Received June 17, 2020, accepted June 29, 2020, date of publication July 6, 2020, date of current version July 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3007388

A Low Resource Consumption Clone Detection Method for Multi-Base Station Wireless Sensor Networks

CANREN TANG AND DEZHI HAN, (Member, IEEE)
School of Information Engineering, Shanghai Maritime University, Shanghai 200135, China
Corresponding author: Dezhi Han (dzhan@shmtu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61672338 and Grant 61873160.

ABSTRACT To make up the existing deficiencies of clone attack detection methods of wireless sensor networks, a low resource consumption clone detection method (MSCD) for multi-base station wireless sensor networks is proposed. MSCD has the following characteristics: (1) Running in each ring network with base station as the center and using nodes in non-hotspot area to complete clone attack detection, which reduces the effect of clone attack detection on the network lifetime; (2) Combine the head node rotation mechanism and the backup head node mechanism to ensure the energy balance of the network; (3) The ring head node path can find clone nodes that come from different local networks, which makes the MSCD method be suitable for the whole multi-base station network. Meanwhile, in the detection domain of the head node, local broadcast is used to ensure the encounter of legitimacy verification messages and witness nodes; (4) It is proved theoretically that the clone detection probability of MSCD can reach 1 when the witness is credible. The theoretical analysis and the simulation results show that the MSCD clone detection probability is still above 98% when the number of clone nodes accounts for 10% of the total number of nodes, and the network lifetime and storage requirements are significantly better than the existing similar methods.

INDEX TERMS Clone attacks, wireless sensor networks, network lifetime, multi-base station networks.

I. INTRODUCTION

Wireless sensor networks (WSNs) is a kind of multi-hop self-organizing network which combines a large number of distributed deployed sensor nodes together through wireless communication technology to collect, process and transmit the surrounding data to support the user's decision [1], [2]. WSNs are widely used for traffic monitoring, navigation, temperature sensing, water energy measurements, tracking transportation systems, security, disaster management, and other utilities [3]. There require a large number of sensors deployed in harsh environments, and lack effective physical protection. Attackers often take advantage of these characteristics of wireless sensor network to carry out some malicious attacks [4]. Clone attack is an attack mode that captures some nodes in the sensor network, decrypts the internal secret information, and then massive copies these nodes and redeploys them to the network [5]. Since these copied nodes have exactly the same key information as the captured nodes, such as cryptographic mechanism and node ID, they can be added to the network like legitimate nodes [3]. Attackers can carry out a variety of internal attacks like wormhole attack and selective forwarding attack through these illegal nodes [6]. Therefore, it is very important to find out a method that can effectively discover clone attack and reduce the consumption of network resources as much as possible.

Generally speaking, in order to increase the harmfulness of the attack, the attacker will not place the illegal nodes in their original position after obtaining the illegal nodes by copying the node information. Therefore, some nodes with the same ID but in different positions will appear in the network, which can play an important role in the detection of the clone attack. In the clone detection methods, a part of nodes are usually selected as witness nodes to store the IDs and position information of other nodes to detect whether there are clone nodes in the network [7]. Besides, detection methods also need to ensure that at least one witness node can receive the legitimacy verification message sent by the node to be verified [8], [9].

The associate editor coordinating the review of this manuscript and approving it for publication was Ghufran Ahmed.

On the other hand, due to the energy and storage space of sensors are limited to some extent, if the energy consumption of sensor nodes is too fast, the lifetime of the network will be shortened. Although the existing methods have made some improvements, the energy consumption and storage requirement are still at a high level. In addition, with the expansion of the current scale of wireless sensor networks, the distance between sensor nodes and base station keep increasing, resulting in high energy consumption of network because of the transmission of data. Moreover, nodes nearby the base station will shorten their lifetime due to frequent message transmission, so the multi-base station wireless sensor network divided by monitoring area appears [10]. If multi-base station wireless sensor networks use the same set of encryption and decryption method, the attacker can capture the nodes in one of the local network and deploy the cloned nodes in another network, so as to reduce the risk of detected. However, the current methods are not applicable to the clone detection of multi-base station wireless sensor network. Therefore, this paper proposes a low resource consumption clone detection method for multi-base station wireless sensor networks (MSCD).

The main features and contributions of MSCD are as follows:

(1) In MSCD, clone attack detection is extended from only applicable to single-base station network to multi-base station network. In each single-base station network, the legitimacy verification messages are transmitted along the head node path (The head node here is a node in the area elected to communicate with other areas). If the nodes with the same ID but different positions are found, the clone attack from the same network is reported to base station. In a multi-base station network, if the corresponding witness node cannot be matched, legitimacy verification messages will continue to be transmitted along the ring path consisting of head nodes until the detection information traverses all the head nodes of the witness area, and then report to the base station that the clone attack from another local network has been found.

(2) In MSCD, nodes in non-hot spots area are used for clone detection, which extends the life of the network. The head node rotation mechanism [11] is adopted to balance the energy consumption of the network, and the standby head node mechanism [12] is introduced to avoid the influence of single point failure on the detection method. Under the same conditions, the additional communication load of clone attack detection is less than that of similar methods.

(3) Theoretical analysis and simulation results show that under the premise of credible witness nodes, the clone detection probability of MSCD can theoretically reach 1. Even if the number of clone nodes accounts for 10% of the total number of nodes, the clone detection probability can still be maintained at 98% to 99%.

The rest of this paper is organized as follows. Section 2 introduces the previous scholar's researches. Section 3 describes the system model and assumptions. Section 4 introduces the content of MSCD method in detail. Then section 5 has carried on theory analysis of several aspects. Section 6 presents simulation results. Finally, it is a summary of the paper.

II. RELATED WORK

As one of the most harmful attacks on wireless sensor networks, clone attack has attracted the attention of many researchers. The detection methods can be divided into different categories according to their characteristics, among which distributed and centralized [13] is the most common classification.

A. CENTRALIZED APPROACH

In most centralized methods, the detected tasks are typically done by base stations or witness nodes in the center of the area, which store the identity information of the sensor nodes in the area. The advantage of the centralized methods is that the additional communication load of clone detection is small and the detection probability is high under ideal conditions. The shortcoming is that centralized detection methods will make around the center node energy consume quickly because of frequent transfer messages, which will lead to the network lifetime shortened. In addition, it is make the center node become the main attack target of the attacker. If the center node fails or compromises, it will have a great influence on the network [14].

Some researchers have made some improvements against the shortcomings of the centralized method. H. Choi proposed a detection method based on multiple trees [15]. First, each node generates a mutually exclusive subset, and then randomly determines multiple roots in the network and constructs its own subtree. Leaf nodes send their subset report to the parent node step by step. Finally, the root node submits the report to the base station, and the base station compares whether the subset has intersection to detect the clone attack. W. Naruephiphat proposed a region-based clustering detection method [16]. The central node is selected by the maximal neighbor node method, and the network is divided into multiple sub-regions. Each sub-region selects a witness node. The local detection is performed by the witness node. If there is no abnormality in each sub-area, the central node performs global detection to save energy consumption of the network.

B. DISTRIBUTED METHOD

Distributed methods usually select a subset of nodes as witness nodes, and these witness nodes are located at different positions on the network. The advantage is that the resource consumption of the entire network is relatively balanced, and the disadvantage is that the average energy consumption is relatively large. The distributed method can be subdivided into three types according to the way the witness node chooses, which are: (1) deterministic selection; (2) randomness selection; (3) semi-random selection.

The RED [9] is a typical method for deterministic selection of witnesses. Its witness node is obtained by the mapping

function of the source node ID so that nodes with the same ID will select the same witness node. The detection messages of RED can be sent to the witness nodes at a small cost during the detection process. However, if the attacker cracks the mapping function of select the witness node, the witness node of the entire network node is equivalent to being completely open to the attacker, and the attacker can easily launch various attacks.

In order to solve the above problems, the researchers proposed some methods for randomly selecting witnesses, such as the CDLR [17] method, the ERCD [18] method, and the LSCD [19] method. All three methods divide the network into multiple virtual rings, and randomly select witness nodes in these rings. In the ERCD method, each node has a circular witness path in the corresponding witness ring. The detection messages are broadcast in the witness ring and its neighbor rings to ensure that the witness nodes can receive the messages. However, the ERCD method requires each source node to generate a complete witness path in the witness ring, which may result in greater energy consumption. The LSCD method generates a fixed length witness arc in the corresponding witness ring, and can dynamically adjust the number of centrifugal detection paths according to the length of the witness arc to ensure that the detection messages meet the witness arc. The shortcoming of the LSCD method is that each detection starts from the second ring, which will result in excessive energy consumption of the second ring and shorten the life of the network. The CDLR method enables the witness node to receive the legitimacy verification messages through broadcast in witness ring, but when the node density is large, a lot of energy consumption will be generated.

The semi-random method attempts to combine the advantages of the randomness method with the deterministic method. P-MPC [20] is a typical semi-random method. The method determines an area based on the mapping function and then randomly selects the witness in the area. Since the witness node is selected in two steps, the energy consumption and time complexity of the method are higher than deterministic.

To sum up, the work of predecessors has greatly improved the detection probability of clone attacks, but the general problem is that energy consumption is high, resulting in a decrease in network lifetime, and most of them are not applicable to multi-base station networks. This paper designing a distributed clone detection method with random witness selection through the head node path, not only effectively improves the detection probability, but the network communication load and the storage requirements is lower than similar methods. Meanwhile, the method is suitable for multi-base station networks.

III. SYSTEM MODEL AND ASSUMPTIONS

This section describes the system model and assumptions used in this paper. The system model includes the network model and the attacker model.

A. NETWORK MODEL

In MSCD, the network model consists of multiple local networks, and the base station is located at the center of each local network. It is assumed that the base station is sufficiently secure and will not be damaged by attackers [21]. The sensors in the network are densely and evenly distributed around the base station. The collected data by sensors is periodically transmitted to the base station, and the density of nodes is ρ. It is assumed that each local network is divided into h concentric virtual rings, which is recorded as 1 to h according to the distance to the base station. The width of each ring is equal to the communication radius r of the sensor nodes, and there are enough nodes in each ring to build a head node path. since the node in the first m rings frequently transmits data to the base station, and needs to bear a high-intensity communication load, so the first m rings are divided into hotspot areas. The clone detection task is completed by the remaining h-m rings. Multiple local networks use the same set of identity-based encryption and decryption methods [22], and base stations can communicate with each other through data centers (DC).

In Fig.1, a multi-base station network model consisted of four single-base station networks of ABCD is shown, and each single-base station network performs clone detection separately. The base station is responsible for transmitting the collected data and the abnormal information to the data center DC. Fig. 2 is a model of a single-base station network, and each non-hotspot ring has a head node path.

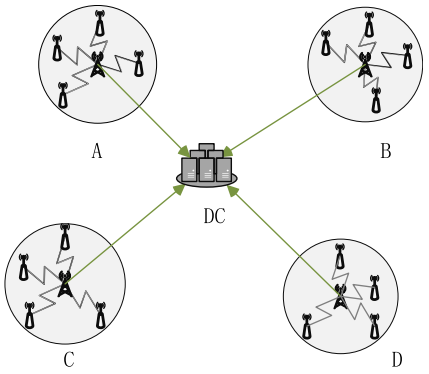

FIGURE 1. Multi-base station network model.

Each node has a unique ID for the entire multi-base station network. After the network deployment is complete, nodes with new IDs are no longer added. The sensor can obtain its own geographical location information and basic information of neighbor nodes through existing positioning methods [23]–[25]. The position of the base station it is known to all nodes. Each node has a certain amount of energy and storage space. In addition, the power supply cannot be replaced.

In order to prevent the attacker from attacking intensively on the head node and causing the position of the witness node to be exposed, the correspondence between the source node ID and the witness node is not saved in the head

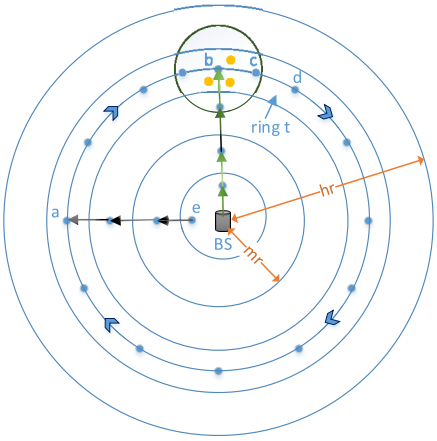

FIGURE 2. Single-base station network model.

node. At the same time, the backup head node mechanism [11] is introduced, and the backup head node is selected by calculating the ratio of energy to distance. When the head node is captured or fails, the standby head node assumes the task of the head node to ensure that the detection is not interrupted. The standby head node needs to be authenticated by the MSCD method to ensure that the clone node is not selected as the head node. In order to ensure the energy balance of the network, the head node rotation mechanism [12] is introduced so that the energy consumption of the same ring node is basically the same, which avoids shortening the network lifetime due to head node energy exhaustion. When the energy of the head node is lower than the threshold or after a period of time, the standby head node is changed to a new head node. The combination of these two mechanisms can ensure that the energy consumption of the head node is not quickly exhausted, thereby extending the lifetime of the network.

B. ATTACKER MODEL

After the network deployment is completed, attacker may launch a clone attack to obtain information collected by the network or interfere with the normal operation of the network. First, the attacker needs to capture some legitimate nodes and obtain key information including encryption and authentication methods. The attacker's ability to capture is limited and does not focus on capturing the nodes in the center of the area, because the centralized capture will cause the attack behavior to be easily discovered. Therefore, only a small number of sensor nodes in the network are randomly captured. Second, the attacker obtains a large number of cloned nodes by copying key information, but cannot create sensor nodes with new IDs. Next, the cloned node will be redeployed to the network and exchange information with the new neighbor nodes and update the adjacency list. At last, the attacker uses the clone node to launch various internal attacks to affect the normal operation of the sensor network while avoiding the exposure of the clone node as much as possible. In addition, if these clone nodes are selected as witness nodes, they will not respond to the verification request of the source node during the clone detection process.

Attacker can launch two different types of clone attacks. The first type is a local clone attack. The attacker re-delivers the copied node to the local network to which the captured node belongs. The methods of the predecessors are all proposed to solve this attack mode. The second type is a global clone attack. An attacker can capture a node of a local network and copy it to other local networks to reduce the detection probability of the algorithm. For example, in the network model shown in Fig. 1, an attacker can capture nodes in the network A and, after replication, deliver them to the network B, C, and D. Because the used encryption and decryption methods are consistent, and nodes of the same ID may not exist in the same local network, general clone detection method cannot effectively detect such global clone attacks.

TABLE 1. Symbol and significance.

Symbol	Significance
h	number of rings in a local network
t	ring mark
r	sensor communication radius
R	radius of the local network
m	the ring number of hotspot area
B_x, B_y	base station coordinates
L_{ix}, B_{iy}	coordinates of sensor node i
S_n	number of local network nodes
ρ	node density
D	average degree
$f_{1,2,3,4,5}$	message frequency
$W_{1,2,3,4,5}$	message size
θ	threshold of detection table
$C^t_{1,2,3,4}$	communication load
k	time-to-live
T_n	number of head node in ring n
T_{max}	maximum number of messages a node can send

IV. MSCD METHOD

A. METHOD OVERVIEW

MSCD is a distributed low resource consumption clone attack detection method that is suitable for multi-base station networks. It mainly includes the following three parts:

(1) Establishing the head node path: in the MSCD network model, the ring m+1 to the ring h are defined as non-hotspot areas. The base station sends a message to each ring of the non-hotspot area about starting to establish path, and the first node that receives the message in each ring is the first head node. In this paper, the detection range of each head node is called the detection domain, and the nodes in the ring determine the detection domain to which they belong according to the distance to the head node.

(2) Witness selection: after the head node path is established, each node determines a ring in non-hotspot area as

witness ring according to the hash function F (ID, h-m), and sends a witness selection message to the witness ring. Starting from the first node that receives the witness selection message and forwarding k times along the head node path, two nodes are randomly selected in the detection domain of the current head node as the witness node to store the witness information carried by the witness selection message. We call this node that sends the witness selection message the source node of the witness node.

(3) Legitimacy verification: The source node needs to perform legality verification before sending the message, except the message of establishing the head node path and the message of witness selection [18]. In the legality verification process, the legitimacy verification message is also forwarded along the head node path of the witness ring. If a head node finds that there is a witness node of the source node in its detection domain, it stops forwarding along the path and locally broadcasts the legitimacy verification message in its own detection domain to verify the legality of the source node. Particularly, if the legitimacy verification message traverses all the head nodes in the witness ring and still does not match the witness node, then there are considered clone nodes from other local networks.

B. ESTABLISHING THE HEAD NODE PATH

After the network deployment is completed, any sensor node i can obtain its own geographical position (L_{ix},L_{iy}) through the existing positioning algorithm and exchange ID and position information with the neighbor node to establish an adjacency list. The node can determine the ring mark L =D_{iB}/r by the ratio of the Euclidean distance D_{iB} to the base station and the radius r of each ring, the expression of D_{iB} is as follows:

$$D_{iB} = \sqrt{(L_{ix} - B_x)^2 + (L_{iy} - B_y)^2}$$

Above expression, (B_x, B_y) is the coordinate of the base station. The message that establishe a path along the ring is forwarded from the base station to the outer ring until the message is delivered to the ring h. When any node of the non-hotspot ring receives a message of establishing a ring path, that is, as the first head node of the ring, and then select the farthest node in the adjacency list as the second head node. The path direction (clockwise or counterclockwise) can be determined by the selection of the first two head nodes. Next, select the node with the longest projection on the extension line of the first two head nodes from the neighbor node of the second head node as the third head node. The node with the longest projection is selected repeatedly as the next-hop node until the first node appears again in the selection range of next-hop node, then mark the first head node as the next hop node to form a circular path.

In Fig.2, when node b in the non-hotspot ring t receives the message, it is the first head node of the ring. Then, the node c farthest from b is selected from the neighbor node of the same ring of b as the second head node, so it can be determined that the direction of the ring is clockwise. Next, node d becomes the third head node as the node with the longest projection on the extension line bc. Continue to select the next hop node on the extension line of the line segment until node b appears again in the selection range of the head node. Take b as the next hop node and finally the head node path in the ring is established.

In Fig.3, three possible circumstances of head node selection are shown. Part1 is a normal circumstance, and the black node is the node within the communication range of head node b. The longest projection on the extension line of ab is L_1, so c is taken as the next hop head node. Parts 2 and 3 are two unusual circumstances that require a new selection of the head node. The node c with the longest projection within the communication range of b in part2 is located above b. If c is used as the next hop node, the path will be set up in reverse. In part3, no node with positive projection exists within the communication range of b, the next hop head node need to be determined by the path of other rings.

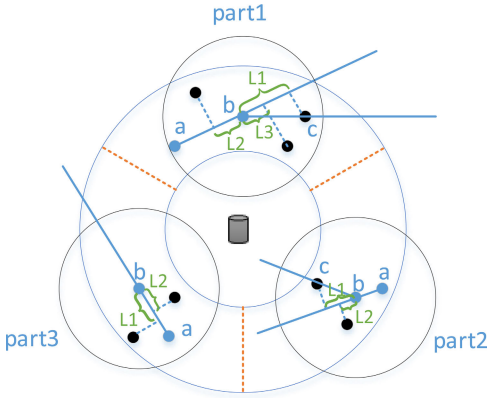

FIGURE 3. Head node selection.

In the path establishment process, the head node broadcasts its own identity information within the communication range. After receiving the identity information of the head node, the ordinary node selects the closest head node in the same ring and applies to join the detection domain of the head node. The head node saves the ID and position information of the node in the detection domain.

C. WITNESS SELECTION

After the path of the head node has been established, it is necessary to select the corresponding witness node for each node in the network. For each node, a hash function can determine a non-hotspot ring as a witness ring according to its ID, and then select two witness nodes in the detection domain of a head node of the witness ring.

Depending on the location of the witness ring, the witness selection messages from source node can be sent in three ways: centrifugal, centripetal, and forwarded in the current ring. Particularly, if the source node selects a witness in the ring in which it is located. In order to interfere with the attacker's judgment, it is necessary to give the witness selection message a time-to-live k, and then forward the witness

selection message along the head node path in the current ring, and k is a randomly generated integer. When the head node receives the witness selection message with the time-to-live, it checks whether the time-to-live of the message is greater than 0. If it is greater than 0, the time-to-live is decremented by 1 and then forwarded to the next hop head node. If the head node finds that the time-to-live of the witness selection message is 0, two nodes are randomly selected in itself detection domain to store witness information. The witness information includes the ID of the source node and position information.

As shown in Fig. 4, S_1 indicates that the witness node is in the inner ring of the source node;S_2 indicates that the source node is in the same ring as its corresponding witness, and node a endows the witness selection message with the time-to-live of k, and then forwards along the path of the head node. After the witness selection message reaches the head node b, the time-to-live is 0, and in the detection domain of b, two nodes W_1 and W_2 are randomly selected as the witness nodes of the node a; S_3 indicates that the witness selection message is being forwarded along the path of the head node; S_4 indicates that the witness node is in the outer ring of the source node.

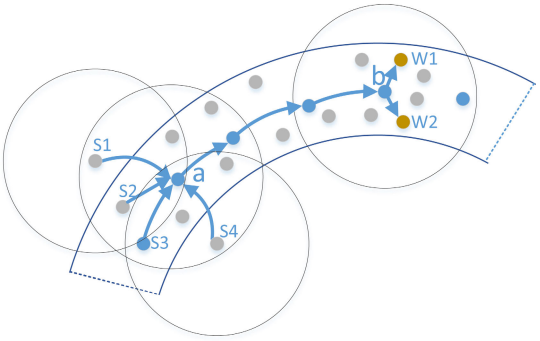

FIGURE 4. Witness selection.

In order to avoid information disclosure and more convenient to complete the detection, the detection table of the head node only stores the ID of source node of all witness nodes in the detection domain, and does not store the corresponding relationship between the ID of source node and witness node. If the number of IDs in the detection table of the head node is greater than the threshold θ, a new head node is added between the head node and its next hop head node. The detection domain and the detection table information of the head node are updated to make the witness information in the detection domain be consistent with the detection table. In section 5, we give the specific process of evenly increasing the head node.

D. LEGITIMACY VERIFICATION

Each node needs to perform legitimacy verification before sending a message, except the message of establishing the head node path and the message of witness selection. The legitimacy verification message contains the current ID and position information of the source node. In order to prevent the clone node from forging its own position, the head node of the source node should check the correctness of the coordinates when forwarding the message.

In the process of clone node detection of single-base station network, the position of witness ring is also obtained by hash function, and then the legitimacy verification message is forwarded to witness ring. After the head node in the witness ring receives the detection message, it firstly needs to check whether the ID is included in its own detection table. If the ID is not included in the detection table, it will continue to forward the message along the head node path. Otherwise, the detection message will be broadcasted in the detection domain so that the witness node can receive the detection message, and then the consistency between the detection message and the witness information stored by the witness node will be compared. If not consistent, the clone node will be reported to the base station; if consistent, the node security will be reported to the head node. The path e→a→b in Fig. 2 is a simple legitimacy verification process. The detection domain of head node b contains the witness of node e, so after receiving the legitimacy verification message, b will broadcast the message in its detection domain to make the witness node complete the detection.

In the process of legitimacy verification of the multi-base station network, if the detection message returns to the head node of the first received message again, it means that there is no witness node of the source node in the ring, and the head node reports to the base station that a clone attack from other local network is found.

V. THEORETICAL PERFORMANCE ANALYSIS

This section will conduct theoretical analysis on MSCD through several commonly used indicators, such as detection probability, communication load, network lifetime and storage requirements, and provide the corresponding proof process. Since MSCD method is applied to each local network independently, this paper only analyzes the theoretical performance of local network.

A. DETECTION PROBABILITY ANALYSIS

The detection probability in this paper refers to the probability that the detection message of the source node meets its witness node and successfully detected a clone attack.

Theorem 1: If the witness node is credible, the clone detection probability is 1.

Proof: as can be seen from Section IV, the legitimacy verification message sent by the source node must contain its real position information. Otherwise, the head node will detect the abnormality and directly detect the cloned node.

In the MSCD method, all source nodes have two witness nodes in the corresponding witness ring. The detection message is sent along the head node path to the head node where the witness node is located, and then the head node performs local broadcast in its detection domain, which can ensure that the witness node and the detection message must meet each

other. Therefore, under the condition that the witness node is credible, the clone detection probability is 1.

B. COMMUNICATION LOAD

For ease of analysis, this paper assumes that all message sizes are the same. At the same time, during the execution of the method, the number of messages sent and received is also the same. Therefore, the communication load and network lifetime in this section are analyzed only by the number of messages sent. In addition, because of the random forwarding of messages and the head node rotation mechanism, it can be considered that the communication load of nodes in the same ring is basically the same.

Theorem 2: The communication load C_1^t of the head node path establishment process is represented by the formula (1).

$$C_1^t = \frac{T_n w_1 f_1 + T_n \times \pi r^2 \rho w_2 f_2}{\pi\,(2t-1)\,r^2\rho} \tag{1}$$

Proof: C_1^t consists of the communication load of head node selection and the communication load of establishing detection domain. Assuming the node density in the network is ρ. w_1, f_1 respectively represent the size and frequency of the messages of head node selection. We first calculate the number of nodes of the entire network, which is $S_n = \pi(hr)^2\rho$. Therefore, the number of nodes in the ring t can be expressed by formula (2).

$$\pi(tr)^2\rho - \pi\,((t-1)\,r)^2\,\rho = \pi\,(2t-1)\,r^2\rho \tag{2}$$

θ is the threshold of storage source node IDs in the detection table. When the ID in the detection table is larger than θ, it is necessary to evenly increase the number of head nodes, We call the path without adding other head nodes as the initial path. Since the head node of the initial path is determined according to the longest projection, for the convenience of calculation, it is assumed that the distance between the head nodes is r, and the initial path length T_l of the ring t is approximately equal to the circumference of the outer circle of the ring t, that is, $T_l = 2\pi tr$. Therefore, the number of head nodes of the initial path is $T_l/r = 2\pi t$. The total number of head nodes of the ring t can be expressed by equation (3).

This paper gives a method of evenly increasing the head node: on the line segment formed by a certain head node t_i of the initial path and its next hop head node t_{i+1}, calculate the d bisector coordinates of the line segment, and then among the neighbor nodes of t_i, the node closest to the bisector coordinate is selected as the new head node, where d-1 is the number of head nodes that need to be added between t_i and t_{i+1}.

$$T_n = \begin{cases} 2\pi t & \dfrac{S_n}{\theta(h-m)} \le 2\pi t \\ \left\lceil \dfrac{S_n}{\theta(h-m)} \right\rceil & \dfrac{S_n}{\theta(h-m)} > 2\pi t \end{cases} \tag{3}$$

The total communication number of the head node selection is equal to the number of head nodes T_n, so the total communication load of the head node selection in the ring t is $T_n w_1 f_1$. Then the head node broadcasts its own coordinates to its $\pi r^2\rho$ neighbor nodes, and the communication load for establishing the detection domain is $T_n \times \pi r^2 \rho w_2 f_2$, where w_2, f_2 is the size and frequency of the broadcast messages. In summary, the communication load of the head node path establishment process can be expressed by formula (1).

Theorem 3: The communication load of witness node selection C_2^t can be expressed by formula (4), as shown at the bottom of the page.

Proof: set w_3 and f_3 as the size and frequency of the witness selection messages. For nodes in the hotspot ring t, only the witness selection messages of the inner ring and the same ring need to be sent to the outer ring. Therefore, the node average communication load of the ring t can be expressed by the formula (5).

$$\frac{\pi\,(tr)^2\,\rho w_3 f_3}{\pi\,(2t-1)\,r^2\rho} = \frac{t^2 w_3 f_3}{2t-1} \tag{5}$$

For the non-hotspot ring t, it is necessary to bear the 1/(h-m) detection task, and naturally there is a 1/(h-m) node looking for the witness node in the ring t. We first discuss the average communication load of witness messages forwarded in the ring t. After the witness messages arrives at the non-hotspot ring, it is forwarded k times along the path of the head node and then the witness messages is randomly forwarded to the two nodes in the detection domain of the head node. Therefore, the average communication load of the witness messages forwarded in the ring t is represented by the formula (6).

$$\frac{1}{h-m} \times \frac{\pi(hr)^2\rho(k+2)w_3 f_3}{\pi\,(2t-1)\,r^2\rho} = \frac{h^2(k+2)w_3 f_3}{(h-m)\,(2t-1)} \tag{6}$$

$$C_2^t = \begin{cases} \dfrac{t^2 w_3 f_3}{2t-1} & t \le m \\ \dfrac{(h^2\,(k+2) + (h-m-1)\,t^2) w_3 f_3}{(h-m)\,(2t-1)} & t = m+1 \\ \dfrac{\left(h^2\,(k+2) + (h-t)\,(t-1)^2 + (t-m-1)\left(h^2 - t^2\right) + (h-m-1)\right) w_3 f_3}{(h-m)\,(2t-1)} & m+1 < t < h \\ \dfrac{h^2(k+2) w_3 f_3}{(h-m)\,(2t-1)} + \dfrac{(h-m-1)\,w_3 f_3}{h-m} & t = h \end{cases} \tag{4}$$

Next we will analyze the average communication load of the witness messages transferred between the rings. According to the location of the node, three cases can be considered.

(1) The node is located in the ring m+1. The (h-m-1)/(h-m) witness selection messages of the current ring and its inner ring needs to be forwarded to the outer ring. The average communication load in this case can be expressed by formula (7).

$$\frac{h-m-1}{h-m}\times\frac{\pi(\mathrm{tr})^2\rho w_3 f_3}{\pi\,(2t-1)\,r^2\rho}=\frac{(h-m-1)t^2 w_3 f_3}{(\mathrm{h}-\mathrm{m})(2t-1)} \tag{7}$$

(2) The node is located in the ring h. The (h-m-1)/(h-m) witness selection messages of the ring h needs to be forwarded to the inner ring. The average communication load in this case can be expressed by formula (8).

$$\frac{h-m-1}{h-m}\times\frac{\pi\,(2t-1)\,r^2\rho w_3 f_3}{\pi\,(2t-1)\,r^2\rho}=\frac{(h-m-1)w_3 f_3}{h-m} \tag{8}$$

(3) The node is between the ring m+1 and the ring h. The (h-t)/(h-m) witness selection messages of its inner ring need to be forwarded to outer ring, the (t-m-1)/(h-m) witness selection messages of its outer ring need to be forwarded to inner ring and the (h-m-1)/(h-m) witness selection messages of its same ring need to be forwarded to other hotspot ring. The average communication load in this case can be expressed by formula (9).

$$\frac{((h-t)\,(t-1)^2+(t-m-1)\left(h^2-t^2\right)+(h-m-1))w_3 f_3}{(\mathrm{h}-\mathrm{m})(2t-1)} \tag{9}$$

Therefore, C_2^t can be expressed by formula (4).

Theorem 4: The communication load C_3^t in the legality verification phase can be expressed by the formula (10), as shown at the bottom of the page.

Proof: let w_4,f_4 denote the size and frequency of legality verification message. Each detection task can be divided into two parts in the non-hotspot ring. The first part is that the detection message forward k times along the path of the head node to find the head node. The communication load of this part is kw_4f_4. The second part is to broadcast the detection message in the detection domain. The average number of nodes in the detection domain of each head node is $(\pi\,(2t-1)\,r^2\rho)/T_n$, and the communication load of this part is $(\pi\,(2t-1)\,r^2\rho w_4 f_4)/T_n$, so the average communication load of each node after the detection message reaches the non-hotspot ring t can be expressed by the formula (11).

$$\frac{S_n(k+\frac{\pi(2t-1)r^2\rho}{T_n})w_4f_4}{(h-m)\,\pi\,(2t-1)\,r^2\rho} \tag{11}$$

The communication load process of message passing between rings is similar to formula (4), and the proof is not repeated.

Theorem 5: The communication load C_4^t of the node located on the ring t transmitting the collected data to the base station can be expressed by the formula (12).

$$C_4^t=\frac{(h^2-(t-1)^2)w_5 f_5}{2t-1} \tag{12}$$

Proof: let w_5, f_5 denote the size and frequency of data message. After collecting the data, the sensor node transmits to the base station in a multi-hop manner. The node located in the ring t needs to transmit the data collected by its outer ring and the same ring to base station. Therefore,C_4^t can be expressed by formula (12). □

Fig.5 shows that the average communication load of the three methods varies with the number of hotspot rings m, and m takes 1, 2 and 3 respectively to get three curves. Obviously, for the MSCD method, the average communication load of the first ring is the most. This is because the first ring undertakes the task of transmitting all the data in the network to the base station. Naturally, the communication load of the first ring also becomes the restriction of the whole network lifetime. If the first ring also needs to perform clone detection task, it will inevitably lead to increased energy consumption, which also reflects the necessity of dividing hotspots. At the same time, it can be observed that under the same conditions of other parameters, the average communication load of the MSCD method is lower than the CDLR method and the ERCD method. The main reason is that the MSCD method has less communication load in the legality verification stage than the other two methods. The CDLR method uses a form of

$$C_3^t=\begin{cases}\dfrac{t^2w_4f_4}{2t-1} & \mathrm{t}<\mathrm{m}\\[2ex] \dfrac{S_n(k+\frac{\pi\,(2t-1)\,r^2\rho}{T_n})w_4f_4}{(h-m)\,\pi\,(2t-1)\,r^2\rho}+\dfrac{(\mathrm{h}-\mathrm{m}-1)\,t^2w_4f_4}{(h-m)\,(2t-1)} & \mathrm{t}=\mathrm{m}{+}1\\[2ex] \dfrac{S_n(k+\frac{\pi\,(2t-1)\,r^2\rho}{T_n})w_4f_4}{(h-m)\,\pi\,(2t-1)\,r^2\rho}+\dfrac{\left((h-t)\,(t-1)^2+(t-m-1)\left(h^2-t^2\right)+(h-m-1)\right)w_4f_4}{(\mathrm{h}-\mathrm{m})\,(2t-1)} & \mathrm{m}{+}1<t<h\\[2ex] \dfrac{S_n(k+\frac{\pi\,(2t-1)\,r^2\rho}{T_n})w_4f_4}{(h-m)\,\pi\,(2t-1)\,r^2\rho}+\dfrac{(h-m-1)\,w_4f_4}{h-m} & \mathrm{t}=\mathrm{h}\end{cases} \tag{10}$$

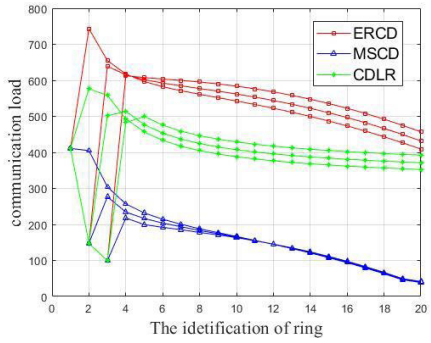

FIGURE 5. The comparison of communication load of three methods (h=20, f4=10).

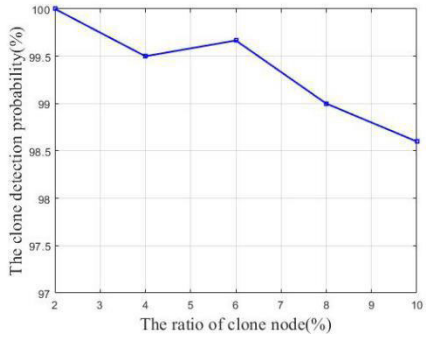

FIGURE 6. Clone detection probability (h = 20, f4 = 10).

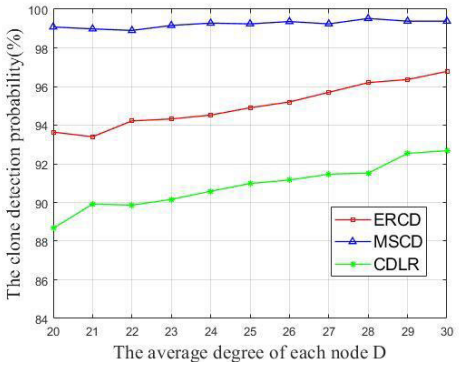

FIGURE 7. The comparison of detection probability of three methods with different D (h = 20, f4 = 10).

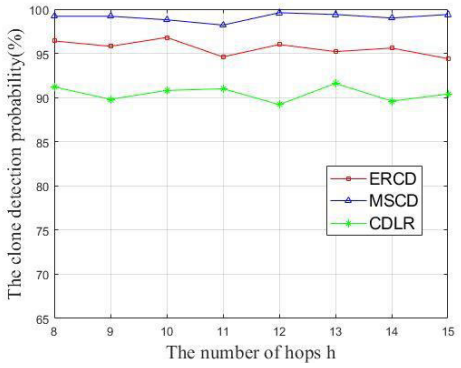

FIGURE 8. The comparison of detection probability of three methods with different h (f4 = 10).

three-ring broadcast to find witness nodes, while the ERCD method needs to broadcast messages throughout the witness ring, so the energy consumption of these two methods is greater.

C. NETWORK LIFETIME

Network lifetime is another major measure of sensor network performance. If the energy of any node in the network is exhausted, the network lifetime is considered to be over. In order to reduce the difficulty of network lifetime assessment, we assume that the messages sent by the nodes are the same size, and the maximum number of messages that can be sent by each node is T_{max}. When the number of messages sent by the node reaches T_{max}, the node energy is considered exhausted.

According to section V, the average communication load C^t of the ring t is $C^t = C_1^t + C_2^t + C_3^t + C_4^t$. Therefore, the network lifetime TL_{MSCD} can be expressed by formula (13).

$$TL_{MSCD} = \frac{T_{max}}{\max(C^t)} 1 \le t \le h \tag{13}$$

D. STORAGE REQUIREMENT

Theorem 6: The storage requirements of each node using MSCD are O(θ).

Proof: in the MSCD method, the storage requirements of the head node are the largest, mainly including the witness information and the detection table. The total number of witness information in a local network is $2\pi\,(hr)^2\,\rho$, and the number of nodes from the ring m+1 to the ring h is $\pi(h^2 - m^2)r^2\rho$. Therefore, the cost of storing witness information for each node can be expressed by formula (14).

$$\frac{2\pi\,(hr)^2\,\rho}{\pi(h^2 - m^2)r^2\rho} = \frac{2h^2}{h^2 - m^2} \tag{14}$$

It can be known from formula (14) that the number of stored witness node information of each node is related to the total number of rings h and the number of hotspot rings m, independent of the number of nodes in the network and the density. At the same time, since the number of hotspots is relatively small compared to the total number of rings in the network, it can be approximated that the storage requirement for storing witness information is a constant level. Moreover, since the maximum capacity of the detection table in the head node does not exceed the threshold θ, the storage requirements of each node are O(θ).

VI. SIMULATIONS

This section will continue to evaluate the performance of the MSCD method through simulations, and the performance comparison with related methods is achieved using matlab under the same parameter values. Similarly, a local network is used as a unit for performance evaluation. We placed 4,000 sensors evenly in a ring network with a radius of 800m.

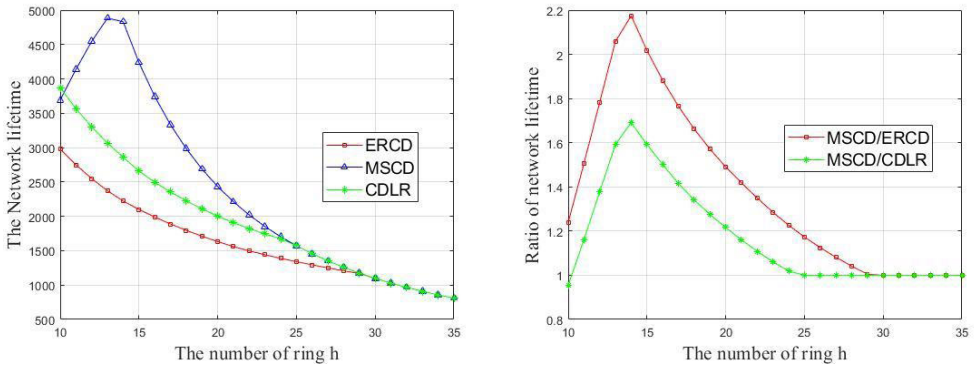

FIGURE 9. The comparison of network lifetime of three methods with different h (f4 = 10).

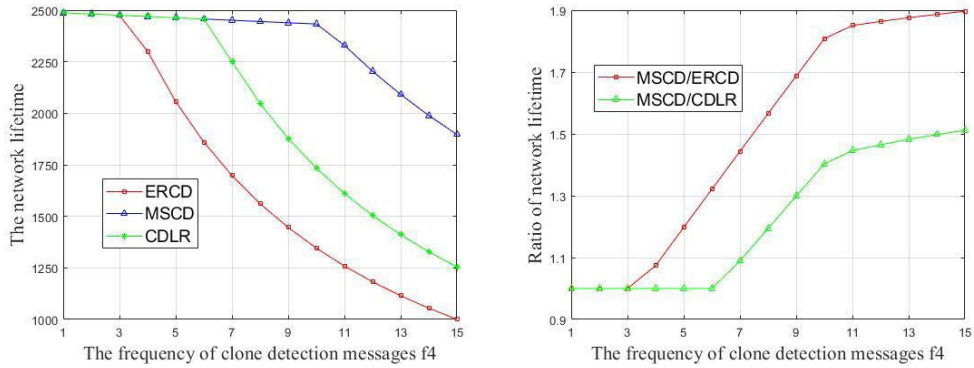

FIGURE 10. The comparison of network lifetime of three methods with different f_4(h = 20).

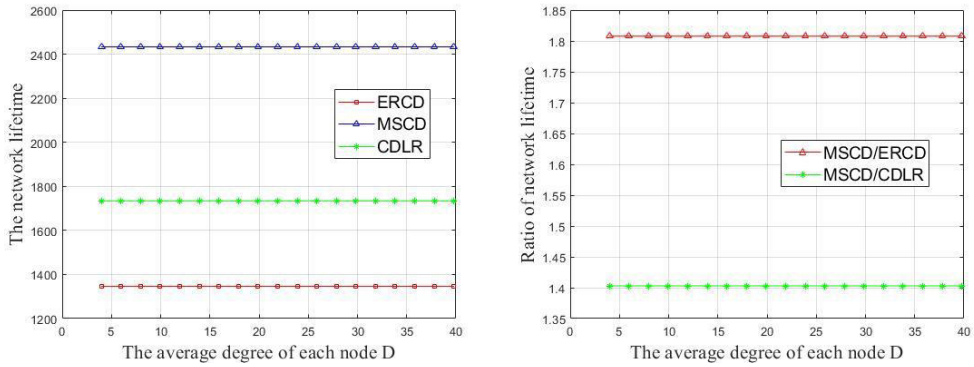

FIGURE 11. The comparison of network lifetime of three methods with different D (h = 20, f4 = 10).

The base station is located in the center of the network. The communication radius of each sensor is 40m. The network is divided into 20 virtual rings. The width of each ring is 40m, and the number m of hotspot rings is set to 1 to 3 according to the energy consumption. In these simulations, the frequency of head node path establishment, witness selection and data collection is set same that is $f_1 = f_2 = f_3 = f_5 = 1$. The clone detection frequency f_4 can be freely set depending on the demand. In the simulation in this section, a general energy consumption model is used [18], which gives the energy consumption calculation method for message sending and receiving. The values of some parameters of the model are given in Table 2.

In Section V, we demonstrate that the clone detection probability of MSCD can reach 1 when the witness node is trusted. However, some of the witness nodes are captured by the attacker, which may lead to the failure of the clone detection. As shown in Fig.6, even when the number of cloned nodes is set to 2%-10%, the detection probability of the MSCD method is reduced from 100% to 98.6%. it remains at a high

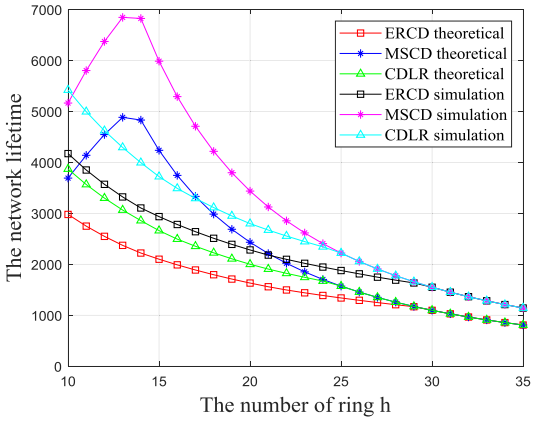

FIGURE 12. The Comparison of theoretical and simulation network lifetimes under different h.

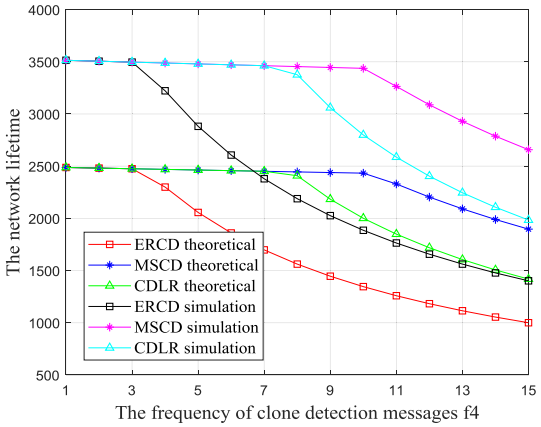

FIGURE 13. The Comparison of theoretical and simulation network lifetimes under different f4.

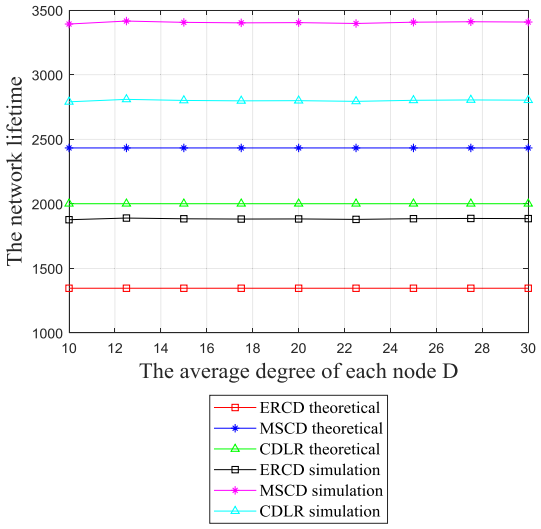

FIGURE 14. The Comparison of theoretical and simulation network lifetimes under different D.

level because the probability of two witnesses at the source node being compromised at the same time is extremely low.

The detection probability of MSCD, ERCD and CDLR with the average node degree is shown in Fig.7. The average node degree refers to the number of neighbor nodes of the node. In the simulation of this paper, the node degree is between 20 and 30, and the number of clone nodes is fixed. It can be seen that the variation range of the MSCD method is the smallest. This is because each source node of the MSCD has two witness nodes in the detection domain of the corresponding head node. When the average node degree reduces and the number of clone nodes is fixed, the MSCD method still has a higher probability of detecting the clone node. The ERCD method and the CDLR method are significantly reduced. This is because the degree of node reduction is reduced, which reduces the success rate of the three-ring broadcast of the ERCD method. In addition, the proportion of cloned nodes in the CDLR method directly determines the probability of successful clone detection.

Set the number of clone nodes to 10% of the total number of normal nodes. It can be seen in Fig. 8 that when the number of rings of the network changes from 8 to 15, the detection probability of the three methods remain basically unchanged, maintaining 99%, 96% and 92% respectively, and MSCD still has the highest detection probability.

Next, we test the impact of the three methods on the network lifetime by changing the number of network rings h and the detection frequency f_4. We first reflect the changing trend of network lifetime through changes in the number of messages. It is assumed here that the size of each message is 1 bit, that is, $w_1 = w_2 = w_3 = w_4 = w_5 = 1$ bit, and the maximum number of transmitted messages T_{max} is 1 million. In other similar methods, the test method of changing a single parameter is mostly adopted, but the change of the number of rings h is not considered to affect the optimal number of hotspots, so that the highest average energy consumption of each ring is not an optimal solution. Therefore, we will consider the effects of h and m at the same time. For each network ring number h, determine the optimal number of hotspots when m is taken from 1 to 3, and then calculate the highest energy consumption of each ring.

As can be seen in Fig. 9, the network lifetime of MSCD is at most 2.2 times higher than ERCD and 1.7 times higher than CDLR. When the total number of rings in the network is small, the detection tasks undertaken by the rings of the MSCD method are the main causes of energy consumption. As the number of rings increases but the total number of nodes in the network does not change, the number of detection tasks undertaken by each ring in the MSCD method decreases, and the data transmission from the first ring node to the base station becomes the most energy consuming part, and the energy consumption of the first ring node become a bottleneck restricting network lifetime. It can be seen from Fig. 10 that the energy consumption of the first ring is the bottleneck of the entire network when the number of clone detections is not higher 3 times. After the number of detections is more than 3 times, the energy consumption of the non-hotspot ring becomes a new life bottleneck. The CDLR method detects

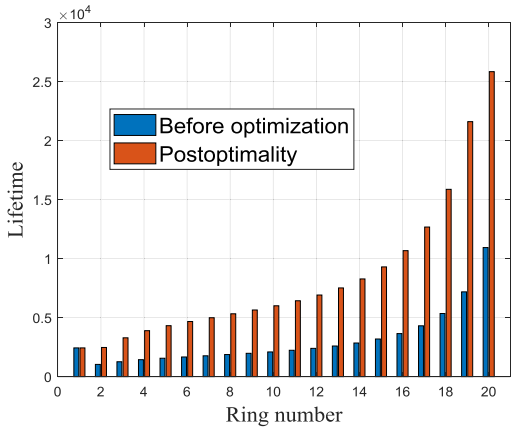

FIGURE 15. Energy optimization effect comparison.

TABLE 2. Parameters and values.

Parameters	Values
h	20
r	40 m
R	800 m
m	1-3
S_n	4000
k	1
f_4	10
$W_{1,2,3,4,5}$	100 byte
$f_{1,2,3,5}$	1
T_{max}	1000000
E_e	5 ×10-8J/bit
E	120J
ε_{fs}	1 ×10-11J/(bit • m^2)
ε_{amp}	1.3 ×10-15J/(bit • m^4)

more than 6 times, forming a new life bottleneck. The number of detections by the MSCD method is more than 10 times, and the network lifetime is obviously changed.

It can be found from Fig.11 that the network lifetimes of the three methods basically do not change with the change of D, and under the same conditions, the network lifetime of the MSCD method is 1.8 times that of ERCD and 1.4 times that of CDLR. A separate theoretical analysis cannot truly reflect the performance of a method, so we use a general energy consumption model to evaluate the performance of the MSCD method.

Formula (15) gives the energy consumption expression for two nodes with distance d to send μ bit data. When the distance d between the receiving and sending nodes is less than the distance threshold d_0, the free space path loss model is used, and when d is greater than d_0 the multi-path fading model is used. Here ε_{fs} and ε_{amp} respectively represent the energy consumed by the two models of the power amplifier, and E_e represents the energy consumed when receiving 1 bit data.

$$E_r = \begin{cases} \mu E_e + \mu \varepsilon_{fs} d^2 & d < d_0 \\ \mu E_e + \mu \varepsilon_{amp} d^4 & d > d_0 \end{cases} \quad (15)$$

We put the energy model into the derivation of section V to calculate the real energy consumption of the nodes, and then simulate the real network lifetime of the sensor network. At this time, the message size is set to 100 byte, and the initial energy of the sensor node E is set to 120 J. Figure 12-14 is the comparison between the theoretical network lifetime and the simulate network lifetime, which further verifies the rationality of the algorithm. Fig.15 shows the energy optimization effect after using the simplified head node rotation mechanism. The results show that the introduction of the head node rotation mechanism can effectively extend the network lifetime.

Through the comparison of the above parameters, it can be seen that the performance of MSCD is better than that of CDLR and ERCD.

VII. CONCLUSION AND FUTURE WORK

In this paper, we propose a clone detection method suitable for multi-base station networks (MSCD), which mainly includes three processes: head node path establishment, witness selection and legality verification. In the MSCD, running in each ring network with base station as the center and using nodes in non-hotspot area to complete clone attack detection, which reduces the effect of clone attack detection on the network lifetime; combine the head node rotation mechanism and the backup head node mechanism to ensure the energy balance of the network; the ring head node path can find clone nodes that come from different local networks, which makes the MSCD method be suitable for the whole multi-base station network. Further theoretical analysis and simulations prove that the proposed method has better performance in most aspects and the additional cost is less than similar methods.

In the next work, we will continue to study efficient clone detection methods under different network models. For example, the network model in this paper assumes that the sensor nodes in the network do not need to sleep, and are always in working state. In fact, the sensor nodes usually use the sleep mode to save their own energy consumption, and how to ensure the detection probability of the method when some nodes are in the dormant state, which will be the focus of the next study. At the same time, both the MSCD method and the similar method assume that the nodes are evenly distributed in the network, but due to the influence of the environment, the node distribution is not necessarily uniform, which may affect the detection probability of the clone detection method. So we will try to make some improvements in these parts.

REFERENCES

[1] A. Jarwan, A. Sabbah, and M. Ibnkahla, "Data transmission reduction schemes in WSNs for efficient IoT systems," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 6, pp. 1307–1324, Jun. 2019.

[2] Y. Zhang, S. He, and J. Chen, "Data gathering optimization by dynamic sensing and routing in rechargeable sensor networks," in *Proc. IEEE Int. Conf. Sens., Commun. Netw. (SECON)*, New Orleans, LA, USA, Jun. 2013, pp. 273–281.

[3] R. Grewal, J. Kaur, and K. S. Saini, "A survey on proficient techniques to mitigate clone attack in wireless sensor networks," in *Proc. IEEE Int. Advance Comput. Conf. (IACC)*, Jun. 2015, pp. 1148–1152.
[4] M. Sharma, A. Tandon, S. Narayan, and B. Bhushan, "Classification and analysis of security attacks in WSNs and IEEE 802.15.4 standards: A survey," in *Proc. 3rd Int. Conf. Adv. Comput., Commun. Autom. (ICACCA) (Fall)*, Sep. 2017, pp. 1–5.
[5] K. Cho, M. Jo, T. Kwon, H.-H. Chen, and D. H. Lee, "Classification and experimental analysis for clone detection approaches in wireless sensor networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 26–35, Mar. 2013.
[6] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 677–691, Jun. 2010.
[7] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Compressed sensing-based clone identification in sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3071–3084, Apr. 2016.
[8] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy (S&Amp;P05)*, Oakland, CA, USA, May 2005, pp. 49–63.
[9] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 5, pp. 685–698, Sep. 2011.
[10] Z. Zhiping, S. Nannan, and Z. Xuebo, "A novel authentication protocol for mobile nodes in multi-base-station wireless sensor network," in *Proc. Int. Conf. Inf. Netw. Secur. (ICINS)*, Beijing, China, 2014, pp. 52–59.
[11] D. Lin and Q. Wang, "An energy-efficient clustering algorithm combined game theory and Dual-Cluster-Head mechanism for WSNs," *IEEE Access*, vol. 7, pp. 49894–49905, 2019.
[12] S. Murugaanandam and V. Ganapathy, "Reliability-based cluster head selection methodology using fuzzy logic for performance improvement in WSNs," *IEEE Access*, vol. 7, pp. 87357–87368, 2019.
[13] A. Lal and J. Selvakumar, "Secure low-storage clone detection technique for wireless sensor networks," in *Proc. Int. Conf. Electron., Commun. Aerosp. Technol. (ICECA)*, Coimbatore, India, Apr. 2017, pp. 669–672.
[14] S. V. Autkar, M. R. Dhage, and S. P. Bholane, "A survey on distributed techniques for detection of node clones in wireless sensor networks," in *Proc. Int. Conf. Pervas. Comput. (ICPC)*, Pune, India, Jan. 2015, pp. 1–4.
[15] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in *Proc. 3rd Int. Conf. Secur. Privacy Commun. Netw. Workshops (SecureComm)*, Nice, France, 2007, pp. 341–350.
[16] W. Naruephiphat, Y. Ji, and C. Charnsripinyo, "An area-based approach for node replica detection in wireless sensor networks," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Liverpool, U.K., Jun. 2012, pp. 745–750.
[17] Z. Zhang, S. Luo, H. Zhu, and Y. Xin, "A clone detection algorithm with low resource expenditure for wireless sensor networks," *J. Sensors*, vol. 2018, Mar. 2018, Art. no. 4396381.
[18] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "Energy and memory efficient clone detection in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 5, pp. 1130–1143, May 2016.
[19] M. Dong, K. Ota, L. T. Yang, A. Liu, and M. Guo, "LSCD: A low-storage clone detection protocol for cyber-physical systems," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 35, no. 5, pp. 712–723, May 2016.
[20] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, pp. 913–926, Jul. 2010.
[21] J. Ren, Y. Zhang, K. Zhang, A. Liu, J. Chen, and X. S. Shen, "Lifetime and energy hole evolution analysis in data-gathering wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 12, no. 2, pp. 788–800, Apr. 2016.
[22] Z. Li and G. Gong, "On the node clone detection in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 6, pp. 1799–1811, Dec. 2013.
[23] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," *IEEE Pers. Commun.*, vol. 7, no. 5, pp. 28–34, Oct. 2000.
[24] P. R. Gautam, S. Kumar, A. Verma, T. Rashid, and A. Kumar, "Energy-efficient localization of sensor nodes in WSNs using beacons from rotating directional antenna," *IEEE Trans. Ind. Informat.*, vol. 15, no. 11, pp. 5827–5836, Nov. 2019.
[25] L. Lazos and R. Poovendran, "SeRLoc: Robust localization for wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 1, no. 1, pp. 73–100, 2005.
[26] T. Bonaci, P. Lee, L. Bushnell, and R. Poovendran, "Distributed clone detection in wireless sensor networks: An optimization approach," in *Proc. IEEE Int. Symp. World Wireless, Mobile Multimedia Netw.*, Lucca, Italy, Jun. 2011, pp. 1–6.

CANREN TANG is currently pursuing the M.S. degree with the School of Information Engineering, Shanghai Maritime University, Shanghai, China. Her current research interests include cryptology, cloud computing security, and network security.

DEZHI HAN (Member, IEEE) received the B.S. degree in applied physics from the Hefei University of Technology, China, in 1990, and the M.S. and Ph.D. degrees in computing science from the Huazhong University of Science and Technology, China, in 2001 and 2005, respectively. He has been a Professor with the Department of Computer, Shanghai Maritime University, China, since 2010. His research interests include cloud and outsourcing security, wireless communication security, and network and information security.