Sensors and Materials, Vol. 32, No. 1 (2020) 115–134
MYU Tokyo

S & M 2090

IoT Network Security and Applications via Long Range Technology

Wen-Tsai Sung[1] and Sung-Jung Hsiao[2*]

[1]Department of Electrical Engineering, National Chin-Yi University of Technology,
No. 57, Sec. 2, Zhongshan Rd., Taiping Dist., Taichung 41170, Taiwan
[2]Department of Computer Science and Information Engineering, Hungkuo Delin University of Technology,
No. 1, Ln. 380, Qingyun Rd., Tucheng Dist, New Taipei City 236, Taiwan

(Received August 29, 2019; accepted October 13, 2019)

Keywords: multisensor fusion calculation, LoRa, localization system, IoT, network security

In this research project, we aim to build a long-range (LoRa)-based Internet of Things (IoT) secure localization system and application based on multisensor fusion calculation. The LoRa technology is used to design a network security system and immediately address the computing system, where the purpose is to develop a network server host that collects and processes position signals from the multisensing signal collection and analysis processing module, and instantly detects location by network nodes through the sensors cloud, the Arduino UNO high-level development platform, and the multisensor fusion computing workstations, which send the results to the central monitoring system through the wireless devices of the LoRa network. The secure localization computing chip outcome, as developed in this project, can be used in the domains of energy management, environmental management, information management, factory monitoring, and renewable energy management. The system of this project comprises LoRa hosts, which receive signals from various nodes and are connected to a multisensor fusion arithmetic system through a wireless network. To sum up, in this study, we emphasize using multisensor fusion computing technology to implement a secure localization system of a wireless sensor network (WSN), and we consider using the embedded system and LoRa technology to develop a monitoring system for factory fire control, anti-theft, energy, information, and security based on secure localization. In this study, we cross domains and integrate related engineering automation, network security technology, multisensor fusion calculation design, and the LoRa localization technique, and the research findings are expected to contribute to the network security of the defense industry and research on the LoRa IoT localization system.

1. Introduction

The Internet of Things (IoT) is a new domain of information technology development, which is characterized by rapid deployment, cooperative perception, and high fault tolerance. Thus, it has extensive application prospects in the domains of military affairs, environmental

*Corresponding author: e-mail: topdike@gmail.com
https://doi.org/10.18494/SAM.2020.2569

ISSN 0914-4935

surveillance, forecasting, and city management. In most IoTs, the location information of nodes has a key effect on application effectiveness. As the IoT is tightly coupled with the real physical world, the IoT must create the spatial relations of the network depending on the location information of nodes, which report events and track external objects accordingly.[1–3] In addition, the location information of nodes is an important basis of network functions, such as providing network topology self-configuration, instantly calculating the quality of network coverage and assisting routes, and is one of the bottommost functions and services of self-localization in the IoT. In the IoT, determining the location of a node or event is very important for monitoring activities, as the accurate location of a node not only provides the precondition of monitoring an event and target location information, it also provides network topology self-configuration, increases routing efficiency, reports the network coverage quality to the deployer, and provides the basis of network functions, such as the namespace for a network.[4,5]

This project is based on long-range (LoRa) wireless transmission technology, which is a low-power wide-area network (LPWAN), and this technology represents the new trend of the continuous evolution of wireless communication technology.[6–9] While the traditional broadband communication has a higher transmission rate, the LPWAN dismisses the high transmission rate and pays more attention to energy efficiency, scalability, and coverage.[10,11] A lot of sensor terminal nodes can coexist in the LPWAN architecture, as the information of each sensor node can be sent to multiple gateways, and the data are transmitted through these gateways to the internet server side with strong arithmetic capability, as well as to the application server side after the filtration of the redundant information of the entire network and the validation of security, where the user can evaluate and control various classes of data, as shown in Fig. 1(a). How to provide a secure node location system for IoT applications with the possibility of hostile attack is a key problem that must be solved. In this study, we aim to analyze and compare the attack types when using LoRa technology to develop different location techniques, and probe into the implementation principles, characteristics, limitations, and relations of the proposed security measures, in order to advance the research directions of related domains.

2. LoRa IoT Localization System Security Analysis

2.1 LoRa IoT node location system

The location refers to how one node obtains its geographic location information. As they are limited by the price, volume, power consumption, and scalability factors, most sensor network node location systems use a beacon-node-assisted node location plan, that is, the network contains a few beacon nodes, which obtain their location information by carrying the GPS location element, and send a beacon message containing the location reference information in order to build the coordinate system. In the unknown node location process, the position relations (distance, angle, or region inclusion relation) of the unknown node to multiple adjacent beacon nodes are measured or estimated, and then the coordinates of the unknown node are calculated by using these position relations and specific algorithms, where

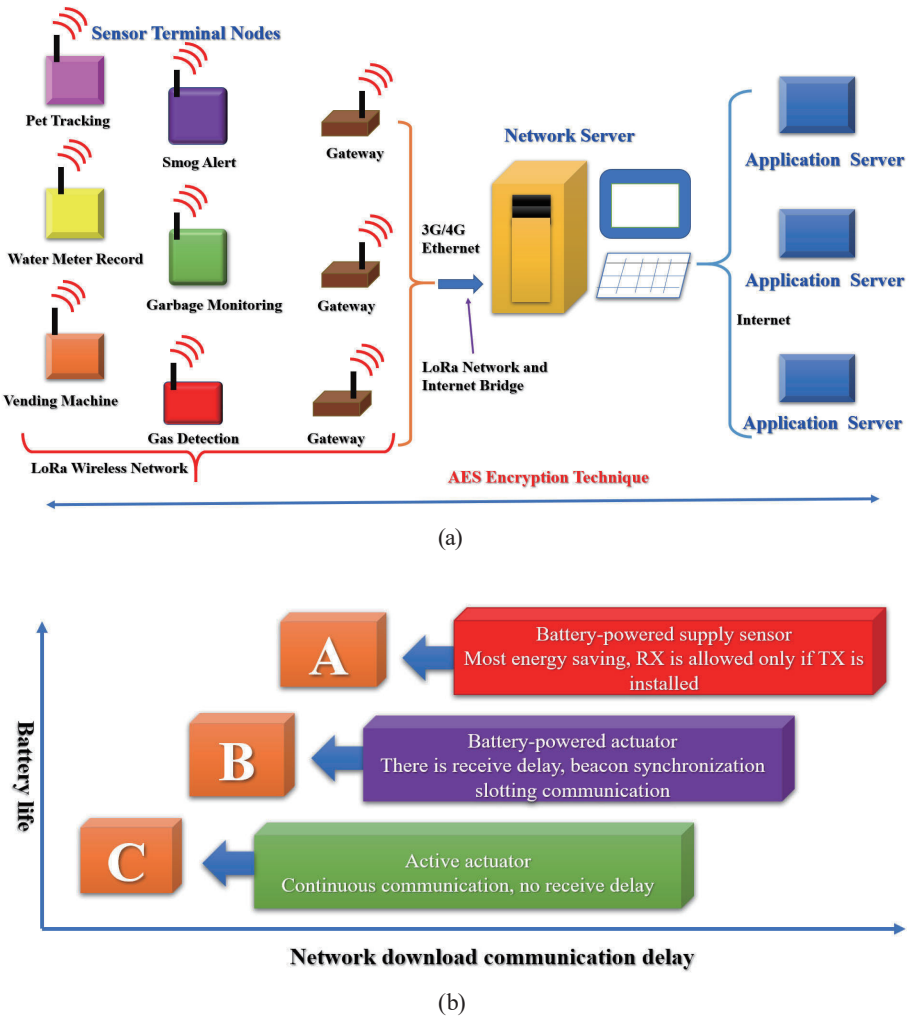


Fig. 1. (Color online) (a) LoRa network architecture. (b) LoRa class comparison.

the calculation-performing subject can be the unknown node, beacon node, or some authority node, and the common algorithms include trilateration, triangulation, and multilateration. The localization systems include range-based localization and range-free localization. Range-based localization measures the point-to-point distance or angle information between nodes, where the common measuring techniques include time of arrival (TOA), time difference of arrival (TDOA), angle of arrival (AOA), and received signal strength indicator (RSSI). Range-free localization uses network connectivity to estimate the position relation between nodes, where the common algorithms include the centroid algorithm, approximate point-in-triangulation test (APIT) algorithm, distance vector (DV)-Hop algorithm, convex programming algorithm, and amorphous algorithm.[12–14]

2.2 Analysis of attacks on the node localization system

Attacks on a node localization system mainly occur in the position relation measuring and estimation stages. The attack target is usually the beacon node or the wireless link for transmitting beacon messages. As different localization systems are based on different physical attributes and localization processes, the means of an attack are closely related to the location technique used by the system, which is analyzed, as follows.

2.2.1 Attack on range-based localization

Range-based localization is especially exposed to ranging interference or spoofing attacks in the physical layer or link layer; thus, the deviation of the ranging result from the actual result exceeds the normal range. An attacker can move and isolate the beacon node to reduce localization accuracy, as well as initiate a radio interference attack; for example, an obstacle is placed between the sender and the receiver, meaning that the beacon message is transmitted on multiple paths, the signal transmission time is prolonged, and the AOA or strength of the signal is changed. The TOA/TDOA[11] location technique measures the round-trip time of a call-reply message to calculate the distance between nodes, and the response message is sent earlier or later to spuriously reduce or increase the nodal distance. The AOA algorithm[5] measures the relative orientation or angle between the receiving node and the transmitting node, and a reflector is located to change the AOA of the signal. The RSSI ranging technology[6] uses a theoretical or empirical model to convert the transmission loss into distance, where an obstacle with the absorption function is located between the beacon node and the unknown node, or ambient channel noise is partially increased to attenuate the signal, which renders the measured distance of the unknown node longer than the actual distance. Moreover, the attacker can use different transmission media or transmission powers to create illusions, leading to false measurement results.[15,16]

2.2.2 Attack on range-free localization

Similarly, range-free localization is exposed to attacks with the purpose of interference or cheating in the position relation estimation stage. However, in addition to the aforesaid attacks on nodes, the physical layer, or the link layer of a wireless channel, there are attacks on the network layer, such as replaying, forging, tampering, dropping beacon messages, wormhole attacks, and Sybil attacks. A Sybil attack on a localization system means that one malicious node fabricates many different identities; thus, multiple nonexistent nodes occur in the network, which disturb the normal operations of the localization protocol. To be more specific, in the centroid algorithm,[7] the location of the unknown node is determined as the polygonal centroid formed of k adjacent beacon nodes:

$$\left(X_{est}, Y_{est}\right) = \left[\frac{X_1 + ... + X_k}{k}, \frac{Y_1 + ... + Y_k}{k}\right], \tag{1}$$

where (X_i, Y_i), $1 \leq i \leq k$, are the beacon node coordinates. Clearly, a small number or a nonuniform distribution of adjacent beacon nodes can directly affect the accuracy of unknown node location estimation. At this point, the attacker can isolate a part of the neighboring nodes (e.g., arranging an obstacle with strong signal-absorbing capacity near the node) to reduce judgment accuracy. The perfect point-in-triangulation test (PIT) theory assumes that all neighbor nodes of node M are simultaneously not far from or close to three beacon nodes (A, B, and C) in relation to node M, where M is in ⊿ABC; otherwise, M is out of ⊿ABC. In the APIT algorithm,[8] which is based on the PIT theory, the attacker can initiate a wormhole attack, as shown in Fig. 2. If there is a wormhole link between node S and node 5, and node 5 is simultaneously far from the three beacon nodes, according to the PIT principle, S is misidentified as being out of the triangle.

In the range-free localization based on the distance vector,[9,10] the attacker can directly remove the node to induce the calculation error of each skip distance, and use jamming or a wormhole attack to induce the unknown node to obtain a false minimum hop count value from the beacon node, and the beacon node works out the false average hop distance. Figure 3 shows network-layer attacks on the localization algorithm that are based on the distance vector. Figure 3(a) shows the normal condition. Figure 3(b) corresponds to a wormhole attack with the purpose of reducing the hop count. Figure 3(c) corresponds to a jamming attack with the purpose of increasing the hop count.

However, the security problem is less considered in the initial design of the LoRa IoT node localization system. For a period of time, domain research has concentrated on how to enhance

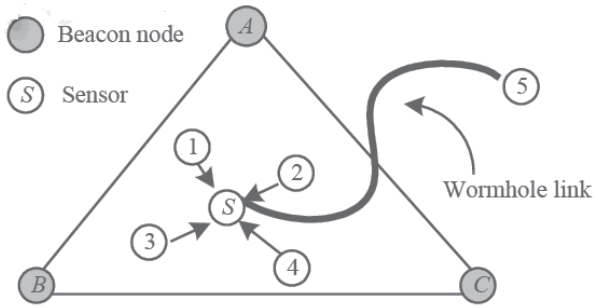
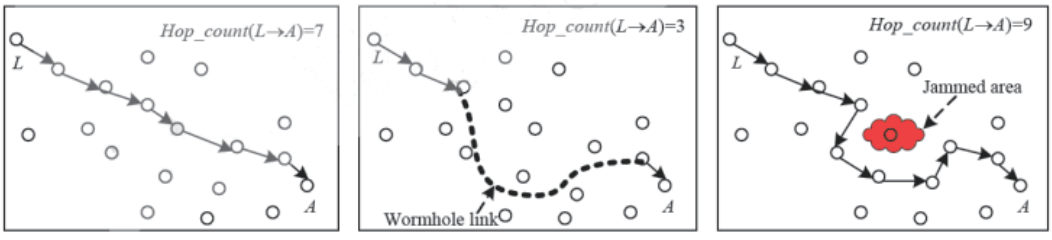


Fig. 2. Wormhole attack towards APIT algorithm.



(a) (b) (c)

Fig. 3. (Color online) Network-layer attacks towards DV-based localization algorithms.

localization accuracy and energy efficiency, while, in fact, the lack of an effective security mechanism has become the principal restriction on using LoRa IoT. As the node localization system is the key service of LoRa IoT, an attacker may damage the effectiveness of the LoRa IoT application with attack position information. Thus, this security problem has gradually attracted attention. To date, many security solutions for localization systems that can solve different security threats and support different applications have been proposed, which have different localization principles, network facilities, security techniques, attack resistances, and space-time complexities. A wireless message with localization reference information is called a beacon, a node with a known location that provides the beacon is called an anchor node, and the LoRa IoT node to be localized is called an unknown node.[17,18]

3. Sensor Localization Techniques and Analysis

In the study of wireless sensor networks (WSNs), the node localization problem is a popular research area, as the accurate localization of a node is the fundamental condition of the WSN application; for example, the location information of sensor nodes must be known in battle zone reconnaissance, ecological environment monitoring, and earthquake, flood, and fire site monitoring in order to obtain the accurate location of an information source. In addition, the location information of nodes can be used to increase routing efficiency, report network coverage quality to the deployer, and implement the network load balancing and self-configuration of the network topology.[19–24] As sensor nodes are limited by cost, energy, and volume, the localization ability of WSNs encounters a new challenge. While GPS is a method to obtain location information, it requires numerous sensor nodes; thus, the cost of the GPS scheme is very high. Furthermore, as sensor nodes are powered by a battery, the electric energy is very limited and cannot be supplemented, meaning that it is not feasible to provide each node with high-energy-consuming GPS equipment. In addition, the electric energy consumed by the wireless communication between nodes is much higher than the electric energy consumed by other parts. Thus, the wireless communication between nodes should be reduced as much as possible, and a low-energy-consuming node localization algorithm should be designed to prolong the lifetime of the sensor network as much as possible.

Since AT&T Laboratories Cambridge developed the localization system Active Badge in 1992,[25–27] researchers have been developing self-localization systems and algorithms. During these years, while many of the developed techniques can solve the self-localization problem of wireless sensors, many types of systems and algorithms have been used to solve different problems or to support different applications. There are different physical phenomena for localization, the composition of LoRa IoT equipment, energy demands, infrastructure, and space-time complexity, and most have high communication energy consumption and require additional hardware.

In a WSN, the location information is very important for the monitoring activity of the sensor network, and the location of an event or the acquired node location is important information contained in the sensor node monitoring information. The localization of a sensor node is the process of determining the node location from a few nodes with known locations and some

localization mechanisms. Only when the sensor node is localized can the specific location of an event monitored by a sensor node be determined. Therefore, in the sensor network, the correct localization of a sensor node is a precondition of many practical applications. Many researchers are currently working on this issue, and they have proposed many solutions regarding localization problems.[1] Table 1 compares the existing typical localization algorithms.

Their characteristics and analysis of the various positioning algorithms are as follows:

(1) The unknown node must be directly adjacent to the anchor node, and the density of the anchor node is too high, such as in the centroid algorithm, DV-Hop. The anchor must have a device that receives GPS data, so the cost of the sensor will increase.

(2) Positioning accuracy depends on network deployment conditions. For example, DV-Hop is only suitable for densely deployed isotropic networks. The convex programming algorithm requires anchor nodes to be deployed at the edge of the network. Limiting the sensor's deployment conditions will increase the cost of the sensor.

(3) There is no measure for suppressing the distance/angle measurement error, resulting in error propagation and error accumulation. The positioning accuracy depends on the accuracy of the distance/angle measurement, for example, DV-distance. Error propagation and error accumulation increase the amount of data transmitted by the sensor, which obviously consumes the power of the sensor.

(4) Relying on the loop refinement process to suppress the ranging error and improve positioning accuracy. Although the loop refinement process can significantly reduce the impact of the ranging error, it not only requires a large amount of communication and computational energy but also increases the uncertainty of the algorithm because it cannot predict the number of loops, for example, a convex programming algorithm. A large amount of communication and computational energy is also a cost burden since it increases the power and space of the sensor.

(5) Existing algorithms do not consider indoor environments, such as environmental noise, penetration effects, multipath effects, and nonline of sight (NLOS) caused by complex indoor environments.

Therefore, the paper proposes the architecture of a WSN of LoRa to solve the problem of power consumption and reduce the cost of using the sensor. Although the LoRa WSN architecture cannot completely solve the problems of various positioning algorithms described above, the LoRa WSN has the characteristics of low cost, low power consumption, and long-distance transmission of data. Therefore, our proposed LoRa WSN uses RSSI technology to calculate the positioning points. The features of the proposed method include:

Table 1
Comparison of typical sensor network localization algorithms.

Algorithm name	Distributed/centralized	Ranging required	Distance estimation method	Localization method
RADAR	Centralized	No	None	Match
Centroid localization	Distributed	No	Communication range	Centroid
Convex programming	Centralized	No	Communication range	Optimization
DV-hop	Distributed	No	One-hop distance	Triangulation
DV-distance	Distributed	Yes	Signal strength	Triangulation

a. The hardware consumes low energy: the sensor node does not require additional positioning hardware devices that consume power, volume, and weight, such as GPS sensing devices.
b. The computational and communication energy consumption is low: this can extend the life cycle of the sensor network and reduce the power consumption of the system.
c. Easy to implement: it can be easily ported on existing sensor network systems.
d. Positioning self-organization: does not depend on other fixed equipment and fixed structures, as well as external positioning systems.
e. Accurate results: the location information provided can meet the application needs.

However, the security problem was less considered in the initial design of the IoT node localization system. For a period of time, research on this domain has been concentrated on how to enhance localization accuracy and energy efficiency, while in fact, the lack of an effective security mechanism has become the principal restriction for IoT applications. As the node localization system is the key service of IoT, an attacker may damage the effectiveness of the LoRa IoT application using the attack position information; thus, the security problem has gradually attracted attention. To date, many security solutions for the localization system have been proposed, and these solutions can solve different security threats and support different applications, as they differ in localization principles, network facilities, security techniques, attack resistance, and space-time complexity.

4. Research Method and Problem Analysis

In this study, we use LoRa wireless transmission to solve various problems, such as short transmission distance. LoRa is one of the LPWAN wireless transmission technologies, and its main advantages include low power consumption and LoRa, meaning one battery can sometimes supply power for a long time. It is most suitable for the farming culture, which requires extensive monitoring. As this test simulates a fish pond culture system, and the ordinary ZigBee is mainly for short-range wireless transmission, simple distance testing is performed on LoRa to determine its advantages in terms of transmission distance. In this study, we use a remote mobile phone connection to operate a laboratory computer, where the signals are sent to the designed LoRa mobile transceiver for testing, as shown in Fig. 4(a). When the LoRa mobile transceiver receives data, the data displayed on the liquid crystal display (LCD) are immediately updated, and then the received confirmation message is fed back to the laboratory computer in order to ensure that the data are received and correctly fed back, and the LoRa transmission is carried out after the site of the received data is confirmed by the phone GPS positioning, as shown in Fig. 4(b). Figure 4(c) uses the periphery map of the Chin-Yi campus, as drawn by Google, where the yellow star indicates the E315 laboratory computer on the 3rd floor of the Chin-Yi Engineering Hall, i.e., the location of the LoRa receiving-transmitting site. The blue part is the area where the signals are easily received, which covers the entire Chin-Yi campus; the signals are good in this range, the sent data are correctly received, and the characters are fed back by both sides each time. The yellow part is the area where the data are likely to be lost during testing, meaning that the mobile transceiver terminal

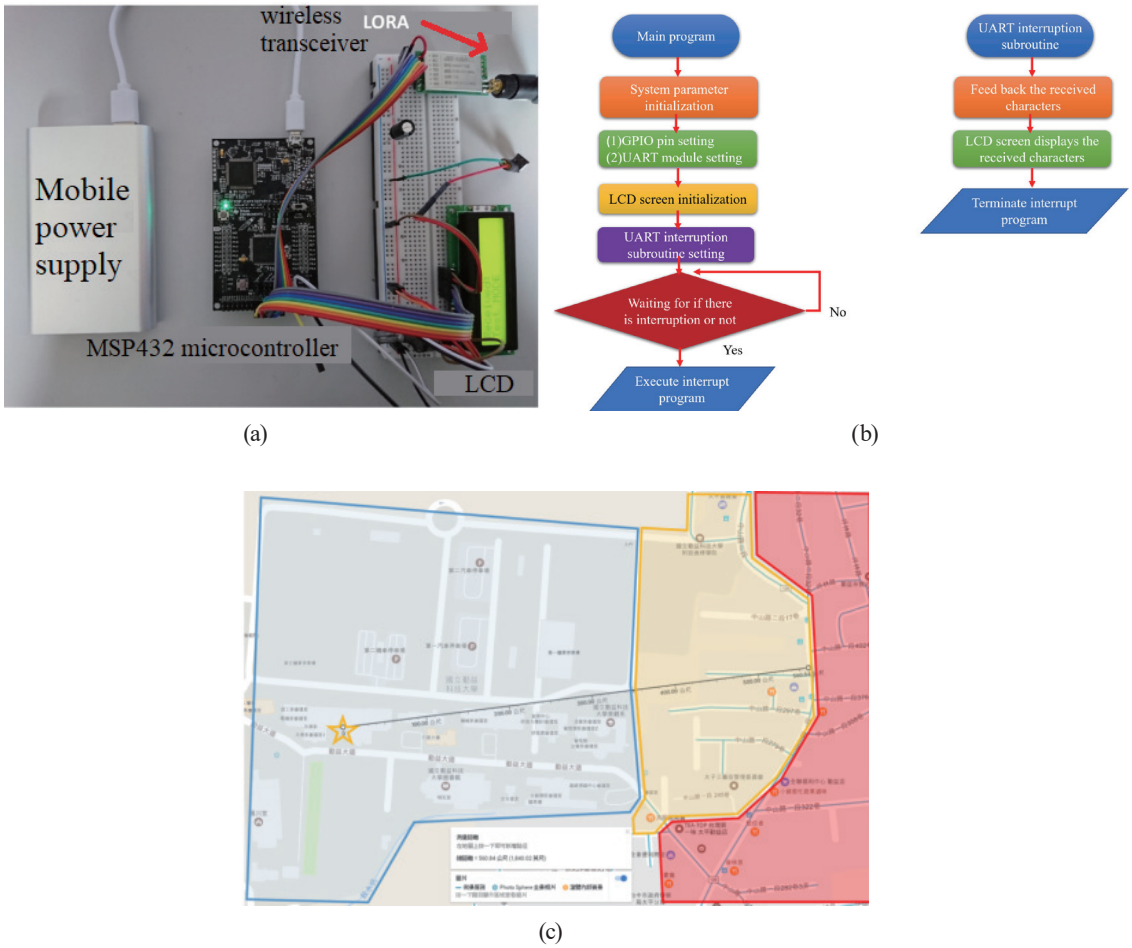
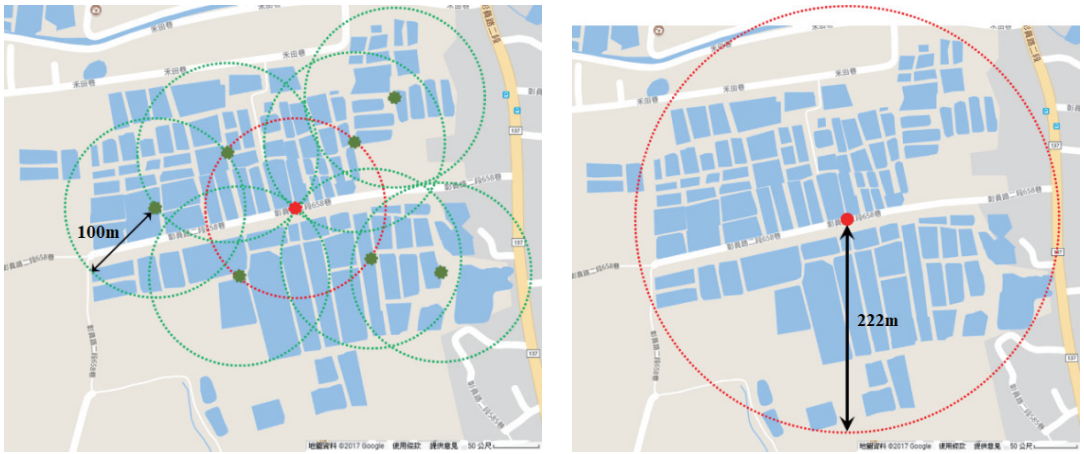


Fig. 4. (Color online) (a) LoRa mobile transceiver. (b) LoRa mobile transceiver program flow. (c) Illustration of LoRa transmission.

has received data, but the data cannot be correctly fed back to the laboratory computer terminal, or the data are received after a long time. The red area is where none of the data has been received.

Figure 5 shows a map of a fish pond cultivation farm in Changhua County. The blue block areas are the fish ponds, and the entire cultivation farm is about 450 m long and 400 m wide. In this study, we assume that the cultivation farm is clear and obstacle-free, and the frameworks of ZigBee and LoRa networks are arranged while disregarding the sensing terminals, as shown in Figs. 6(a) and 6(b), where the red point is the coordinator, the green points are routers, and the dotted circles represent the signal coverage areas. As the universal ZigBee transmission distance is about 100 m, the radius of the ZigBee transmission coverage is set as 100 m, and the entire cultivation farm can be covered provided that the radius of the LoRa transmission coverage area is larger than 222 m. According to the aforesaid distance test, the LoRa transmission distance exceeded 222 m; thus, the cultivation farm can be covered, and even

Fig. 5. (Color online) Map of cultivation farm.



(a) (b)

Fig. 6. (Color online) (a) ZigBee network plan. (b) LoRa network plan.

exceeded, by placing one coordinator. The two maps show that the number of network nodes of ZigBee is much larger than that of LoRa; thus, the cost can be reduced by using a LoRa network.

5. System Encryption and Decryption Process

Asymmetric encryption requires higher computational cost than symmetric encryption, while the sensor computing power and storage space are small, and it is not suitable for performing the asymmetric computation of many computations, such as the Rivest–Shamir–Adleman (RSA) algorithm.[28] This paper uses the Rabin asymmetric key encryption algorithm.[29] This algorithm is more in line with the low power consumption of the LoRa wireless sensing network.

This article takes the application of the RoLa sensing network architecture as an example and applies the Rabin asymmetric key encryption algorithm to the node sensor to achieve the purpose of lightweight encryption. After the sensor adds the plaintext to the confirmation data, the ciphertext is obtained by using the Rabin encryption, and then the ciphertext is divided into two packets and sent out, and decrypted on the server side.

When using the Rabin asymmetric key encryption algorithm, the longer the plaintext data is, the longer it will take to encrypt. The encryption method is based on the formula

$$C = M^2 \bmod N. \tag{2}$$

Here, C is the ciphertext, M is the plaintext, N is the public key, and $N = P \times Q$. P and Q are private keys, which are composed of prime numbers, and $P \bmod 4 = 3$, $Q \bmod 4 = 3$. The squared value of the plain text is divided by the value of the public key, and finally, the remainder is obtained. This remainder is the ciphertext generated after encryption. This study selected a private key of approximately 512 bits in size, resulting in a public key of approximately 1024 bits. This setting is more suitable for information encryption of the sensor.

After the server receives the complete ciphertext C transmitted by the sensor, the four sets of plaintexts M_1–M_4 can be calculated by using the two private keys P and Q and the public key N. The decryption formula is as follows:

(i)

$$W_1 = C^{(P+1)/4} \bmod P \tag{3}$$

$$W_2 = P - C^{(P+1)/4} \bmod P \tag{4}$$

$$W_3 = C^{(Q+1)/4} \bmod Q \tag{5}$$

$$W_4 = Q - C^{(Q+1)/4} \bmod Q \tag{6}$$

(ii)

$$a = Q \times \left(Q^{-1} \bmod P \right) \tag{7}$$

$$b = P \times \left(P^{-1} \bmod Q \right) \tag{8}$$

(iii)

$$M_1 = \left(a \times W_1 + b \times W_3 \right) \bmod N \tag{9}$$

$$M_2 = \left(a \times W_1 + b \times W_4\right) \bmod N \tag{10}$$

$$M_3 = \left(a \times W_2 + b \times W_3\right) \bmod N \tag{11}$$

$$M_4 = \left(a \times W_2 + b \times W_4\right) \bmod N. \tag{12}$$

Among $\{M_1, M_2, M_3, M_4\}$, only one solution is equal to the original M.

Due to the Rabin asymmetric key encryption algorithm, a ciphertext will be solved by four sets of plaintexts. Therefore, when the correct plaintext is found, the original text can be added to the original text. The method used in this article is to take a letter from the original plaintext as the comparison data and attach it to the original plaintext to form a new plaintext for encryption, as shown in Fig. 7.

In the same way, when the ciphertext is reduced to plaintext, the correct plaintext can be verified by comparing the data, as shown in Fig. 8. If there are M letters in the original plaintext and N letters are selected for comparison, the probability of correcting the result of one or more plaintext verifications by this method is $10^{(M-N)}/10^M$. Therefore, the more data are selected, the lower the probability that the same clear text verification result will be the same.

6. System Architecture

The positioning used in this project is based on the dynamic adjustment method. We call this system the intelligent optimization positioning system. RSSI is the foundation of our proposed method. We will determine the basis of the deployment through the signal

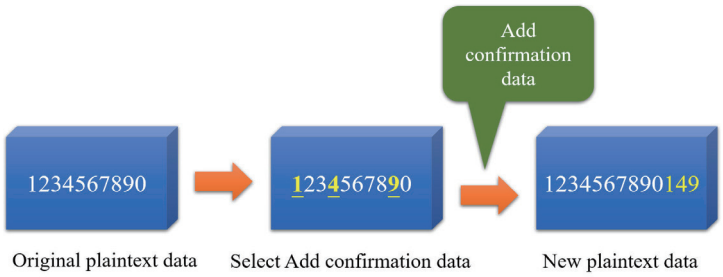


Fig. 7. (Color online) Adding confirmation data.

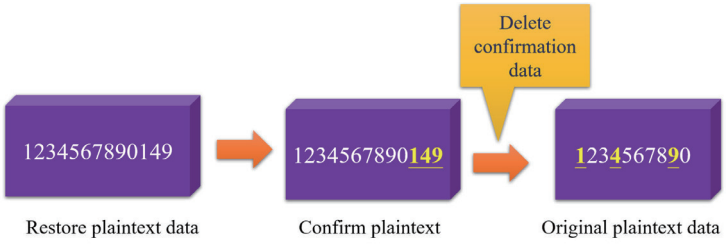


Fig. 8. (Color online) Verification of confirmation data.

receiving strength and the packet reliability, so we will summarize and create new algorithms. The algorithm used is called Secure Information Based Multi-Sensors Fusion Computing Localization (SIBMSFCL).[30,31] On this basis, using the predicted residual root mean square difference based on the minimum-security reference set, the remaining reference points are diagnosed one by one, which improves the ability of the positioning system to tolerate attacks. When the packet of the sensing signal is transmitted by the network protocol, the positioning result is affected by the packet delay. The algorithm diagnoses an abnormal point and calculates the number of tolerant attacks, and a positioning multisensing fusion computing service is present. In the network protocol, as the packet delay affects the localization result, LoRa is selected for its lower delay probability than the traditional ZigBee packet transmission (10.5% < 34.6%) on the basis of the analysis of the LoRa IoT platform localization technique, network security, multisensor fusion computing, and low power consumption. Thus, a low-cost LoRa IoT secure localization multisensor fusion computing experiment platform with independent intellectual properties is designed, where the SaaS and PaaS application security is developed as the main multisensor fusion service for specific applications in order to design a new low-power-consumption and easily implemented secure sensor network localization algorithm, which is an important research subject of sensor networks at the present stage. This secure localization system is substantially a cooperative mechanism for determining the spatial relationship of nodes according to the physical phenomenon of wireless communication, and its security implementation is confronted with huge challenges. The security of a localization system depends to a great extent on the security service ability of the entire network system. Owing to the inherent weak points of LoRa IoT, including its open deployment and node resource constraints, the network cannot be completely trusted. Regarding the broadcasting characteristics of radio, as the physical phenomena that localization depends on are likely to be tampered with, it is difficult for this traditional technology to withstand such external threats. As localization information is naturally asymmetric, it is difficult to check whether the unknown node received the correct beacon. Thus, the localization attack or anchor node trust is judged by itself. Therefore, the localization system has been one of the outstanding security weaknesses of LoRa IoT.

The overall system is divided into three parts according to the operational flow: a sensor terminal (wireless humidity, temperature, and infrared sensor terminal), the Raspberry Pi high-level development platform (chip programming) function of MQTT, which is a multisensor fusion computing platform for secure localization calculation, and a network server host of the central monitoring system. Figure 9 presents the system architecture. Figure 10 shows the system circuit diagram. Figure 11 presents the LoRa network and security mechanism calculation design and multisensor fusion computing platform construction.

7. Experimental Results and Analysis

7.1 LoRa network topology and actual execution of localization

(a) Indoor localization experiment: The high based enhancements (HBE) values within 1 to 4 m are measured by using the method proposed in Ref. 13, where each meter is measured 20

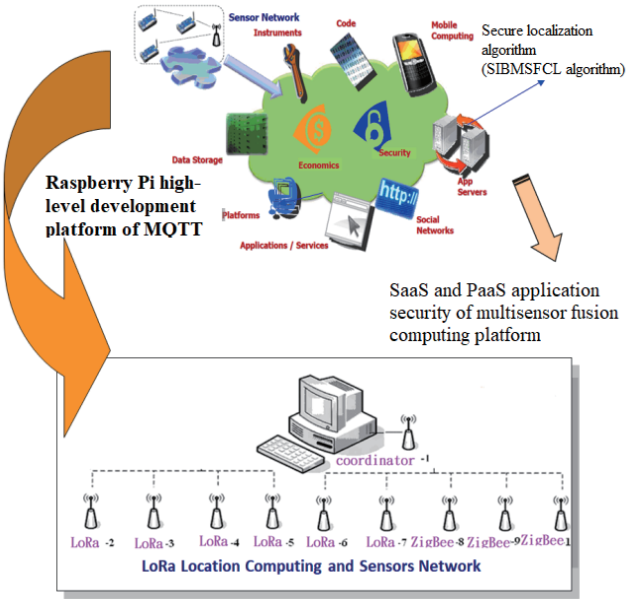


Fig. 9. (Color online) System architecture.

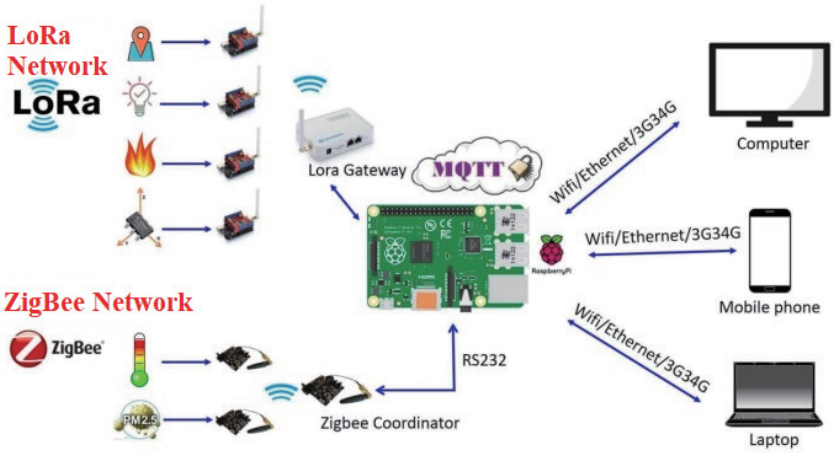


Fig. 10. (Color online) System circuit diagram.

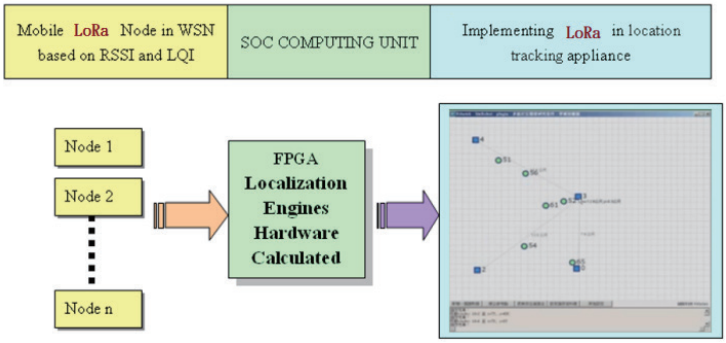


Fig. 11. (Color online) LoRa network and security mechanism calculation design and multisensor fusion computing platform construction.

times, the average is taken, and the line chart is made, as shown in Fig. 12. The linear equation of HBE is calculated according to the figure, as expressed by Eq. (13), the measured RSSI is calculated using Eq. (14) to obtain the distance $d1$ affected by HBE, $d1$ is substituted in Eq. (13) to obtain HBE, and the distance $d2$ not affected by HBE is calculated using Eq. (15).

$$HBE = -1.166d1 - 2.334 \tag{13}$$

$$RSSI = -30 - 10 \times 3.3219 \times \log\,(d1) \tag{14}$$

$$RSSI - HBE = -30 - 10 \times 3.3219 \times \log(d2) \tag{15}$$

The reference points are in the space for this experiment, as shown in Fig. 13. The range of the experiment is 2 to 4 m, and the subjects compared are the first RSSI primal algorithm and the RSSI weighting method with the corrected propagation coefficient n under the HBE effect, as proposed by scholars in 2012. The comparison results are shown in Table 2. This experiment proves that the accuracy of the localization distance error correction algorithm is higher than that of the RSSI primal algorithm by 50%, and higher than that of the RSSI weighting method with the propagation coefficient n by about 8%.

(b) Outdoor localization experiment: the HBE values from 10 to 50 m are measured using the method proposed in Ref. 13, where every 10 m is measured 30 times, the average is taken, the line chart is made, and the linear equation of HBE is calculated according to the chart, as

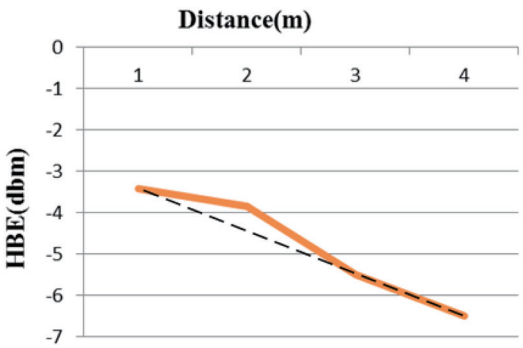


Fig. 12. (Color online) Relationship between HBE and distance within 1 to 4 m.

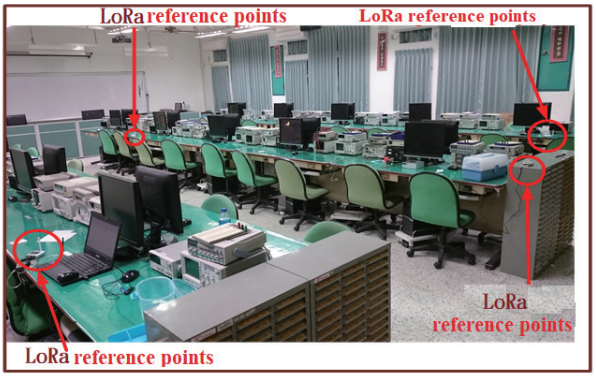


Fig. 13. (Color online) Actual layout of reference points in laboratory class.

Table 2
Comparison between indoor localization distance error correction algorithm and other algorithms.

Actual distance (m)	RSSI primal algorithm (m)	RSSI weighting method with propagation coefficient (m)	Localization distance error correction algorithm (m)
2	0.71	1.71	1.78
2.5	1.22	2.16	2.23
3	1.53	2.51	2.71
3.5	1.71	2.72	3.15
4	2.03	3.45	3.77

expressed by Eq. (13). The measured RSSI is calculated using Eq. (13) to obtain the distance $d1$ affected by HBE, $d1$ is substituted in Eq. (13) to obtain HBE, and the distance $d2$ not influenced by HBE is calculated using Eq. (15). Figure 14 shows the actual layout of the outdoor reference points. Table 3 shows the comparison between outdoor localization distance error correction algorithm and other algorithms.

7.2 LoRa network and security mechanism calculation design and multisensor fusion computing platform construction

The recovery time for correcting the error localization information is determined according to the number of reference points; the larger the number of reference points, the larger the number of counts. However, the accuracy is better, as described in Table 4.

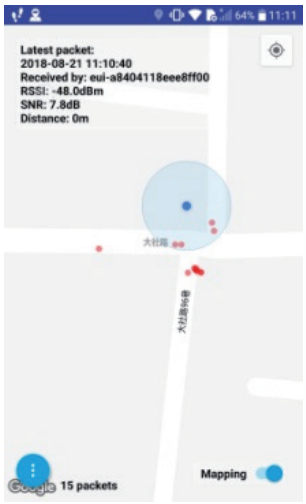


Fig. 14. (Color online) Actual layout of outdoor reference points.

Table 3
Comparison between outdoor localization distance error correction algorithm and other algorithms.

Actual distance (m)	RSSI primal algorithm (m)	RSSI weighting method with propagation coefficient (m)	Localization distance error correction algorithm (m)
10	3.68	5.32	2.36
20	4.85	7.62	2.54
30	5.12	7.78	2.48
40	5.58	8.03	2.38
50	6.31	8.62	3.10

Table 4
Recovery time experiment.*

		Number of reference points			
		3	4	5	6
Item	Number of error localizations	1	1	1–2	1–3
	Accuracy (%)	88.3	91.1	95.8	96.1
	Recovery time (s)	0.23	0.78	1.52	1.87

*The environmental conditions of all experiments are identical, but the number of reference localization points is varied.

7.3 LoRa IoT localization calculation using the design of Arduino UNO

This project uses the SIBMSFCL algorithm to validate the effect of this localization algorithm, and the organization state of the nodes is dynamically and adaptively adjusted. The comparison between the localization result of this algorithm and the GPS positioning result shows that the error is less than 5%. In this project, we perform abnormality diagnosis on the basis of the predicted residual root-mean-square deviation of the security reference set in order to avoid (a) the covering phenomenon, i.e., failing to identify abnormal points, and (b) the flooding phenomenon, i.e., misidentifying normal points as abnormal points.

7.4 Jamming test for LoRa and other wireless communication frequency bands

The interference source and experimental equipment of this project are tested using the same and multiple frequency bands. When there is too much interference in the localization system operating frequency band, it is necessary to skip to another clean frequency band. According to the experimental analysis of this project, when the RFID UHF starts working, the signal strength of the LoRa network is affected, meaning that it is slightly weakened, and the RSSI of the server side and client side changes and recovers its stability. Thus, there is no packet loss, which is a characteristic of LoRa. If the communication frequency bands are different, the other different wireless frequency band communications will not affect the signal intensity or packet transmission of LoRa communication. Thus, the LoRa network is tested in a heterogeneous network environment and the LoRa-influencing network bandwidth is 915 MHz, which is an ultrahigh frequency; therefore, in an environment with other networks, e.g., a Zigbee network, the transmission efficiency is not affected, and there is no packet loss or packet collision. LoRa wireless communication technology can use a multihop network to expand its monitoring range and reduce the arrangement costs. If there is packet loss, the retransmission mechanism can be used to enhance the integrity of data, and the nonperiodic packet is sent for real-time reporting when an exception or a critical event is detected, meaning that the gateway can respond to the situation to completely analyze data.

A new algorithm, called SIBMSFCL, is concluded and created, where the residual reference points are diagnosed one by one according to the predicted residual root-mean-square deviation of the minimum security reference set, in order to enhance the attack tolerance of a localization system. The parameters of the SIBMSFCL equation can be estimated according to the known sample data. Regarding the signal source of unknown coordinates, the unknown object location is calculated. The steps are described below.

1. A random coordinate point s is selected as the starting point as well as a fixed range ε.
2. For six points along x, y, and z axes, and at a distance of ε units from s, the signal strength of various readers is estimated.
3. The signal strength of each point, as well as the RMSE of the actual signal strength, is calculated.
4. The point p with the minimum error is selected, and s is replaced by p.
5. When s no longer changes, it is taken as the estimated location, and searching is stopped.

Experimental results: according to the RSSI data of the test sample, the location of the test sample is estimated by using the SIBMSFCL algorithm, the distance error to the actual location is calculated, and the error accumulation probability is shown in Fig. 15. The localization accuracy of SIBMSFCL within 21 m is 99–100%, whereas the localization accuracy within 32 m is about 85%. In addition, as the interval between sampling points increases, the error increases slightly; thus, it is obvious that the effect of the sampling interval is slight, and there is no large difference within at least 50 m.

Regarding reliability, as proposed by Kelly and coworkers,[32,33] the reliability of the LoRa system in this project is obtained by calculating the correct information content received by sensors, the number of lost packets, and the total number of packets from the terminal node to the coordinator. In this study, according to the distance between the target and the system, under the condition of signal transmission reliability are 10, 30, and 50 m on a sunny day, 50 m on a cloudy day, and 50 m on a rainy day, where the data are sent once per second, and reliability is rounded to two decimal places. The experimental results of one day are shown in Table 5; the longer the transmission distance, the lower the packet reliability. However, the reliability is relatively high within 30 m. Equation 16 shows the formula used to obtain the percentage reliability.

$$\text{Reliability}(\%) = \frac{\text{Received packet number}}{\text{Total number of packets}} \times 100\% \tag{16}$$

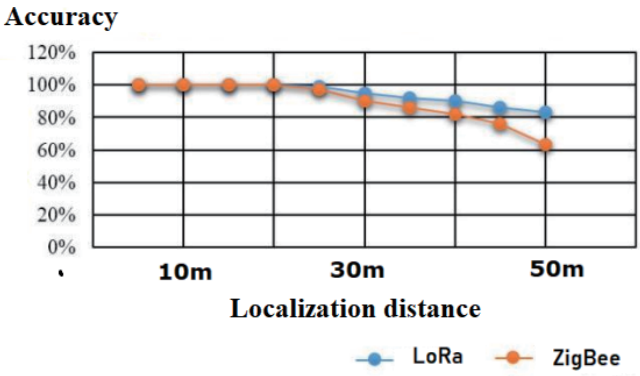


Fig. 15. (Color online) Error accumulation probability of the SIBMSFCL algorithm. The environmental conditions of all experiments are identical, but the localization point distance is varied.

Table 5
Distance-based received packet reliability.*

		Transmission distance (m)				
		Sunny 10	Sunny 30	Sunny 50	Cloudy day 50	Rainy day 50
Item	Total number of packets (pcs)	86394	84760	81843	66.672	43.210
	Number of packets received (pcs)	84422	82466	77807	59.231	38.956
	Number of packets lost (pcs)	1972	2294	4036	5823	7538
	Reliability (%)	97.72	97.29	95.07	84.05	73.68

*The number of reference localization points is fixed for all experiments, but the environmental conditions are varied.

8. Conclusion and Future Work

In recent years, with the rapid development of network security, multisensor fusion computing, and LoRa technology, the localization system of a national security monitoring system has become a very important part of technology enhancement, and the various techniques applied to the LoRa wireless sensor security localization design are gradually attracting attention as their high potential for development is revealed. Therefore, in recent years, many universities have studied automation engineering and communication technology domains in succession. In terms of the development of traditional wireless sensor design systems, many experts and scholars have studied relevant localization calculations and obtained good outcomes. However, in comparison with the development using network security, multisensor fusion computing, and LoRa technology to integrate traditional national security monitoring systems, there has been less effort devoted to input research, and this secure localization computing technology has an absolutely profound effect on the development of national security monitoring systems. Therefore, the construction of a national security monitoring system using network security, multisensor fusion computing, and LoRa technology, as developed in this study, will have specific and substantive contributions. In this project, we calculated packets and compared other improvement methods with ZigBee, and the results showed that reliability can be increased by about 30%, thus meeting the required unit system specifications. The findings of this study will be adapted to a national security monitoring system platform with practical popularization values, and related results will be published in international journals.

Acknowledgments

This research was supported by the Department of Electrical Engineering, National Chin-Yi University of Technology, Taiwan. The authors would like to thank the National Taipei University of Technology, Hungkuo Delin University of Technology, Taiwan, for financially supporting this research.

References

1 A. Lavric and V. Popa: 2017 Int. Symp. Signals, Circuits and Systems (2017) p. 1.
2 R. Tomar and O.-G. Gemein: 2018 Global Internet of Things Summit (2018) p. 1.
3 X. Zhang, M. Zhang, F. Meng, Y. Qiao, S. Xu, and S. Hour: IEEE IoT J. **6** (2019) 590.
4 F. Y. Ren, H. N. Huang, and C. Lin: J. Software **14** (2008) 1282 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1282.htm
5 F. B. Wang, L. Shi, and F. Y. Ren: J. Software **16** (2011) 857 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/857.htm
6 A. Harter, A. Hopper, P. Steggles, A. Ward, and P. Webster: Mobile Computing and Networking (ACM Press, 2008) p. 59.
7 N. Priyantha, A. Chakraborty, and H. Balakrishnan: Mobile Computing and Networking (ACM Press, 2010) p. 32.
8 D. Nicelescu and B. Nath: IEEE Computer and Communications Societies (IEEE Press, 2009) p. 1734.
9 P. Bahl and V. N. Padmanabhan: IEEE Computer and Communications Societies (IEEE Press, 2011) p. 775.
10 N. Bulusun, J. Heidemann, and D. Estrin: IEEE Pers. Commun. **7** (2010) 28.

11 T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher: Mobile Computing and Networking (ACM Press, 2008) p. 81.
12 D. Niculescu and B. Nath: J. Telecommun. Syst. **22** (2008) 267.
13 R. Nagpal, H. Shrobe, and J. Bachrach: Information Processing in Sensor Networks (Springer-Verlag, 2008) p. 151.
14 S. Brands and D. Chaum: Theory and Application of Cryptographic Techniques on Advances in Cryptology (Springer-Verlag, 2010) p. 344.
15 A. Mahmood, E. Sisinni, L. Guntupalli, R. Rondón, S. A. Hassan, and M. Gidlund: IEEE Trans. Ind. Inf. **15** (2019) 1425.
16 R. M. Sandoval, A.-J. Garcia-Sanchez, J. Garcia-Haro, and T. M. Chen: IEEE IoT J. **5** (2018) 3114.
17 L. Feltrin, C. Buratti, E. Vinciarelli, R. D. Bonis, and R. Verdone: IEEE IoT J. **5** (2018) 2249.
18 J.-T. Lim and Y. Han: IEEE Commun. Lett. **22** (2018) 800.
19 N. Sastry, U. Shankar, and D. Wagner: 2003 ACM Workshop on Wireless Security (ACM Press, 2010) p. 1.
20 C. Meadows, R. Poovendran, D. Pavlovic, L. W. Chang, and P. Syverson: Wireless Sensor and Ad Hoc Networks (Springer-Verlag, 2007).
21 S. Capkun and J. P. Hubaux: IEEE Computer and Communications Societies (Computer Society Press, 2005) p. 1917.
22 Y. Zhang, W. Liu, Y. Fang, and D. Wu: IEEE J. Sel. Areas Commun. **24** (2010) 829.
23 S. Capkun, M. Cagalj, and M. Srivastava: IEEE Conf. Computer Communications (IEEE Computer Society Press, 2009) p. 23.
24 F. Anjum, S. Pandey, and P. Agrawal: IEEE International Conf. Mobile Ad-Hoc and Sensor Systems (IEEE Computer Society Press, 2005)
25 L. Lazos and R. Poovendran: ACM Transactions on Sensor Networks (ACM Press, 2004) p. 21.
26 L. Lazos, R. Poovendran, and S. Capkun: Information Processing in Sensor Networks (IEEE Computer Society Press, 2005) p. 324.
27 L. Lazos and R. Poovendran: HiRLoc: IEEE J. Sel. Areas Commun. **24** (2006) 233.
28 R. Rivest, A. Shamir, and L. Adleman: Commun. ACM **21** (1978) 120.
29 M. Rabin: MIT Tech. Rep. 212 (1979).
30 W. T. Sung and M. H. Tsai: Comput. Math. Appl. **64** (2012) 1450.
31 Y. Zhang, W. Liu, and Y. Fang: IEEE Military Communications Conf. (2005).
32 S. D. T. Kelly, N. K. Suryadevara, and S. C. Mukhopadhyay: IEEE Sens. J. **13** (2013) 3846.
33 N. K. Suryadevara, S. C. Mukhopadhyay, S. D. T. Kelly, and S. P. S. Gill: IEEE/ASME Trans. Mechatron. **20** (2015) 564.