure Time Synchronization Algorithms for Industrial Wireless Sensor Networks (IWSNs)

2.1 Examination of Detection Techniques Within Localization Frameworks

Considering two centralized networks with single-hop and multi-hop, the whole network has a source node as the time source. At the same time, assume that each node only knows whether it is a malicious node. As shown in Equation (1), τ is the source node, β is the slave node, α is the attack node, t is the attack time, the single-hop network consists of 1 source node, 1 slave node, 1 reference forwarding node and one attack node, and the multi-hop network consists of 1 source node and 10 normal nodes.

$$\tau_i = \alpha_i t + \beta_i \tag{1}$$

In an industrial wireless sensor network, the clock of the node depends on the crystal oscillator timing process, as shown in Equation (2), i, j are the specific locations at the time of attack, where the crystal vibration provides the timing signal of the clock source. The local time obtained by timing the crystal vibration is called the hardware clock. In this paper defines the hardware clock as and uses the first-order linear model to describe it. The difference of the crystal oscillator process leads to the slope and offset of the node hardware clock.

$$\tau_i = \frac{\alpha_i}{\alpha_j}\tau_j + \left(\beta_i - \frac{\alpha_i}{\alpha_j}\beta_j\right) = \alpha_{ji}\tau_j + \beta_{ji} \tag{2}$$

Furthermore, changes in temperature, EMI and other external environments also affect the hardware clock slope and offset, therefore, each sensor node has a different hardware clock. As shown in Equation (3), k is the source clock reference, assume that the hardware clock slope in IWSNs satisfies the

following conditions, however, the absolute time is agnostic for the nodes.

$$\tau_j(k+1) = \alpha_j t(k+1) + \beta_j \tag{3}$$

Therefore, the hardware clock slope and offset, as the hardware features of the nodes, cannot be directly adjusted. By comparing the master node i, as shown in Equation (4), sm, r, m are the attack identification numbers, the linear relationship between the local clock and the master node.

$$\tau_{sm} = (\tau_m - \tau_r) - (\tau_s - \tau_r) \tag{4}$$

The security of the network should be considered when designing the IWSNs application protocol. There are various types of attacks, as shown in Equation (5), for example, the attack node drops, modior even falsified the exchange timing message to interrupt the time synchronization process.

$$\tau_{sm} = (\alpha_m - \alpha_s)t + (\beta_m - \beta_s) \tag{5}$$

As shown in Equation (6), sending the wrong synchronization message to mislead its neighbors and breaking the synchronization.

$$t = \frac{\tau_s - \beta_s}{\alpha_s} \tag{6}$$

2.2 Security Evaluation of Localization Algorithms

Rereplay attack, assuming that FTSP during synchronization, attacker a can replay the old timing data packet of node j, misleading node i to synchronize to the wrong time. For example, FTSP in normal conditions yields the node hardware time when node i receives a time stamp from the neighbor node j. However, under the replay attack, as shown in Equation (7), the attack node transmits the hardware time information of the previous moment to node i, causing the node to synchronize to the wrong clock, and the synchronization of the whole network fails.

$$\tau_{sm} = \frac{(\alpha_m - \alpha_s)(\tau_s - \beta_s)}{\alpha_s} + (\beta_m - \beta_s) \tag{7}$$

The existing security time synchronization method involves few intelligent attacks in the centralized topology, so the research direction of this paper is mainly the security time synchronization protocol that can resist witch attacks in the centralized network topology environment. As shown

in Equation (8), n is the total number of attacks, under the witch attack, malicious nodes will disguise themselves as multiple identities in the network, including normal nodes including the source nodes, and send false messages to unsynchronized nodes, resulting in synchronization failure.

$$\alpha_{sm} = 1 + \frac{\sum_{i=1}^{n} (\tau_s^i - \overline{\tau_s})(\tau_{sm}^i - \overline{\tau_{sm}})}{\sum_{i=1}^{n} (\tau_s^i - \overline{\tau_s})^2} \tag{8}$$

As shown in Equation (9), under the FTSP protocol, when a node i receives the hardware clock information and the attack node at the node, the node fails to distinguish which message is correct, and the wrong message may be used to adjust the clock, resulting in the failure of the entire network synchronization. At present, although the information filtering technology can resist witch attacks, it is only suitable for distributed network, not for centralized industrial wireless sensor network. Although the message manipulation attack problem is solved by threshold detection technology, this mechanism will fail when the attack node is disguised as a normal node under a witch attack.

$$\beta_{sm} = \overline{\tau_{sm}} - (\alpha_{sm} - 1)\overline{\tau_s} \tag{9}$$

The core idea of this algorithm is first described as a small-scale network model. The network contains the public reference forwarding nodes, source nodes, and slave nodes participating in time synchronization. First, the reference forwarding node r sends its local clock information to the source node m and the slave node s. As indicated in Equation (10), ds is the acceptance time, the source node and the source node respectively record the message and calculate the time difference between sending and receiving the message.

$$ds = \alpha_{sm}\alpha_s - \alpha_m \tag{10}$$

When the reference forwarding node sends its local clock message, the message contains a randomly generated serial number. Since the sending period of the message is fixed, the problem of the message serial number can be solved by designing a timer. Therefore, in the single-hop network, as shown in Equation (11), $E()$ is the single-hop network function, E is the single-hop compensation, d is the number of single hops, and ξ is the serial number value, both the source node and the slave node receive the hardware clock information from the reference forwarding node. When the message of the source node is forwarded to the slave node, the slave node will check the message serial number.

$$E_{Tx}(k, d) = kE_{elx} + k\xi_{fs}d^2 \tag{11}$$

If the two serial numbers do not match, the slave node does not use this message for the synchronization compensation value calculation. A known attacker can only disguise as a sending node, not a receiving node. In this network synchronization model, the nodes that an attacker can disguise are the reference forwarding nodes and the source nodes. As shown in Equation (12), moreover, due to the information encryption mechanism, the attacker cannot directly change the information received. The following three cases of the attack nodes disguised as reference forwarding nodes.

$$E_{Rx}(k, d) = kE_{ekc} \tag{12}$$

3 Positioning Systems in Wireless Sensor Networks

3.1 Structural Composition of Wireless Sensor Networks

Wireless Sensor Networks (WSN) in addition to have the characteristics of other network and the following several uniqueness, large-scale network [14]. In order to collect more accurate in the monitoring area of the data, the accuracy of data acquisition, then use distributed way to process data, so not only can reduce the output of the information also can reduce the data error of a single node produced [15]. Because the wireless network generates more interference nodes, WSN has strong error processing power. Large-scale network coverage can reduce the monitoring of blind spots. AD hoc network and the maintenance for random spread a large number of sensor node network, Figure 1 for intelligent network system, where each node is equal, there is no absolute control center, due to the relationship between the communication nodes and the corresponding location is uncertain, which requires wireless sensor network automatically management and configuration, nodes in the WSN through mutual cooperation and automatic network [16]. However, the change of the environment will make several or more nodes invalid, and the network will also change at any time, which requires the wireless network to have self-maintenance function, so as to ensure that the normal operation of WSN will not be affected by the failure of some nodes.

A reliability network, such as a wireless sensor network (WSN), is specifically designed to operate in challenging environments. Consequently, the hardware of the nodes must be durable and resilient to damage. Given the large coverage area of the network, sensor nodes may occasionally change their positions, which necessitates secure transmission of the monitored data. Both the hardware and software components of the WSN must be highly reliable and capable of adapting to various environmental conditions [17]. The

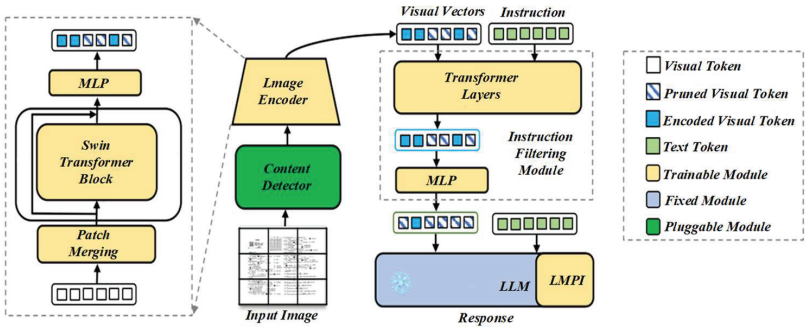

Figure 1 Intelligent network system diagram.

relationship between communication nodes and their corresponding locations is often uncertain, which calls for automatic management and configuration within the wireless sensor network. Nodes in the WSN collaborate with one another and automatically form the network. However, environmental changes can cause some nodes to become inoperative, leading to dynamic changes in the network. As a result, it is essential for the wireless network to possess self-maintenance capabilities to ensure that the overall operation of the WSN remains unaffected by the failure of individual nodes [18]. WSN is a network designed for special environments, usually working in relatively harsh environments, so the hardware equipment of the node is required to be very strong and not easy to damage [19, 20]. Due to the large area to be detected, the position of the sensor node sometimes changes, and the network cannot be maintained manually in time. In order to ensure the safe transmission of the monitored data and information, the software and hardware of the whole WSN are required to have high reliability and can adapt to various environmental conditions. Different communication modules can be used according to the different distance [21, 22]. Data fusion technology can also be used to reduce network traffic. As a research hotspot in the field of information today, WSN is not a single discipline but involves the integration of multiple disciplines. Through continuous innovation, now many network technologies have been applied to real life, but there are still some key technologies need to be further improved, the following focus on several key technologies [23, 24].

3.2 RSSI-Based Localization Algorithm

Wireless sensor networks are all self-organized networks. Network topology technology eliminates the redundant transmission paths in the case of

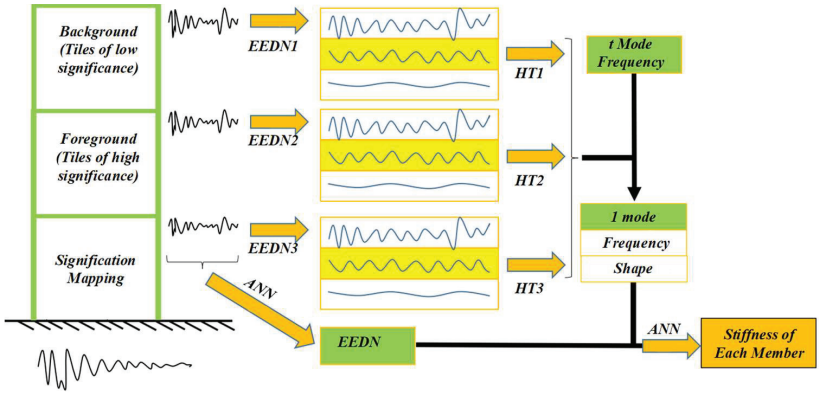

Figure 2 Self-organization diagram of the RSSI positioning algorithm.

ensuring the network connectivity and node coverage rate to form the optimal network structure [25]. As a self-organized network, WSN also needs to process the data in addition to transmitting data. How to ensure the authenticity of data, the reliability of information and the security of communication are the main problems of WSN research in network security. In order to ensure the safe transmission of data and information, WSN technology needs to provide security mechanisms, such as point-to-point authentication, integrity authentication and authentication broadcasting, so as to eliminate malicious attacks in time [26]. Positioning is the basis of WSN to complete other tasks and is an essential part of data collection. In practice, if location information is not available, node positioning is the basic capability of WSN. Figure 2 shows the self-organization diagram of RSSI positioning algorithm. Due to the limitations of cost, power consumption and node volume, only some node locations are known, while other nodes can only determine their location in the network through the positioning algorithm [27]. In WSN, due to the limited energy of the sensor node, data fusion is required to reduce the amount of data transmission, thus reducing the energy loss [28]. Due to the large amount of redundant information in the communication network, multiple transmission of the same information will cause unnecessary energy loss, thus shortening the life cycle of the network [29].

Each sensor node has an embedded system. Due to the small size of the nodes and the limited hardware conditions, the micro and small operating systems are usually embedded for the efficient use of resources [30]. The presence of embedded operating systems allows multiple applications to efficiently share and utilize limited system resources concurrently, making

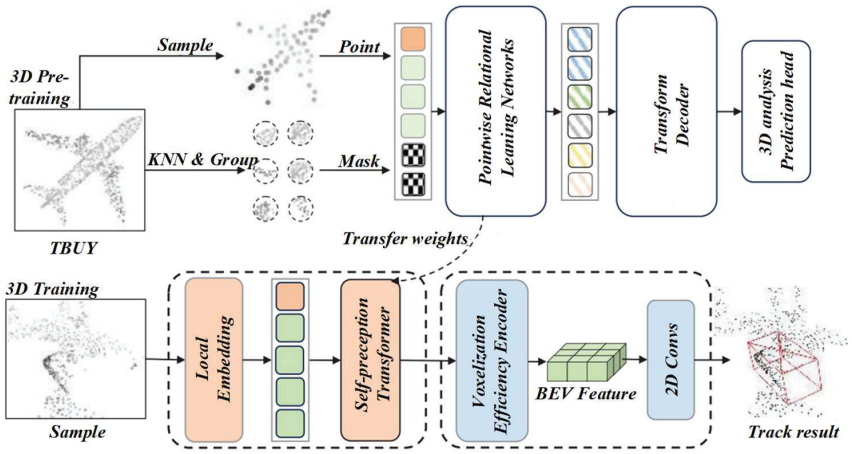

Figure 3 Embedded system evaluation diagram.

research on these systems a focal point in the field of wireless sensor networks (WSN). WSNs are inherently self-organized networks, with network topology technology playing a crucial role in maintaining connectivity and node coverage to achieve the optimal network structure. This has a direct impact on the overall effectiveness and performance of the WSN. As a self-organized network, WSNs must not only transmit data but also process it. Ensuring data authenticity, information reliability, and secure communication are key challenges in the realm of WSN security research. Figure 3 illustrates the evaluation of the embedded system. Effective broadcast authentication mechanisms are essential for timely detection and elimination of malicious attacks. Positioning serves as a foundational component for WSN operations, playing a critical role in data collection. In practical scenarios, accurate location information is vital; therefore, node positioning remains a fundamental capability of WSNs. Given constraints such as cost, power consumption, and node size, the locations of only some nodes are predetermined. Other nodes must rely on positioning algorithms to establish their locations within the network.

In WSN, due to the limited energy of the sensor node, data fusion is required to reduce the amount of data transmission, thus reducing the energy loss. Due to the large amount of redundant information in the communication network, multiple transmission of the same information will cause unnecessary energy loss, thus shortening the life cycle of the network. Each sensor node is equipped with an embedded system. Given the small size and limited

hardware capabilities of these nodes, micro and lightweight operating systems are typically embedded to optimize resource usage. The incorporation of embedded operating systems enables multiple applications to efficiently share and utilize limited system resources, making this a key focus of research within the field of wireless sensor networks (WSNs). Distance measurement in WSNs is commonly achieved through two primary methods. The first involves measuring the time difference of data signals. Here, a signal-sending node transmits a message and records the transmission time, while the receiving node immediately sends a feedback message upon receipt. The sending node calculates the time difference between the initial signal and the feedback to determine distance, a method requiring extremely high processing speed. The second approach measures the one-way propagation time of a data signal, using the time consumed during data transmission. This method demands precise time synchronization between nodes to ensure accuracy.

4 RSSI Localization Algorithm in Strong Topological Contexts

4.1 Strong Topology Replication Attack Models and Current Detection Techniques

The RSSI values have a certain symmetry. When determining the RSSI values between two nodes, Figure 4 is a strong topological replication attack model graph, which can be measured without the need to transmit messages back and forth. When the requirement for positioning accuracy is low, a simpler positioning algorithm with reduced complexity can be utilized. In earlier developments, the RSSI (Received Signal Strength Indicator) ranging technique included systems like the SpotONtags indoor positioning system, created by Hightower and colleagues. This system measured the linear distance between nodes using RSSI values within a 3 m $\times$ 3 m $\times$ 3 m space, achieving a positioning accuracy of approximately 1 meter. Distance measurement using the RSSI-based positioning algorithm generally falls into two categories. The first involves pre-assessing environmental factors. This approach requires building an RSSI database within the test area prior to algorithm implementation by repeatedly sending and receiving RSSI signals and conducting extensive experiments to store approximate values at different locations, which are then used to create fitting curves for actual testing. The second method entails performing direct experiments within the monitoring area, where signals are transmitted and received among arranged nodes to enable real-time positioning and distance calculation.

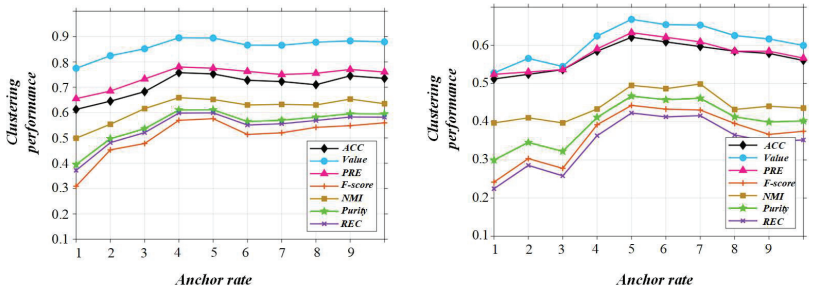

Figure 4 Strong topology replication attack model diagram.

Table 1 RSSI signal simulation parameters value setting

Parameter Name	Parameter Values
Number of nodes	100
Node communication radius, R	50 m
The RSSI path-loss index, n	3
Monitoring area	100 m * 100 m
Node initial energy	0.5 J
Data packet	3000 bit
Master bundles	100 bit
Number of samples	100

According to a large number of previous experiments, the degree of decay and distance of RSSI signal is not a simple linear relationship can represent, environmental factors have a great impact on the attenuation of RSSI signal, and the intensity of the obstacle, the height of nodes, the direction of the antenna, Table 1 for the RSSI signal simulation parameter setting, in the distance between the node and the ground is greater than 2 meters, the direction of the antenna is not excessive influence on the accuracy of RSSI positioning.

RSSI positioning technology is divided into three steps: first, ranging process; second, positioning calculation process; and third, coordinate correction. The ranging stage of RSSI location algorithm: the unknown node sends the location request, and the beacon node receives its own position coordinate and RSSI signal strength. The unknown node receives the signal and measures the received RSSI signal intensity. Energy loss was calculated and converted to distance according to the energy loss model. The positioning phase of the RSSI (Received Signal Strength Indicator) algorithm involves measuring and selecting data from nearby beacon nodes. This data is processed through geometric models or systems of equations,

using algorithms such as triangulation, trilateration, and maximum likelihood estimation to determine location. During the correction phase, variations in distance between beacon nodes and the target node can cause differing levels of influence on localization accuracy. Each beacon node's proximity to the target node impacts signal transmission processing. Beacon nodes closer to the estimated coordinates exert greater influence on those coordinates, and thus a weighting factor is assigned to reflect this influence. Since wireless communication experiences varying degrees of signal attenuation, selecting an appropriate signal transmission loss model and a suitable positioning algorithm for sensor nodes is critical for accurate localization.

The RSSI values collected by test nodes often exhibit significant instability, with potential limitations stemming from a singular positioning method. Factors such as irrational weighting settings and special node conditions can skew positioning results and lead to errors. A detailed examination reveals that RSSI values are highly sensitive to environmental changes. During RSSI-based ranging, fluctuations in temperature, obstacles, and propagation modes can impact values inconsistently. These conditions rarely remain ideal, contributing to instability. Additionally, RSSI values do not consistently reflect signal energy loss during transmission; when highly biased values are used, localization accuracy suffers greatly. Furthermore, inappropriate weight factor allocation can negatively impact positioning accuracy. For some algorithms, the influence of beacon nodes on positioning weights diminishes with distance, potentially introducing correction errors. Isolated nodes also pose challenges: in sparse network regions or in cases where nodes are affected by environmental factors, other nodes may fail to meet localization criteria, leading to the creation of isolated nodes unable to participate in positioning. Limited resources, through the study of the wireless sensor network, has the characteristics of low cost, many functions, easy to use. However, it also needs portable micro-batterie to node has a certain life cycle. When the battery runs out, the node will lose the ability to collect and transmit information, so the local network structure will change accordingly. If the node is a beacon node, it may appear that the surrounding nodes cannot locate or cause a greater error.

4.2 Improvements to RSSI Localization Algorithms Under Strong Topological Replication Attacks

DD routing algorithm based on witch attack: taking data as the center, classifying tasks by type, detecting areas into blocks, and proposing the path

Table 2 Value setting of strong topology simulation parameters

Parameter Name	Parameter Values
Number of nodes	182
Node communication radius, R	59 m
The RSSI path-loss index, n	42
Monitoring area	400 m * 800 m
Node initial energy	1.7 J
data packet	2400 bit
master bundles	560 bit
number of samples	700

strengthening mechanism, so that the data transmission rate is significantly improved. Node trust and witch attack node parameters are used as constraints, including two stages: the first stage is the initialization of node trust and the update process of node trust. The second stage involves establishing and reinforcing routing mechanisms. The tolerance intrusion technique for countering witch attacks focuses on utilizing redundant data within the node positioning system to detect malicious nodes using variance-unbiased estimation. Initially, a minimum-security reference set is identified, and abnormal data is then detected using predicted residuals, thereby enhancing the system's resilience against intentional adversarial attacks. The MPRP-RSSI algorithm is designed to combat Sybil attacks and enhance positioning accuracy through RSSI-based localization. It works by first encoding RSSI signals using Manchester encoding and then applying pseudorandom processing to generate sequential pseudostochastic codes through a sequence generation algorithm, outputting an encoded signal. During the decoding process, the received signal undergoes initial filtering, followed by channel monitoring and cycle measurement of letter codes. The receiver then reconstructs the code based on pseudorandom parameters, retrieves the codeword, and performs Manchester decoding to extract the message content and verify its accuracy. Table 2 outlines the strong topology simulation parameter values used in this context. The attenuation model assumes that only nodes within the communication range can receive location information from other nodes. This ensures communication is limited to those within effective range, supporting efficient and secure data exchange.

When the RSSI positioning process of wireless sensor network is attacked by the witch, the nodes in the network can use the same physical position RSSI ratio of the same characteristics. In an RSSI-based ranging process, a witch attack node can create multiple forged virtual nodes and engage

in network communication to deceive unknown nodes. Consider a scenario where a witch attack node, S, exists within the communication range of an unknown node, D. During the ranging process, S fabricates location data for four beacon nodes, labeling them as S1, S2, S3, and S4. If D receives these distinct pieces of location data from S and measures identical distances to S1, S2, S3, and S4, it will perceive a distribution of multiple beacon nodes at equivalent distances around itself. If there are no other genuine beacon nodes closer to D than S, the fraudulent location information from S will be factored into the positioning calculation, significantly increasing positioning errors. In the positioning process, accurate correspondence between node identity and actual position forms the basis of the system. However, replication attack nodes provide false location data that does not match their real positions. By masquerading as legitimate beacon nodes, these forged nodes introduce incorrect location data into the positioning calculations, misleading the unknown node. Another potential scenario occurs when a node receives identical location information from multiple nodes simultaneously, resulting in multiple distances to the same coordinates. This causes a failure in the matrix solution during positioning calculations, thereby reducing the overall positioning success rate. Such behavior exemplifies replication attacks within wireless sensor network RSSI positioning processes. Figure 5 illustrates the matrix evaluation for this type of positioning interference.

For the above two cases, two features are proposed to fight the replication attack, identify all attack nodes, and eliminate from the network: the limited communication range limited feature and the unique feature of receiving messages. Finally, the normal RSSI localization calculations were performed. Two judgment processes are added in the ranging phase of RSSI positioning:

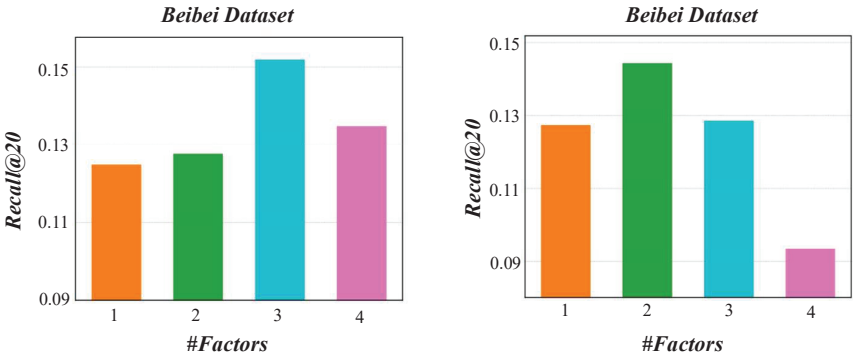

Figure 5 Matrix positioning evaluation map.

both the limited communication range feature and the unique feature of the received message. Normal RSSI location calculation after removing the attack node.

5 Experimental Analysis

The simulation experiment on the RSSI localization algorithm under replication attack uses Matlab2014a. The workshop is an area of 100 m * 100 m, which is divided into 20 m * 20 m grids according to the distribution of the equipment. Figure 6 is the sensor beacon node diagram.

When the number of summary points is 100, Figure 7 shows the evaluation diagram of communication radius. When the communication radius is 20 m, the average error comparison between the number of attack nodes is different. If the number of summary points is 100 and the communication radius is 20 m, the number of attack points increases from 0 to 4.

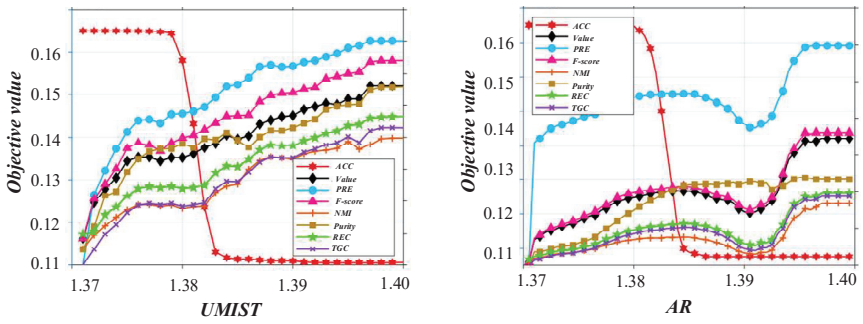

Figure 6 Nodiagram of sensor beacon.

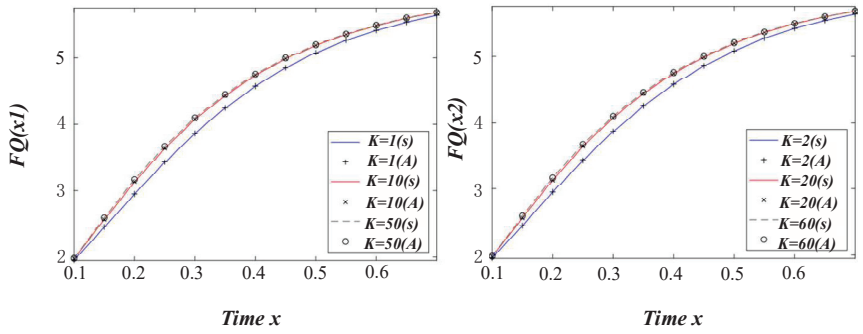

Figure 7 Evaluation diagram of the communication radius.

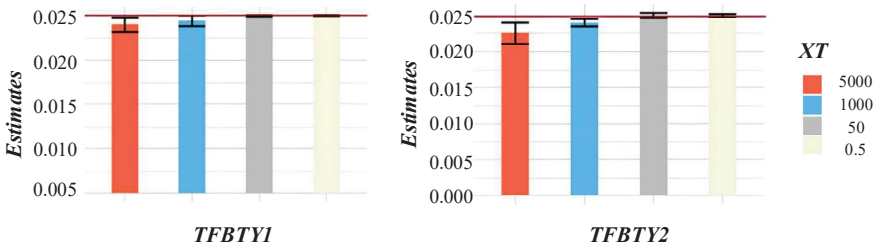

Figure 8 Average positioning error diagram of the attack algorithm.

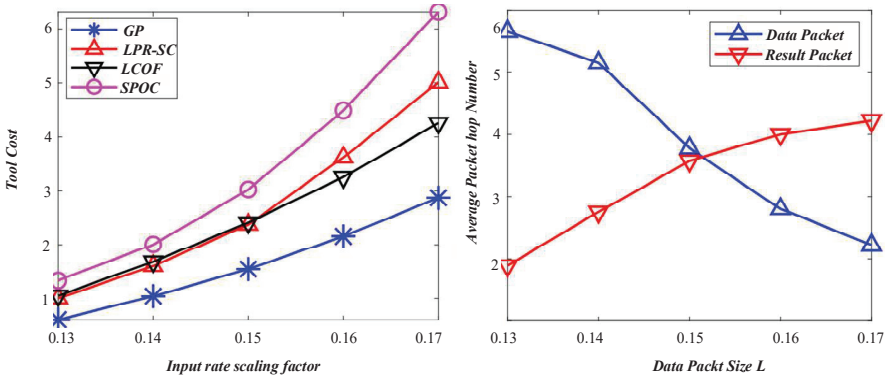

Figure 9 Energy diagram of the CRCDS algorithm

When the number of attack nodes rises to four, the positioning error escalates to approximately 90%, resulting in a near-complete failure of accurate positioning. Figure 8 illustrates the average positioning error of the attack algorithm, emphasizing this significant decline in performance. However, the average positioning error of the algorithm proposed in this chapter remains largely unaffected by the increase in attack nodes. It maintains a level of accuracy comparable to that seen in scenarios without any attacks. This indicates that the detection algorithm presented in this chapter can effectively withstand replication attacks, significantly reducing their impact on positioning accuracy and thereby achieving secure positioning.

Three algorithm survival node comparison, you can see the CRCDS algorithm in about 700 nodes, to 800 round nodes has all dead, Figure 9 for CRCDS algorithm energy diagram, key algorithm is less than 600 nodes began to die, to about 700 rounds have no residual energy, node has all dead, node death rate is very high.

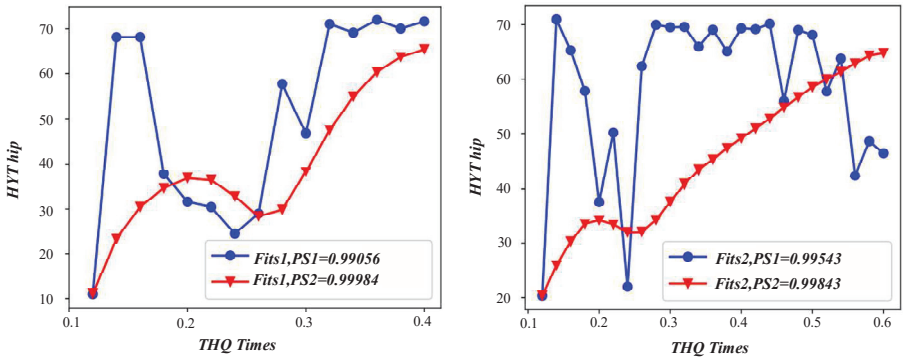

Figure 10 Comparison diagram of the key algorithm and the CRCDS algorithm.

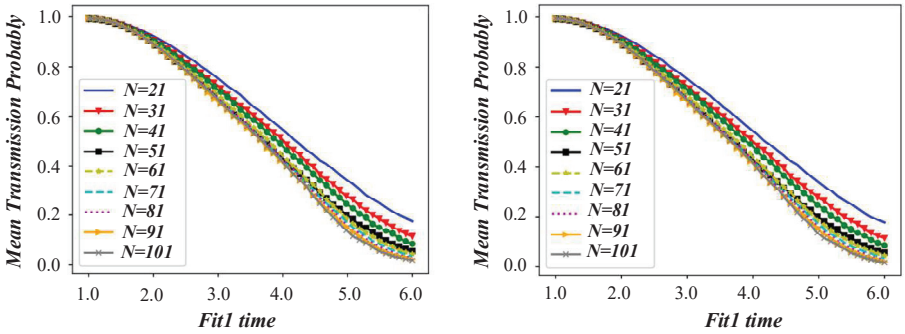

Figure 11 Average residual energy original image.

The nodes of this algorithm have not yet begun to die. Therefore, the algorithm in this chapter can effectively resist replication attacks at the positioning level, and can save energy and significantly extend the life cycle of the network. Figure 10 shows the comparison diagram between key algorithm and CRCDS algorithm, which proves that this chapter has a longer life cycle compared with key algorithm and CRCDS algorithm, and also has advantages in energy consumption.

The effectiveness of the proposed method against message manipulation attacks during network topology construction is illustrated in Figure 11, which depicts the average residual energy in its initial state, with five nodes designated as attack nodes. The relative clock slope and offset error for nodes 1 through 10 show fluctuations within a certain range, while both the mean absolute value and standard deviation of the relative clock offset remain stable, demonstrating consistent performance across these nodes.

6 Conclusion

This research explores advancements in Wireless Sensor Network (WSN) positioning and security technologies, examining various security algorithms designed to address different types of attacks. A comprehensive evaluation of RSSI localization technology reveals several weaknesses, leading to the development of a new secure localization algorithm designed to counter witch attacks, wormhole attacks, and replication attacks through enhanced encryption techniques and targeted filtering of malicious nodes.

(1) The proposed algorithm incorporates features such as communication range constraints and unique message characteristics to combat replication attacks. These measures significantly diminish the success rate of such attacks, ensuring improved localization reliability.
(2) To address wormhole attacks, the algorithm applies restrictions on communication range, message content, and message uniqueness. This layered approach strengthens the detection and mitigation of wormhole attacks, preserving the integrity and accuracy of the positioning system.
(3) Validation of the secure positioning algorithm through Matlab simulations demonstrated substantial enhancements in energy efficiency and resistance to attacks compared to conventional approaches. Over 1000 rounds of network monitoring, the algorithm outperformed existing methods, showing an average residual energy that was 145% greater than the MPRP-RSSI algorithm and 210% higher than the key algorithm at around 400 rounds. While the key algorithm's nodes exhausted their energy by 700 rounds, the proposed algorithm retained over 80% of its energy. Additionally, it achieved 33% lower energy consumption compared to MPRP-RSSI and 20% lower than the key algorithm, illustrating its effectiveness in extending network lifespan and conserving energy.

Funding

This study is supported by Project The 2023 Liaoning Provincial Science and Technology Plan Joint Fund Project(2023-MSLH-236).

References

[1] K. B. Abu Bakar, F. T. Zuhra, B. Isyaku, and S. B. Sulaiman, "A Review on the Immediate Advancement of the Internet of Things in Wireless Telecommunications," Ieee Access, vol. 11, pp. 21020–21048, 2023.

[2] D. Adesina, C. C. Hsieh, Y. E. Sagduyu, and L. J. Qian, "Adversarial Machine Learning in Wireless Communications Using RF Data: A Review," Ieee Communications Surveys and Tutorials, vol. 25, no. 1, pp. 77–100, 2023.

[3] I. Ahmad et al., "Analysis of Security Attacks and Taxonomy in Underwater Wireless Sensor Networks," Wireless Communications & Mobile Computing, vol. 2021, pp. 15, 2021.

[4] J. Amutha, S. Sharma, and S. K. Sharma, "Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions," Computer Science Review, vol. 40, pp. 43, 2021.

[5] A. Attkan and V. Ranga, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security," Complex & Intelligent Systems, vol. 8, no. 4, pp. 3559–3591, 2022.

[6] B. A. Begum and S. V. Nandury, "A Survey of Data Aggregation Protocols for Energy Conservation in WSN and IoT," Wireless Communications & Mobile Computing, vol. 2022, pp. 28, 2022.

[7] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions," Internet of Things, vol. 24, pp. 37, 2023.

[8] C. M. Chen, Z. Li, S. A. Chaudhry, and L. Li, "Attacks and Solutions for a Two-Factor Authentication Protocol for Wireless Body Area Networks," Security and Communication Networks, vol. 2021, pp. 12, 2021.

[9] G. Czeczot, I. Rojek, and D. Mikolajewski, "Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors," Electronics, vol. 12, no. 11, pp. 14, 2023.

[10] W. D. Fang, W. X. Zhang, W. Chen, T. Pan, Y. P. Ni, and Y. X. Yang, "Trust-Based Attack and Defense in Wireless Sensor Networks: A Survey," Wireless Communications & Mobile Computing, vol. 2020, pp. 20, 2020.

[11] Y. Y. Ghadi et al., "Machine Learning Solutions for the Security of Wireless Sensor Networks: A Review," Ieee Access, vol. 12, pp. 12699–12719, 2024.

[12] M. Hanif et al., "AI-Based Wormhole Attack Detection Techniques in Wireless Sensor Networks," Electronics, vol. 11, no. 15, pp. 28, 2022.

[13] M. Z. Hasan and Z. M. Hanapi, "Efficient and Secured Mechanisms for Data Link in IoT WSNs: A Literature Review," Electronics, vol. 12, no. 2, pp. 23, 2023.

[14] M. Z. Hasan, Z. M. Hanapi, and M. Z. Hussain, "Wireless Sensor Security Issues on Data Link Layer: A Survey," Cmc-Computers Materials & Continua, vol. 75, no. 2, pp. 4065–4084, 2023.

[15] N. H. Hussein, C. T. Yaw, S. P. Koh, S. K. Tiong, and K. H. Chong, "A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions," Ieee Access, vol. 10, pp. 86127–86180, 2022.

[16] H. Liazid and M. Lehsaini, "A brief review on integration between wireless sensor networks and Cloud," Concurrency and Computation-Practice & Experience, vol. 33, no. 20, pp. 10, 2021.

[17] J. X. Liu, M. Nogueira, J. Fernandes, and B. Kantarci, "Adversarial Machine Learning: A Multilayer Review of the State-of-the-Art and Challenges for Wireless and Mobile Systems," Ieee Communications Surveys and Tutorials, vol. 24, no. 1, pp. 123–159, 2022.

[18] X. W. Liu, J. G. Yu, F. Li, W. F. Lv, Y. L. Wang, and X. Z. Cheng, "Data Aggregation in Wireless Sensor Networks: From the Perspective of Security," Ieee Internet of Things Journal, vol. 7, no. 7, pp. 6495–6513, 2020.

[19] R. Lohiya and A. Thakkar, "Application Domains, Evaluation Data Sets, and Research Challenges of IoT: A Systematic Review," Ieee Internet of Things Journal, vol. 8, no. 11, pp. 8774–8798, 2021.

[20] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," Journal of Systems Architecture, vol. 113, pp. 45, 2021.

[21] A. Narwaria and A. P. Mazumdar, "Software-Defined Wireless Sensor Network: A Comprehensive Survey," Journal of Network and Computer Applications, vol. 215, pp. 26, 2023.

[22] S. Nobahary, H. G. Garakani, and A. Khademzadeh, "Detecting Non-cooperation Nodes Mechanisms in Wireless Networks: A Survey," Security and Communication Networks, vol. 2022, pp. 20, 2022.

[23] P. Park, P. Di Marco, J. Nah, and C. Fischione, "Wireless Avionics Intracommunications: A Survey of Benefits, Challenges, and Solutions," Ieee Internet of Things Journal, vol. 8, no. 10, pp. 7745–7767, 2021.

[24] D. M. G. Preethichandra, L. Piyathilaka, U. Izhar, R. Samarasinghe, and L. C. De Silva, "Wireless Body Area Networks and Their Applications-A Review," Ieee Access, vol. 11, pp. 9202–9220, 2023.

[25] M. Pundir and J. K. Sandhu, "A Systematic Review of Quality of Service in Wireless Sensor Networks using Machine Learning: Recent Trend and Future Vision," Journal of Network and Computer Applications, vol. 188, pp. 33, 2021.
[26] R. Ramya and T. Brindha, "A Comprehensive Review on Optimal Cluster Head Selection in WSN-IoT," Advances in Engineering Software, vol. 171, pp. 16, 2022.
[27] M. Revanesh, J. M. Acken, and V. Sridhar, "DAG block: Trust aware load balanced routing and lightweight authentication encryption in WSN," Future Generation Computer Systems-the International Journal of Escience, vol. 140, pp. 402–421, 2023.
[28] M. E. Rivero-Angeles, "Quantum-based wireless sensor networks: A review and open questions," International Journal of Distributed Sensor Networks, vol. 17, no. 10, pp. 13, 2021.
[29] M. Saqib and A. H. Moon, "A Systematic Security Assessment and Review of Internet of Things in the Context of Authentication," Computers & Security, vol. 125, pp. 27, 2023.
[30] A. Thakkar and R. Lohiya, "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges," Archives of Computational Methods in Engineering, vol. 28, no. 4, pp. 3211–3243, 2021.

Biography

Yuanyi Dang, born in Tieling City of Liaoning Province in 1981, Graduated from Communication and Information Systems major of Northeastern University in 2007, currently a lecturer at School of Automation, Shenyang Institute of Engineering, His research interests include wireless sensor networks and embedded systems.