Energy and Memory Efficient Clone Detection in Wireless Sensor Networks

Zhongming Zheng, *Student Member, IEEE*, Anfeng Liu, *Member, IEEE*, Lin X. Cai, *Member, IEEE*, Zhigang Chen, *Member, IEEE*, and Xuemin (Sherman) Shen, *Fellow, IEEE*

Abstract—In this paper, we propose an energy-efficient location-aware clone detection protocol in densely deployed WSNs, which can guarantee successful clone attack detection and maintain satisfactory network lifetime. Specifically, we exploit the location information of sensors and randomly select witnesses located in a ring area to verify the legitimacy of sensors and to report detected clone attacks. The ring structure facilitates energy-efficient data forwarding along the path towards the witnesses and the sink. We theoretically prove that the proposed protocol can achieve 100 percent clone detection probability with trustful witnesses. We further extend the work by studying the clone detection performance with untrustful witnesses and show that the clone detection probability still approaches 98 percent when 10 percent of witnesses are compromised. Moreover, in most existing clone detection protocols with random witness selection scheme, the required buffer storage of sensors is usually dependent on the node density, i.e., $O(\sqrt{n})$, while in our proposed protocol, the required buffer storage of sensors is independent of n but a function of the hop length of the network radius h, i.e., $O(h)$. Extensive simulations demonstrate that our proposed protocol can achieve long network lifetime by effectively distributing the traffic load across the network.

Index Terms—Wireless sensor networks, clone detection protocol, energy efficiency, network lifetime

1 Introduction

Wireless sensors have been widely deployed for a variety of applications, ranging from environment monitoring to telemedicine and objects tracking, etc. [2], [3], [4]. For cost-effective sensor placement, sensors are usually not tamper-proof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks [5], [6], [7], [8], [9]. For example, a malicious user may compromise some sensors and acquire their private information. Then, it can duplicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks [10], which is referred to as the clone attack [11], [12], [13]. As the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors, they can easily participate in network operations and launch attacks. Due to the low cost for sensor duplication and deployment, clone attacks have become one of the most critical security issues in WSNs. Thus, it is essential to effectively detect clone attacks in order to ensure healthy operation of WSNs.

To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the location information, is shared with witnesses at the stage of witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if the node fails the certification. To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses should be randomly selected; and 2) at least one of the witnesses can successfully receive all the verification message(s) for clone detection [11]. The first requirement is to make it difficult for malicious users eavesdrop the communication between current source node and its witnesses, so that malicious users cannot generate duplicate verification messages. The second requirement is to make sure that at least one of the witnesses can check the identity of the sensor nodes to determine whether there is a clone attack or not. To guarantee a high clone detection probability, i.e., the probability that clone attacks can be successfully detected, it is critical and challenging to fulfill these requirements in clone detection protocol design.

Different from wireless terminal devices, wireless sensors are usually of smaller size and lower price, and have limited battery and memory capacity. Therefore, the design criteria of clone detection protocols for sensor networks should not only guarantee the high performance of clone detection probability but also consider the energy and memory efficiency of sensors. In the literature, some distributed clone detection protocols have been proposed, such as Randomized Efficient and Distributed protocol (RED) [10] and Line-Select Multicast protocol (LSM) [11]. However, most approaches mainly focus on improving clone detection probability without considering efficiency and balance of energy

- *Z. Zheng and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1. E-mail: {z25zheng, sshen}@uwaterloo.ca.*
- *A. Liu and Z. Chen are with the School of Information Science and Engineering, Central South University, Changsha, China 410083. E-mail: {afengliu, czg}@mail.csu.edu.cn.*
- *L. X. Cai is with the Illinois Institute of Technology, Chicago, IL 60616. E-mail: lincai@iit.edu.*

Manuscript received 8 May 2014; revised 2 Apr. 2015; accepted 16 June 2015. Date of publication 25 June 2015; date of current version 31 Mar. 2016. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TMC.2015.2449847

consumption in WSNs. With such kind of approaches, some sensors may use up their batteries due to the unbalanced energy consumption, and dead sensors may cause network partition, which may further affect the normal operation of WSNs. To prolong network lifetime, i.e., time duration from the start of network until the first occurrence of a sensor that runs out of energy, it is critical to not only minimize the energy consumption of each node but also balance the energy consumption among sensors distributively located in different areas of WSNs. The limited memory or data buffer is another important feature of sensors which has significant impact on the design of clone detection protocols. Generally, to guarantee successful clone detection, witnesses need to record source nodes' private information and certify the legitimacy of sensors based on the stored private information. In most existing clone detection protocols, the required buffer storage size depends on the network node density, i.e., sensors need a large buffer to record the exchanged information among sensors in a high-density WSN, and thus the required buffer size scales with the network node density. Such requirement makes the existing protocols not so suitable for densely-deployed WSNs. Most existing approaches can improve the successful clone detection at the expense of energy consumption and memory storage, which may not be suitable for some sensor networks with limited energy resource and memory storage.

In this paper, besides the clone detection probability, we also consider energy consumption and memory storage in the design of clone detection protocol, i.e., an energy- and memory-efficient distributed clone detection protocol with random witness selection scheme in WSNs. Our protocol is applicable to general densely deployed multi-hop WSNs, where adversaries may compromise and clone sensor nodes to launch attacks. A preliminary work is presented in [1]. In that work, we proposed an energy-efficient ring based clone detection (ERCD) protocol to achieve high clone detection probability with random witness selection, while ensuring normal network operations with satisfactory network lifetime of WSNs. The ERCD protocol can be divided into two stages: witness selection and legitimacy verification. In witness selection, the source node sends its private information to a set of witnesses, which are randomly selected by the mapping function. In the legitimacy verification, verification message along the private information of the source node is transmitted to its witnesses. If any of witnesses successfully receives the message, it will forward the message to its witness header for verification. Upon receive the messages, the witness header compares the aggregated verification messages with stored records. If multiple copies of verification messages are received, the clone attack is detected and a revocation procedure will be triggered. As such, to have a comprehensive study of the ERCD protocol, we extend the analytical model by evaluating the required data buffer of ERCD protocol and by including experimental results to support our theoretical analysis. First, we theoretically prove that our proposed clone detection protocol can achieve probability 1 based on trustful witnesses. Considering the scenario that witnesses can be compromised, our simulation results demonstrate that the clone detection probability can still approach 98 percent in WSNs with 10 percent cloned nodes by using the ERCD protocol. Second, to evaluate the performance of network lifetime, we derive the expression of total energy consumption, and then compare our protocol with existing clone detection protocols. We find that the ERCD protocol can balance the energy consumption of sensors at different locations by distributing the witnesses all over WSNs except non-witness rings, i.e., the adjacent rings around the sink, which should not have witnesses. After that, we obtain the optimal number of non-witness rings based on the function of energy consumption. Finally, we derive the expression of the required data buffer by using ERCD protocol, and show that our proposed protocol is scalable because the required buffer storage is dependent on the ring size only. Extensive simulation results demonstrate that our proposed ERCD protocol can achieve superior performance in terms of the clone detection probability and network lifetime with reasonable data buffer capacity.

We present the remainder of this paper as follows. We summarize the previous works of clone detection protocols in Section 2. In Section 3, the system model and problem statement are introduced. The ERCD protocol is proposed in Section 4. Then, we analyze the performance of the ERCD protocol in terms of clone detection probability, network lifetime and data buffer storage in Section 5. Experiment results are presented in Section 6, followed by the conclusion in Section 7.

2 Related Work

As one of the utmost important security issues, clone attack has attracted people's attention. There are many works [14], [15], [16] that studies clone detection protocols in the literature, which can be classified into two different categories, i.e., centralized and distributed clone detection protocols. In centralized protocols, the sink or witnesses generally locate in the center of each region, and store the private information of sensors. When the sink or witnesses receive the private information of the source node, they can determine whether there is a clone attack by comparing the private information with its pre-stored records [17], [18]. Normally, centralized clone detection protocols have low overhead and running complexity. However, the security of sensors' private information may not be guaranteed, because the malicious users can eavesdrop the transmission between the sink node and sensors. Moreover, the network lifetime may be dramatically decreased since the sensor nodes close to the sink will deplete their energy sooner than other nodes.

Different from centralized protocols, in distributed clone detection protocols, a set of witnesses are selected to match with every sensor [10], [11], which prevents the transmission between the sink and sensors from being eavesdropped by malicious users. There are three different types of witness selection schemes in distributed clone detection protocols: i) deterministic selection, ii) random selection, and iii) semi-random selection. The deterministic witness selection based clone detection protocols like RED [10] choose the same set of witnesses for all sensor nodes. By using deterministic witness selection, a low communication overhead and a high clone detection probability can be achieved. In addition, the required buffer storage capacity of such protocols is very low, which is only related to the number of witnesses without considering network scale and node

density. Nevertheless, due to the deterministic characteristic, the mapping function can be easily obtained and a variety of attacks may be launched by malicious users. To enhance the network security, the distributed clone detection protocols with random witness selection [11], [12] like LSM are proposed, which are closely related to our work. In random witness selection, it is difficult for malicious users to acquire the information of witnesses since the witnesses of each sensor are randomly generated. However, the randomness of mapping function also increases the difficulty for the source node to reach its witnesses, which makes it challenging to achieve a high clone detection probability. To ensure the clone detection probability, LSM lets all the nodes in the route between source and witnesses store the private information of the source node, which leads to a high requirement of data buffer and energy consumption. Thus, it is essential to guarantee the clone detection probability with low energy consumption and required buffer storage in clone detection protocols with random witness selection approach. Other distributed clone detection protocols, such as Parallel Multiple Probabilistic Cells (P-MPC), proposed semi-random witness selection approach [13], [19], trying to combine the advantages of both random and deterministic witness selection approaches. In this kind of witness selection scheme, a deterministic region is generated for the source node according to the mapping function, and then witnesses of the source node will be randomly selected from the sensors in this region. However, the two-phases witness selection and randomness of the witnesses for each sensor leads to a high overhead and time complexity. The energy consumption and the required buffer storage of such protocols are lower than the random witness selection approach but higher than the deterministic ones. Overall, most previous works aim at maximizing the clone detection probability without considering the impact of proposed clone detection protocol on the network lifetime and required data buffer storage. In this paper, we carefully design a distributed clone detection protocol with random witness selection by jointly considering the clone detection probability, network lifetime and data buffer capacity.

3 System Model and Problem Statement

In this work, we consider a network region with one base station (BS) and an enormous number of wireless sensor nodes randomly distributed in the network. We use the sink node as the origin of the system coordinator. Based on the location of the BS, the network region is virtually separated into adjacent rings, where the width of each ring is the same as the transmission range of sensor nodes. The network is a densely deployed WSN, i.e., i) for each node, there exist sensor nodes located in each neighboring ring, and ii) for each ring, in each ring, there are enough sensor nodes to construct a routing path along the ring. The network model can be simply extended into the case of multiple BSs, where different BSs use orthogonal frequency-division multiple access (OFDMA) to communication with its sensor nodes. For each sensor, it has to accomplish the tasks of data collection as well as clone detection. In every data collecting cycle, sensors send the collected data to the sink node through multi-hop paths. To be capable of conducting legitimacy verification, every sensor has the same buffer storage capacity to store the information. Buffer storage capacity should be sufficient to store the private information of source nodes, such that any node can be selected as a witness. When the buffer storage of the sensor node is full, the oldest information will be dropped to accept the latest incoming information.

In our network, the link level security can be guaranteed by employing a conventional bootstrapping cryptography scheme, and the sink node uses a powerful cryptography scheme, which cannot be compromised by malicious users. A key pair (a, b) is assigned to each node, where a and b are the node ID and secret key, respectively. All nodes share their ID information with other nodes in the network. If either side of the link is compromised by malicious users, the link key is compromised. Each sensor node knows the physical information and the relative locations of its neighbors, where the relative location refers to the hop distance between a sensor node and the sink, and the hop distance can be obtained by a breadth-first search. At first, the sink node broadcasts the message, which notifies the receivers that the message comes from index 0. All nodes, which receive the message, will update their ring index to 1 and rebroadcast the message to their neighbors. Each node will update the ring index only when the message has a lower ring index than that it received in previous transmissions. The above procedure repeats until all the nodes broadcast the message and record their ring indexes. A malicious user has the capability to compromise a set of sensor nodes located at arbitrary locations. Utilizing the private information of compromised nodes, a large number of cloned nodes can be generated and deployed into the network by the malicious user [10], [11]. However, we suppose that malicious users cannot compromise the majority of sensor nodes, since no protocol can successfully detect the clone attack with little legitimate sensor nodes [10], [11], [20].

Energy consumption model in [4], [21], [22] is used in this paper. Let $\mathcal{E}_{fs}$ and $\mathcal{E}_{amp}$ denote the energy required by power amplification in free space model and multi-path fading model, respectively. We can obtain the energy consumption, E_t, to transmit ℓ-bit packet over distance $\mathcal{D}$ in multi-path fading and free space channels as follows,

$$E_t = \begin{cases} \ell E_c + \ell \mathcal{E}_{fs} \mathcal{D}^2, & \text{if } \mathcal{D} < \mathcal{D}_0 \\ \ell E_c + \ell \mathcal{E}_{amp} \mathcal{D}^4, & \text{if } \mathcal{D} > \mathcal{D}_0, \end{cases} \tag{1}$$

where E_c and $\mathcal{D}_0$ denote the energy loss per bit and the distance threshold for channel models, respectively. The required energy for receiving and decode the ℓ-bit packet is

$$E_r(\ell) = \ell E_c. \tag{2}$$

In this paper, we focus on designing a distributed clone detection protocol with random witness selection by jointly considering clone detection probability, network lifetime and data buffer storage. Initially, a small set of nodes are compromised by the malicious users. Utilizing the clone detection protocol, we aim at maximizing the clone detection probability, i.e., the probability that cloned node can be successfully detected, to ensure the security of WSNs; meanwhile, the sufficient energy and buffer storage capacity for data collection and operating clone detection protocol should be guaranteed, which means that the network

TABLE 1
Notation List

h	The hop number of network radius
h_a	The hop length from a to the sink
n	The number of nodes in the network
n_i	The number of nodes in i-th ring
r	The transmission range of a node
O_a	The ring index of a
O_a^w	The witness ring index of a
W_a	The set of a's witness
w_a	One of a's witness in W_a
S_a	The witness header of W_a
ID_a	The identity information of a
l_a	The location a claims to occupy
τ_a	The timer of a's verification
K_a	The message including a's private information

lifetime, i.e., the period from the start of network operation until the first outage occurs [21], [22], should not be impacted by the proposed clone detection protocol with sensors' buffer storage. Overall, our objective is to propose a distributed clone detection protocol with random witness selection in order to maximize the clone detection probability while the negative impact of network lifetime and the requirement of data buffer storage should be minimized.

4 ERCD Protocol

In this section, we introduce our distributed clone detection protocol, namely ERCD protocol, which can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity. The ERCD protocol consists of two stages: witness selection and legitimacy verification. In witness selection, a random mapping function is employed to help each source node randomly select its witnesses. In the legitimacy verification, a verification request is sent from the source node to its witnesses, which contains the private information of the source node. If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification, where witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses. If the received messages are different from existing record or the messages are expired, the witness header will report a clone attack to the sink to trigger a revocation procedure.

Initially, network region is virtually divided into h adjacent rings, where each ring has a sufficiently large number of sensor nodes to forward along the ring and the width of each ring is r. To simplify the description, we use hop length to represent the minimal number of hops in the paper. Since we consider a densely deployed WSN, hop length of the network is the quotient of the distance from the sink to the sensor at the border of network region over the transmission range of each sensor, i.e., the distance of each hop refers to the transmission range of sensor nodes. Table 1 shows the mathematical symbols utilized in this section.

The ERCD protocol starts with a breadth-first search by the sink node to initiate the ring index, and all neighboring

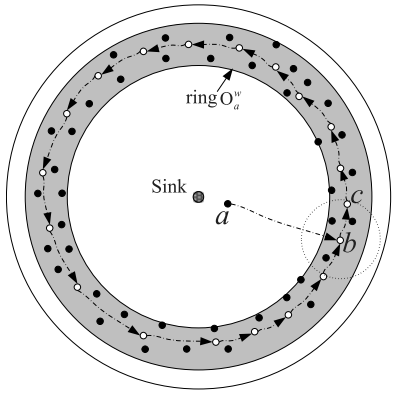


Fig. 1. Ring structure of witnesses.

sensors periodically exchange the relative location and ID information [23], [24]. After that, whenever a sensor node establishes a data transmission to others, it has to run the ERCD protocol, i.e., witness selection and legitimacy verification, to verify its legitimacy. In witness selection, a ring index is randomly selected by the mapping function as the witness ring of node a. To help relieve the traffic load in hot spot, the area around the sink cannot be selected by the mapping function. After that, node a sends its private information to the node located in witness ring, and then the node forwards the information along the witness ring to form a ring structure. In the legitimacy verification, a verification message of the source node is forwarded to its witnesses. The ring index of node a, denoted O_a, is compared with its witness ring index O_a^w to determine the next forwarding node. If $O_a^w > O_a$, the message will be forwarded to any node located in ring $O_a + 1$; otherwise, the message will be forwarded to any node in ring $O_a - 1$. This step can forward the message toward the witness ring of node a. The ERCD protocol repeats above operations until a node, denoted b, located in the witness ring O_a^w is reached. Node b stores the private information of node a and forwards the message to any node located in ring O_a^w within its transmission range, denoted as c. Then, node c stores the information and forwards the message to the node d, where link (c, d) has longest projection on the extension line of the directional link from b to c. The procedure will be repeated until node b reappears in the transmission range. Therefore, the witnesses of node a have a ring structure, consisting of $b, c, ...b$ as shown in Fig. 1.

In the legitimacy verification, node a sends a verification message including its private information following the same path towards the witness ring as in witness selection. To enhance the probability that witnesses can successfully receive the verification message for clone detection, the message will be broadcast when it is very close to the witness ring, namely three-ring broadcasts, i.e., the message will be broadcast in $O_a^w - 1$, O_a^w and $O_a^w + 1$ as shown in Fig. 2. In Theorem 1, we prove that the three-ring broadcasts can ensure the network security, i.e., the clone detection probability is one, under the assumption that all witnesses are trustful. To determine whether there exists a clone attack or not, all the verification messages received by witnesses are forwarded to the witness header along the same route in witness selection. The sensor nodes in the transmission route but not located in the witness ring are called the transmitters.

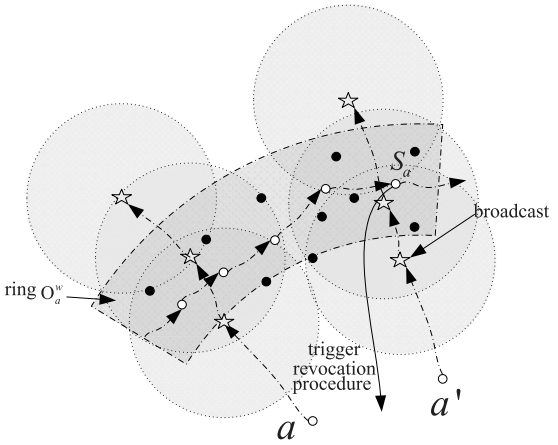


Fig. 2. Legitimacy verification.

The witness header of the source node a, denoted by S_a, is a sensor located in witness ring O_a^w, meanwhile it is also in the communication range of the transmitter located in ring index $O_a^w - 1$ or $O_a^w + 1$. The witness header S_a is randomly selected by the transmitter in the neighboring witness ring, i.e., the ring of $O_a^w - 1$ or $O_a^w + 1$. If more than one copies or incorrect copies or expired copies are received by the witness header, the ERCD protocol will trigger a revocation procedure; if no copy is received from the source node due to packet loss or silent cloned node, transmissions from the source node will not be permitted.

An example is shown in Fig. 2. Let a and a' denote the source node and one cloned node. The verification messages of both a and a' are broadcast in ring $O_a^w - 1$, O_a^w and $O_a^w + 1$. After that, both messages are received by the witness header S_a, and a revocation procedure is triggered. We describe the detail of the ERCD protocol in Algorithm 1.

In addition to the normal operations, the recovery mechanism is very easy to be established based on ERCD protocol. For the case when the clone detection fails due to outage or clone attack, another clone detection cycle will be initiated and the source node will randomly choose a new route and forward the message en route to a new witness header.

5 Performance Analysis

In this section, the performance of the ERCD protocol is evaluated in terms of clone detection probability, power consumption, network lifetime, and data buffer capacity. At first, we prove that the clone detection probability of the ERCD protocol can almost surely achieve probability 1 under the scenario that witnesses are trustful in Section 5.1. After that, we derive the expression of energy consumption and network lifetime by using ERCD protocol, and obtain the ratio of network lifetime by using ERCD protocol over RED or LSM protocol in Section 5.2. Finally, the required data buffer of the ERCD protocol is derived in Section 5.3.

5.1 Probability of Clone Detection

In distributed clone detection protocol with random witness selection, the clone detection probability generally refers to whether witnesses can successfully receive the verification message from the source node or not. Thus, the clone detection probability of ERCD protocol is the probability that the verification message can be successfully transmitted from the source node to its witnesses. In ERCD protocol, the verification message is broadcast when it is near the witness ring, i.e., in the rings of $O_a^w - 1$, O_a^w and $O_a^w + 1$, to guarantee the network security. With such kind of method and assumption of trustful witnesses, we can prove that at least one of the witnesses can receive the message, i.e., the clone attack can be detected with probability one. To simplify the analysis, the transmission ranges of all sensor nodes, r, are the same.

Algorithm 1. Energy-efficient Ring based Clone Detection Protocol

Initialize the ring index of each sensor node;
Exchange the relative information with neighbors;
STAGE I: Witness selection
$K_a \leftarrow$ Encrypt(ID_a, l_a, τ_a);
$O_a^w \leftarrow PseudoRand(ID_a, l_a, \tau_a, h_a)$; $i \leftarrow O_a$;
while $i \neq O_a^w$ **do**
  if $i < O_a^w$ **then**
    $a' \leftarrow$ randomly selected node on $(i+1)$-th ring;
    $i \leftarrow i + 1$;
  else
    $a' \leftarrow$ randomly selected node on $(i-1)$-th ring;
    $i \leftarrow i - 1$;
  end if
  Forward K_a to a';
end while
$b \leftarrow$ a randomly selected node on O_a^w-th ring;
Let b record (ID_a, l_a, τ_a) from K_a; $W_a \leftarrow b$;
$c \leftarrow$ a randomly selected node on O_a^w-th ring;
while $c \neq b$ **do**
  Let c record (ID_a, l_a, τ_a) from K_a; $W_a \leftarrow c$;
  $c \leftarrow$ the farthest node from c on O_a^w-th ring;
end while
STAGE II: Legitimacy Verification
$K_a \leftarrow$ Encrypt(ID_a, l_a);
$O_a^w \leftarrow PseudoRand(ID_a, l_a, h_a)$;
$j \leftarrow O_a$; $j' \leftarrow O_a$;
while $(j' < O_a^w \wedge j \neq O_a^w + 2) \vee (j' > O_a^w \wedge j \neq O_a^w - 2)$ **do**
  if $(j' < O_a^w) \wedge (j < O_a^w + 2)$ **then**
    $a'' \leftarrow$ next selected node in STAGE I on $(j+1)$-th ring;
    $j \leftarrow j + 1$;
  else if $(j' > O_a^w) \wedge (j > O_a^w - 2)$ **then**
    $a'' \leftarrow$ next selected node in STAGE I on $(j-1)$-th ring;
    $j \leftarrow j - 1$;
  end if
  if $(j = O_a^w - 1) \vee (j = O_a^w) \vee (j = O_a^w + 1)$ **then**
    Broadcast K_a;
  end if
end while
for all $w_i \in W_a$ **do**
  if w_i hears K_a **then**
    Forward K_a to S_a {S_a is b}
  end if
end for
if (ID_a, l_a) of $S_a \neq (ID_a, l_a)$ in $K_a \vee$ multiple copies $\vee$ time $> \tau_a$; **then**
    Trigger the revocation procedure;
end if

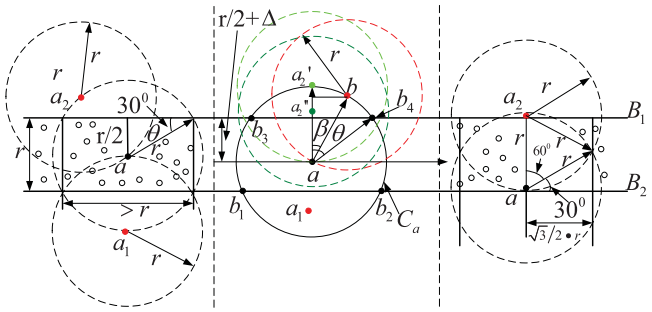


Fig. 3. Case study.

Theorem 1. *Given that the selected witnesses of node a are trustful, if there exist clones of node a, the cloned nodes can be detected with probability 1 in the legitimacy verification stage.*

Proof. We consider a large network area, and simplify the circular arc of ring O_a^w as a rectangular region as shown in Fig. 3. In order to prevent clone attacks, we have to ensure that at least one of the witnesses can be achieved to verify the legitimacy of the source node in each round of clone detection. In the ERCD protocol, witnesses are selected forming a ring structure in the ERCD protocol, and thus any two neighboring witnesses should be within the transmission ranges of each other. Considering that the width of each ring is r, we only need to ensure that the coverage of verification message on the witness ring arc is longer than r. Therefore, we focus on the proof that at least r of circular arc in ring O_a^w is covered by the three-ring broadcasts.

We denote the broadcast nodes of the verification message in rings $O_a^w - 1$, O_a^w and $O_a^w + 1$ by a_1, a_2 and a_3, respectively. B_1 and B_2 are the borderlines between $O_a^w + 1$, O_a^w and $O_a^w - 1$. Let Δ be the distance from the center point between B_1 and B_2 to node a_2. We separate the proof into three cases, i) a_2 locates at the center of ring O_a^w, i.e., $\Delta = 0$, ii) a_2 locates at the lower part of the ring O_a^w, and iii) a_2 locates at the upper part of the ring O_a^w. For the first case, the coverage of witness ring arc is longer than $\sqrt{3}r$, which is larger than r. For the second case, if δ approaches 0 as shown in Fig. 3c, the coverage of witness ring arc is $\sqrt{3}r$, which is larger than r. For the second case, if δ approaches 0 as shown in Fig. 3c, the coverage of witness ring arc is $\sqrt{3}r$, which is larger than r. Let C_{a_2} and C_{a_3} stand for the transmission ranges of node a_2 and a_3, respectively. $b1$, $b2$, $b3$ and $b4$ denote the intersections between B_1, B_2 and C_{a_2}, while b_5 and b_6 represent the intersections between C_{a_2} and C_{a_3}. It can be observed that the coverage of O_a^w by the node on the circular arc like a_3'' is smaller than that of the node inside C_{a_2}. Thus, we consider the worst case, i.e., a_3 is on the circular arc of C_{a_2}, to ensure the success of clone detection. To help proof the theorem, a coordinate system with a_2 as the original point is constructed, where x-axis is parallel to B_1 and B_2, and y-axis is perpendicular to B_1 and B_2. We use $i.x$ and $i.y$ to represent the coordinate of node i. To ensure that the coverage is larger than r of witness ring arc, following inequality should be hold:

$$\min(b_2.x, b_4.x, b_6.x) - \max(b_1.x, b_3.x, b_5.x) > r, \quad (3)$$

where $b_5.y < r/2$ and $b_6.y < r/2$. Let β denote the angle between the line (a_2, a_3) and y-axis, then we can obtain

$$\begin{cases} b_5.x = \frac{\frac{r\tan\beta}{2\cos\beta} - r\sqrt{\frac{\tan^2\beta}{4\cos^2\beta} - (1+\tan^2\beta)(\frac{1}{4\cos^2\beta} - 1)}}{1+\tan^2\beta} \\ b_6.x = \frac{\frac{r\tan\beta}{2\cos\beta} + r\sqrt{\frac{\tan^2\beta}{4\cos^2\beta} - (1+\tan^2\beta)(\frac{1}{4\cos^2\beta} - 1)}}{1+\tan^2\beta}. \end{cases} \quad (4)$$

Let θ denote the angle between the line (a_2, b_4) and y-axis, and $\theta = \arccos(\frac{r/2+\Delta}{r})$, $\beta \in (0, \theta)$. We can get

$$\begin{cases} b_1.x = -\sqrt{0.75r^2 - \Delta^2 + \Delta r} \\ b_2.x = \sqrt{0.75r^2 - \Delta^2 + \Delta r} \\ b_3.x = -\sqrt{0.75r^2 - \Delta^2 - \Delta r} \\ b_4.x = \sqrt{0.75r^2 - \Delta^2 - \Delta r}. \end{cases} \quad (5)$$

Combing Eq. (4) and Eq. (5), we can obtain the inequality 3, and thus the coverage area is longer than r of witness ring arc. For the third case, it is obviously that the coverage area is longer than r of witness ring arc. Therefore, at least one of the witnesses can successfully receive the verification messages from node a and cloned nodes. At last, all the received messages will be forwarded to the witness header to determine whether the node is cloned or not. □

5.2 Energy Consumption and Network Lifetime

In WSNs, since wireless sensor nodes are usually powered by batteries, it is critical to evaluate the energy consumption of sensor nodes and to ensure that normal network operations will not be broken down by node outage. Therefore, we define the network lifetime as the period from the start of network operation until any node outage occurs to evaluate the performance of the ERCD protocol. We only consider the transmission power consumption, as the reception power consumption occupies little percentage of total power consumption. Since witness sets in our ERCD protocol are generated based on ring structure, sensor nodes in the same ring have similar tasks. To simplify the analysis, we suppose that all sensor nodes in the same ring have same traffic load. Our analysis in this work is generic, which can be applied to various energy models. Let ε_1 and λ_1 denote the bit size of each collected data and the frequency of data collection, respectively. A node inside (outside) ring k refers to the node which locates in the ring with index smaller than (larger than) k.

First, we analyze the traffic load of each sensor node, such that the energy consumption and network lifetime can be derived based on it. By using the ERCD protocol, traffic load of each sensor node consists of normal data collection, witness selection and legitimacy verification. We can derive the expression for the traffic load of normal data collection as follows.

Theorem 2. *Let T_j and N_k denote the summation traffic load of normal data collection for all the sensor nodes in ring j and the number of nodes in ring k, respectively. The traffic load for data collection of each sensor in ring $k, k \in (1, h)$, can be expressed as*

$$d_k^c = \frac{\sum_{j=k}^{h} T_j}{N_k} = \frac{(h^2 - (k-1)^2)\lambda_1\varepsilon_1}{2k-1}. \quad (6)$$

Proof. In WSNs, the sink node aggregates the collected data of each sensor for analysis. Therefore, nodes in ring k should help to relay the traffic sent from nodes locate outside ring k. Let ρ and s_k denote the density of nodes and the area of ring k, respectively. We can obtain the number of nodes, which do not locate inside ring k, as

$$\begin{cases} s_k = \pi(kr)^2 - \pi((k-1)r)^2 = \pi(2k-1)r^2 \\ N_k = s_k\rho = \pi(2k-1)r^2\rho. \end{cases} \tag{7}$$

The total traffic load of data collection for nodes do not locate inside ring k is $\sum_{j=k}^{h} T_j$, is

$$\sum_{j=k}^{h} T_j = \rho\lambda_1\varepsilon_1 \sum_{j=k}^{h} s_j. \tag{8}$$

Then, the traffic load for data collection of each sensor can be obtained as shown in Eq. (6). □

Second, we calculate the traffic load for legitimacy verification by using ERCD protocol. ε_2 and λ_2 denote the bit size of each request message for verification and the frequency of legitimacy verification, respectively. In order to relieve the traffic burden in hot spot, the mapping function of ERCD protocol does not assign witnesses to the area around the BS. Let ϕ denote the amount of non-witness rings around the BS, i.e., there is no witness located inside the ring ϕ.

Theorem 3. *The traffic load of each sensor node for legitimacy verification in ring k, denoted d_k^v, is*

$$d_k^v = \begin{cases} \frac{k^2\varepsilon_2\lambda_2}{2k-1}, k \le \phi \\ \frac{[(h-k)(k-1)^2+(h^2-k^2)(k-\phi)+\pi kh^2]\varepsilon_2\lambda_2}{(h-\phi)(2k-1)} + \varepsilon_2\lambda_2, k > \phi. \end{cases} \tag{9}$$

Proof. We calculate the traffic load for legitimacy verification of each node according to the position of the node, i.e., whether the node is located outside ϕ or not. If the node does not locate outside ring ϕ, the traffic for legitimacy verification is transmitted from nodes inside ring k to nodes outside ring k, which is $\pi(kr)^2\rho\varepsilon_2\lambda_2$. As the number of sensor nodes in ring k is $N_k = \pi(2k-1)r^2\rho$, the traffic load for legitimacy verification of each node in ring $k, k < \phi$, can be expressed as

$$d_k^v = \frac{k^2\varepsilon_2\lambda_2}{2k-1}, k \le \phi. \tag{10}$$

If the node locates outside ring ϕ, the verification traffic load is composed of the traffic transmitted to the witness ring and the traffic forwarded to the witness header, $d_k^v = d_k^{v1} + d_k^{v2}$. The traffic transmitted to the witness ring can be further divided into three different cases: 1) traffic sent from nodes inside ring k to nodes outside ring k, 2) traffic sent by nodes in ring k, and 3) traffic sent from nodes outside ring k to nodes inside ring k. For the first case, $(h-k)/(h-\phi)$ of the traffic is sent to the nodes outside of ring k, and the traffic sent by the nodes inside ring k is $\pi((k-1)r)^2\rho\varepsilon_2\lambda_2$. Therefore, the traffic relayed by nodes in ring k for the first case is $\pi((k-1)r)^2 \rho\varepsilon_2\lambda_2(h-k)/(h-\phi)$. For the second case, the traffic sent by nodes in ring k is $\pi(2k-1)r^2\rho\varepsilon_2\lambda_2$. For the third case, the traffic can be calculated by the similar method in the first case, which is $\pi r^2(h^2-k^2)\rho\varepsilon_2\lambda_2(k-\phi)/(h-\phi)$. Thus, the verification traffic load by each node in ring $k > \phi$ to the witness ring can be expressed as

$$d_k^{v1} = \frac{\left[\frac{(h-k)(k-1)^2}{h-\phi} + \frac{(h^2-k^2)(k-\phi)}{h-\phi}\right]\varepsilon_2\lambda_2}{2k-1} + \varepsilon_2\lambda_2, k > \phi. \tag{11}$$

After that, we try to obtain the traffic load for forwarding verification to the witness header in the witness ring. We first calculate the verification traffic load of witness ring k, which is $\pi(hr)^2\rho\varepsilon_2\lambda_2/(h-\phi)$. As the verification is only forwarded along at most half of the circumference to reach the witness header, the hop length of the forwarding will not exceed πk. Based on the number of sensor nodes in ring k, $\pi(2k-1)r^2\rho$, the traffic load for forwarding verification to the witness header can be expressed as $d_k^{v2} = \pi kh^2\varepsilon_2\lambda_2/[(h-\phi)(2k-1)], k > \phi$. Overall, the traffic load of each sensor node for legitimacy verification can be expressed in Eq. (9). □

At last, we derive the expression of the traffic load for witness selection by using ERCD protocol. Let λ_3 stand for the frequency of witness selection.

Theorem 4. *The traffic load for witness selection of each node in ring k, denoted by d_k^w, can be expressed as*

$$d_k^w = \begin{cases} \frac{d_k^{v1}\lambda_3}{\lambda_2}, k \le \phi \\ \frac{d_k^{v1}\lambda_3}{\lambda_2} + \frac{2\pi kh^2\varepsilon_2\lambda_3}{(h-\phi)(2k-1)}, k > \phi. \end{cases} \tag{12}$$

Proof. By using ERCD protocol, the traffic load of clone detection consists of witness selection and legitimacy verification. In witness selection, there are two steps: 1) the private information of the source node is sent to its witness ring; and 2) the private information is forwarded along the witness ring to construct a ring structure; in legitimacy verification, there are also two steps: 1) the verification message is first sent to the witness ring of the source node, and 2) the message is forwarded to the witness header. We can observe that, for each witness selection and legitimacy verification, the traffic load by each sensor of first step is the same, i.e., d_k^{v1}. Thus, based on the frequency of witness selection and legitimacy verification, the traffic load by each sensor of first step in witness selection can be expressed as $d_k^{v1}\lambda_3/\lambda_2$. Then, we consider the cases according to the location of ring k and the value of ϕ for the second step in witness selection. If ring k does not locate outside ϕ, there is no witness in ring k and no traffic load of the second step in witness selection. The traffic load by each sensor located within ring k in witness selection is $d_k^{v1}\lambda_3/\lambda_2, k \le \phi$. If ring k locates outside ϕ, the ring k has probability of $1/(h-\phi)$ to be selected as a node's witness ring. The traffic load by each sensor located outside ring k in witness selection should be $2\pi k\lambda_3 n/(h-\phi)$, where $n = \pi h^2r^2\rho$.

Therefore, the traffic load for witness selection of each node in ring $k, k > \phi$ can be expressed as $d_k^{v1}\lambda_3/\lambda_2 + 2\pi kh^2\varepsilon_2\lambda_3/[(h-\phi)(2k-1)]$. □

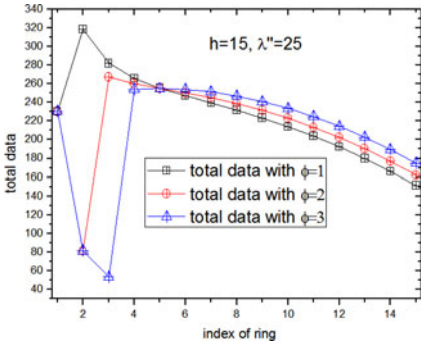


Fig. 4. Traffic load distribution with various ϕ.

Based on the traffic load of data collection, legitimacy verification and witness selection derived from Theorems 2, 3, and 4, we can obtain the expression for total traffic load of each sensor node by using ERCD protocol as $d_k^t = d_k^c + d_k^v + d_k^w$. When we know $\lambda_1, \lambda_2, \lambda_3, \varepsilon_1$ and ε_2, we can derive the optimal ϕ to maximize the network lifetime with $d_k^t = d_k^c + d_k^v + d_k^w$. As shown in Fig. 4, ϕ has significant impact on the energy consumption of sensor nodes. When ϕ is $1, 2$ and 3, sensor nodes with ring indices $2, 3$, and 5 consume the maximal energy throughout the WSN, respectively. Thus, the network lifetime can be determined by different values of ϕ, and it is critical to obtain the optimal ϕ to maximize the network lifetime.

Let g, p and α denote the number of witnesses selected by each neighbor, the probability that a neighbor will copy position information, and the average node degree in the network, respectively. To evaluate the performance, we compare the ERCD protocol with some existing protocols in terms of network lifetime.

Theorem 5. *If $\varepsilon_1 = \varepsilon_2$ and $\lambda_1 = \lambda_3 = 1$, the ratio of network lifetime by using ERCD protocol over RED or LSM protocol is shown as following:*

$$\frac{h^2 + gp\alpha h\lambda_2\sqrt{\alpha+1}}{\max\left((h^2+1+\lambda_2), \max(\frac{h^2-(k-1)^2}{2k-1} + h\lambda_2 + \frac{2\pi kh^2}{(h-\phi)(2k-1)})\right)}, \quad \text{where } k > \phi \geq 1 \tag{13}$$

Proof. Since the network lifetime is ended by the first occurrence of node outage, it is inversely proportional to the maximal energy consumption of sensor nodes. Energy consumption of the RED or LSM protocol includes normal data transmission and legitimacy verification. In data collection, the packet number of nodes in ring k is $(h^2-(k-1)^2)/(2k-1)$. The traffic load of ring 1 has the maximal energy consumption, which is the bottleneck of network lifetime. In ring 1, the packet number for data transmission is h^2, and the packet number for verification is $gp\alpha\sqrt{n}$. Since $\pi r^2\rho = \alpha + 1$ and $n = \pi(hr)^2\rho$, we can get $gp\alpha h\lambda_2\sqrt{\alpha+1}$. Therefore, the expression of the number of transmitted packets through nodes in ring 1 by using RED or LSM protocol is $h^2 + gpdh\lambda_2\sqrt{\alpha+1}$.

In ERCD protocol, suppose that nodes located in ring k have the maximal energy consumption. We consider two cases according to whether nodes with the maximal energy consumption locate in ring 1 or not, i.e., $k \leq \phi$. If $k \leq \phi$, the packet number for transmission by nodes in ring k is $h^2 + 1 + \lambda_2$, where h^2, 1 and λ_2 are the packet number for data collection, witness selection and legitimacy verification, respectively. For the case $k > \phi$, the packet number for data collection, legitimacy verification and witness selection in ring k are $(h^2-(k-1)^2)/(2k-1)$, $h\lambda_2$, and $2\pi kh^2/[(h-\phi)(2k-1)]$, respectively. Therefore, we can obtain the packet number for transmission by nodes in ring k as

$$\begin{cases} \max\left((h^2+1+\lambda_2), \max\left(\frac{h^2-(k-1)^2}{2k-1} + h\lambda_2 + \frac{2\pi kh^2}{(h-\phi)(2k-1)}\right)\right) \\ \text{where } k > \phi \geq 1. \end{cases} \tag{14}$$

After that, the ratio of network lifetime by using ERCD protocol over RED or LSM protocol can be expressed as shown in Eq. (13). □

After the analysis of network lifetime, we further analyze the total energy consumption to have a comprehensive performance evaluation of ERCD protocol. We derive the energy consumption of legitimacy verification and witness selection, which can be expressed in terms of average hop length, to calculate the total energy consumption by using ERCD protocol. Let Ψ_v denote the average hop length of legitimacy verification for each sensor. The average hop length of legitimacy verification for each sensor can be expressed as follows.

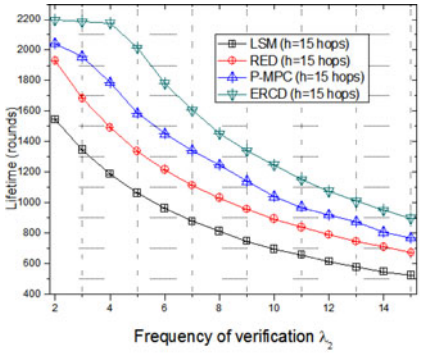
Theorem 6. *By using ERCD protocol, the average hop length of legitimacy verification for each sensor is*

$$\Psi_v = \frac{\sum_{k=1}^{\phi}\left[(2k-1)\frac{\sum_{i=\phi+1-k}^{h-k} i}{h-\phi}\right] + \sum_{k=\phi+1}^{h}\left[(2k-1)\frac{\sum_{i=0}^{h-k} i + \sum_{i=1}^{k-\phi} i}{h-\phi}\right]}{h^2} + \frac{\pi(\phi+1+h)}{2} + 1. \tag{15}$$

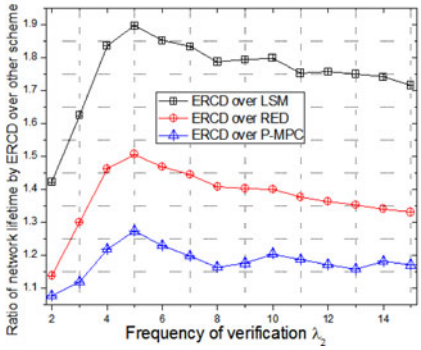
Proof. For the case that $k \leq \phi$, the average hop length of verification traffic sent from ring $k, k \leq \phi$, is $\sum_{i=\phi+1-k}^{h-k} i/(h-\phi)$. If $k > \phi$, the average hop length of verification traffic sent from ring k can be expressed as $(\sum_{i=0}^{h-k} i + \sum_{i=1}^{k-\phi} i)/(h-\phi)$. Since there are total $\pi(2k-1)r^2\rho$ sensors in ring k and total number of sensors is $\pi h^2 r^2\rho$, the average hop length from each sensor node in ring k to its witness ring should be

$$\Psi' = \frac{\sum_{k=1}^{\phi}\left[(2k-1)\frac{\sum_{i=\phi+1-k}^{h-k} i}{h-\phi}\right] + \sum_{k=\phi+1}^{h}\left[(2k-1)\frac{\sum_{i=0}^{h-k} i + \sum_{i=1}^{k-\phi} i}{h-\phi}\right]}{h^2}. \tag{16}$$

As sensor nodes that locate outside ring ϕ need to forward verification message to their witnesses heads, additional $\pi(\phi+1+h)/2$ should be included for each of these sensors. Moreover, one more hop length for three-ring broadcasts should be added to the calculation. Overall, we can express the average hop length of legitimacy

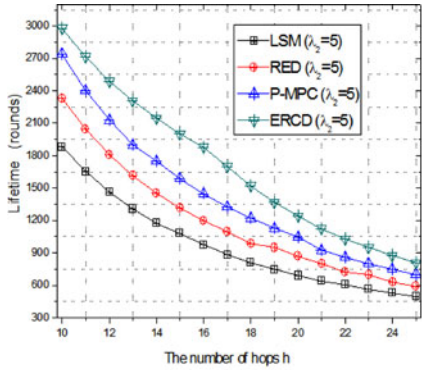


(a) Network lifetime

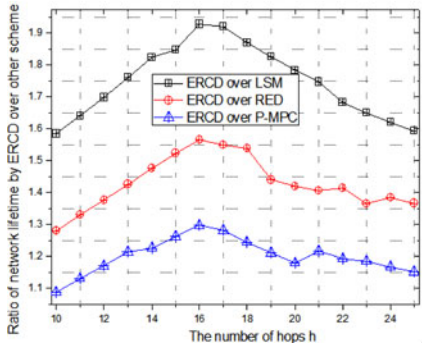


(b) Ratio of network lifetime

Fig. 5. Performance comparison of existing protocols under different λ_2 $(g = 1, p = 0, \alpha = 10)$.



(a) Network lifetime



(b) Ratio of network lifetime

Fig. 6. Performance comparison of existing protocols under different h $(g = 1, p = 0, \alpha = 10)$.

verification for each sensor as $\Psi_v = \Psi' + \pi(\phi + 1 + h)/2 + 1$. □

After that, we calculate the energy consumption for witness selection so as to obtain the total energy consumption. Let Ψ_w denote the average hop length of witness selection for each sensor.

Theorem 7. *By using ERCD protocol, the average hop length of witness selection for each sensor is*

$$\Psi_w = \Psi' + \pi(\phi + 1 + h). \tag{17}$$

Proof. From Theorem 6, we know that the average hop length for each sensor to achieve its witness ring is Ψ'. To construct a ring of witnesses for a source node in ring k, the required hop length is $2\pi k$. As witnesses locate in $h - \phi$ rings, the average hop length for each sensor to generate a ring of witnesses is $\sum_{k=\phi+1}^{h} 2\pi k/(h - \phi) = \pi(\phi + 1 + h)$. Thus, the average hop length of witness selection for each sensor can be expressed as $\Psi_w = \Psi' + \pi(\phi + 1 + h)$. □

Let e denote the energy consumption for transmitting and receiving a bit. From Theorems 6 and 7, we can obtain the total energy consumption of WSNs for clone detection by using ERCD protocol in a data collection cycle, denoted E, as $E = n\Psi_v\varepsilon_2\lambda_2 e + n\Psi_w\varepsilon_2\lambda_3 e$, where n is the total number of nodes.

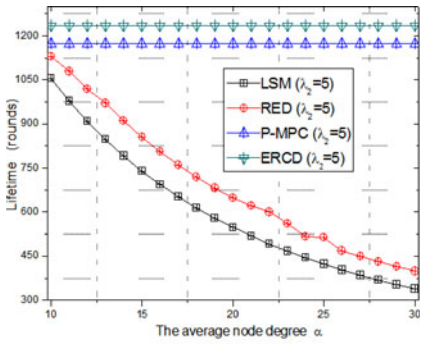
The network lifetime performance of ERCD protocol is compared with that of other protocols including LSM, RED and P-MPC under various parameters in Figs. 5, 6, and 7 according to Eq. (13). It is found that the network lifetime of ERCD protocol outperforms that of other protocols, which is caused by successfully distributing packets all over the network except the non-witness region to release the traffic bottleneck around the sink. We also observe that the network lifetime by using ERCD protocol in a network with dense deployment is independent of the average node degree, which means that the network lifetime will not be impacted with the increase of node density. This is because the maximal energy consumption does not depend on the average node degree α as shown in Eq. (14), which leads to the summary that the network lifetime is not related to average node degree. Overall, we find that the ERCD protocol is a scalable clone detection protocol, which can significantly outperform LSM, RED and P-MPC under various network scenarios.

5.3 Data Buffer Capacity

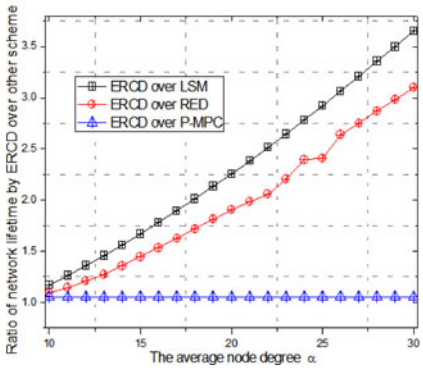
Usually, sensors are of small size and have very limited capacity of both data buffer and energy battery. In this section, we analyze the required data buffer capacity, also referred to as data buffer of sensors to evaluate the performance of the proposed ERCD protocol. Let σ denote the required packet storage size for being a witness of a sensor node.

Theorem 8. *Under the ERCD protocol, the required data buffer for each sensor is $O(h)$.*

Proof. Since the ring index of witnesses is randomly generated, for any ring k, there are $n/(h - \phi)$ nodes choosing ring k as their witness rings. The number of nodes selected as witnesses in ring k is $2\pi k$. The required data buffer for ring k is $2\pi k n\sigma/(h - \phi)$. There are total $\pi(2k - 1)r^2\rho$ nodes in ring k, thus the required data



(a) Network lifetime



(b) Ratio of network lifetime

Fig. 7. Performance comparison of existing protocols under different α $(g = 1, p = 0, h = 15)$.

buffer for each sensor can be expressed as

$$\begin{cases} \frac{2\pi k n \sigma}{(h-\phi)\pi(2k-1)r^2\rho} = \frac{2\pi k h^2}{(h-\phi)(2k-1)} \\ \text{where } k \in (\phi+1, h-1). \end{cases} \quad (18)$$

Obviously, when $k = \phi + 1$, the required data buffer for each sensor is maximized, which is $2\pi h^2(\phi+1)/(h-\phi)$ $(2\phi+1)$. For any given value of ϕ, we can calculate the maximal required data buffer for each sensor node. Therefore, as $2\pi h^2(\phi+1)/(h-\phi)$ $(2\phi+1) = O(h)$, we can conclude that the required data buffer is $O(h)$. □

The required data buffer capacities of most previous works are related to the number of sensor nodes. In ERCD protocol, the required data buffer capacity is related to the hop length of the network area. Therefore, the requirement of data buffer capacity by using ERCD protocol is not related to the node density.

6 Experiment Results

To evaluate the performance of ERCD protocol, the OMNET ++ [25], a well-known open source modular simulation platform for large network, is used in our simulations. As the OMNET++ is a discrete event-driven system, the future event set is stored in the system, and events are released one by one to evaluate our ERCD protocol in the simulation. We set up a circular shaped wireless sensor network, which consists of 2,000 sensor nodes with a radius 600 m. The transmission range of each sensor node is $r = 40$ m. In the simulation, data and verification request messages are of the same size for simplicity, i.e., $\varepsilon_1 = \varepsilon_2 = 100$ bytes. Each cycle of witness selection is followed by a data collection

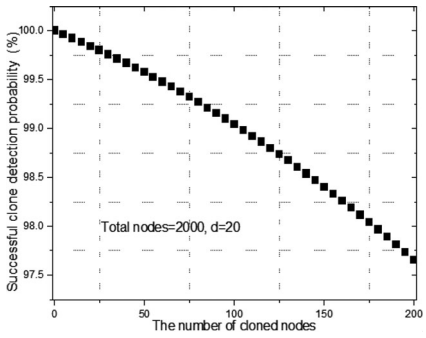
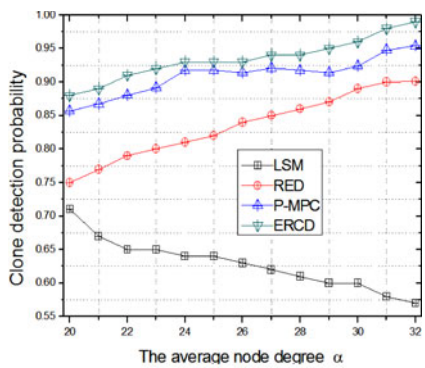


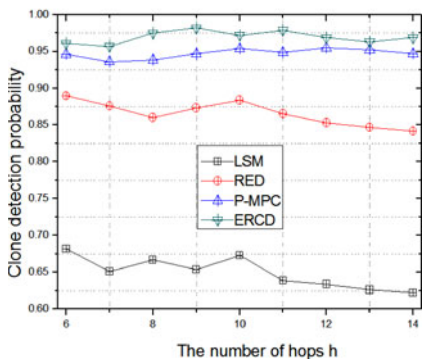
Fig. 8. Clone detection probability (untrustful witnesses).

cycle, $\lambda_1 = \lambda_3 = 1$, and the frequency of legitimacy verification is set as $\lambda_2 = 10$. We set the amount of non-witness rings ϕ as 1. The frequency of clone detection can be determined according to the practical requirement, e.g., once a day for temperature measurement in forest or once an hour for bank monitor.

In Fig. 8, we present the case that witnesses can be compromised, and thus clone detection may fail due to modification of verification messages by compromised witnesses. For untrustful witnesses, since any witness has permission to read the information of verification messages from the source node, compromised witnesses can read the verification message, and modify (regenerate another modified copy of) the verification message before forwarding it to other witnesses. It is hard to determine whether the message sent from a compromised witness is original or modified. In other words, witness nodes may be compromised but it is hard to detect it. Since BSs cannot figure out



(a) The average node degree α



(b) The number of hops h

Fig. 9. Clone detection probability of ERCD or existing protocols under different parameters.

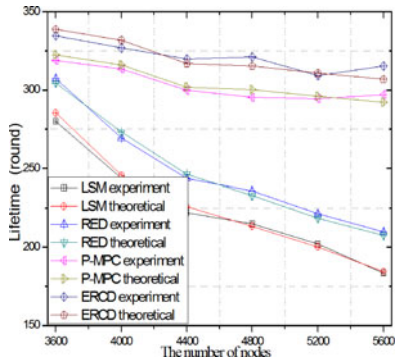


Fig. 10. Network lifetime with different node numbers.

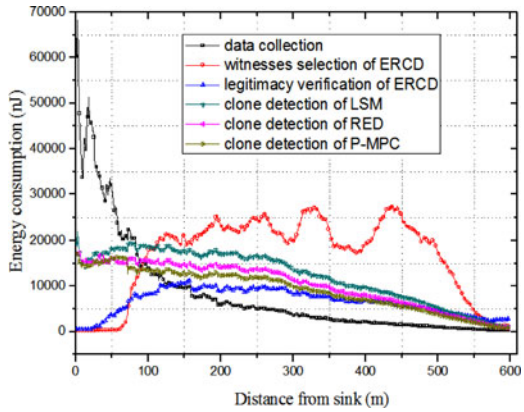


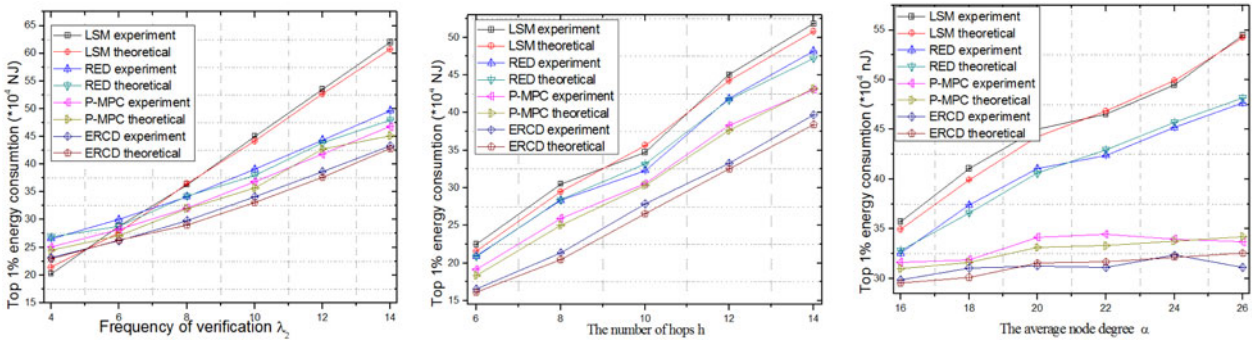
Fig. 11. Energy consumption of each step by using ERCD or existing protocols.

whether the received verification message is the original copy or not, it may be difficult to effectively find out which witness is compromised. Thus, to our best knowledge, there is no efficient method to solve the failure due to untrustful witnesses until now.

Most previous works assume that all selected witnesses are trustful. In our work, we have relaxed the assumption of trustful witness node, and investigated the case that some selected witnesses have been compromised, as shown in Fig. 8. we count a certain round of clone detection as failure if any of selected witnesses is compromised in this round. In ERCD protocol, since we have a set of witnesses for each sensor, the probability that a compromised witness receives the request message is very low. The experiment results demonstrate that the clone detection probability can closely approach 100 percent with untrustful witnesses. Then, the clone detection probability of ERCD and some existing protocols under different node density and network scale are compared in Fig. 9. We have two observations: 1) ERCD protocol has better performance in clone detection probability than other protocols, which can successfully detect the clone attacks with $87\%\sim100\%$; and 2) the clone detection probability of ERCD protocol increases with growth of average node degree, since it has higher probability to successfully conduct witness selection.

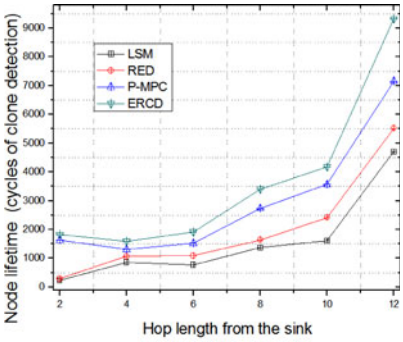
We compare the network lifetime with different numbers of sensor nodes in Fig. 10. Generally, sensor nodes closer to the sink node have relatively heavier traffic load than those far away nodes, and will deplete their energy faster. With the growth of the node number, the traffic load of those sensors increases dramatically, which leads to a much shorter lifetime of those nodes. ERCD protocol distributes the traffic load across the network, which balances the energy consumption of sensors at different locations. Therefore, the proposed ERCD protocol achieves the best network lifetime among the listed protocols, and it does not significantly decrease with the increase of node number as shown in Fig. 10. The energy consumption of each step by using ERCD or some existing protocols is shown in Fig. 11. We calculate energy consumption of ERCD protocol in data collection, witness selection and legitimacy verification, and that of LSM, RED and P-MPC in data collection and clone detection. The energy consumption of data collection for all protocols is the same. In LSM, RED and P-MPC protocols, sensors close to the sink need to relay more traffic of both data collection and clone detection, thus have higher energy consumption and may have higher outage probability around the sink. By using ERCD protocol, energy consumption of sensors close to the sink has lower traffic of witness selection and legitimacy verification, which helps to balance the uneven energy consumption of data collection.

Since network lifetime is closely related to the sensor with the maximal energy consumption, we compare sensor nodes with top 1 percent energy consumption, i.e., 1 percent sensor nodes with maximal energy consumption, under various parameters by using ERCD or some existing protocols in Fig. 12. The top 1 percent energy consumption of ERCD protocol is higher than other protocols when $\lambda_2 < 6$. This is because ERCD protocol has higher energy consumption in witness selection than other clone detection

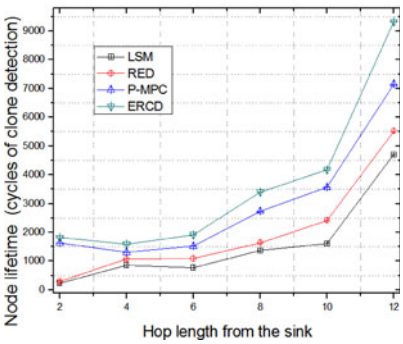


(a) Frequency of legitimacy verification λ_2 (b) The number of hops h (c) The average node degree α

Fig. 12. Top 1 percent Energy consumption of ERCD or existing protocols under different parameters.

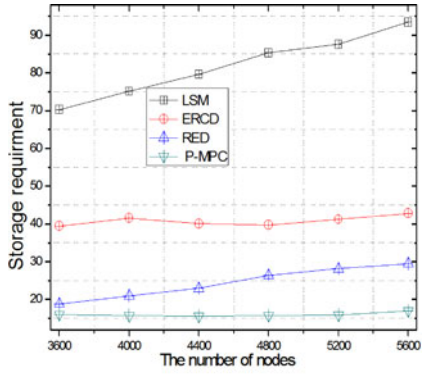


(a) The number of node outage with various clone detection cycles

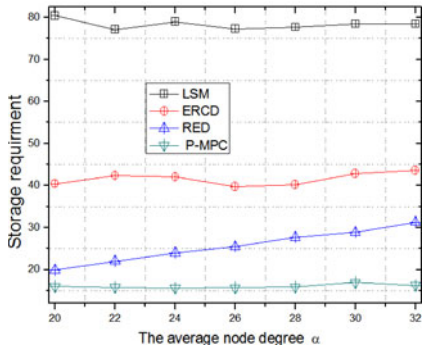


(b) Lifetime of sensor nodes with various hop length from the sink

Fig. 13. Energy consumption of sensor nodes by using ERCD or existing protocols under different parameters.



(a) Different node numbers



(b) Different average node degrees α

Fig. 14. Required data buffer by using ERCD or existing protocols.

protocols. Generally, clone detection frequency is much higher than witness selection or data collection. Under the scenario of large λ_2, our protocol can outperform other protocols as shown in Fig. 12a. From Figs. 12b and 12c, we can observe that ERCD protocol has better performance with a higher node density, which can extend the network lifetime by $10\%\sim80\%$. We further compare the energy consumption of sensor nodes with various cycles of clone detection and hop length from the sink in Fig. 13. The sensor nodes have longer network lifetime under scenarios of the same time period or location by using ERCD protocol comparing with other protocols.

We compare the required data buffer with various node densities by using ERCD or some existing protocols in Fig. 14. ERCD protocol significantly outperforms the LSM, but requires more data buffer than RED and P-MPC, under the scenarios of different node densities. This is because ERCD protocol assigns witnesses with a ring structure, which results high performance in clone detection and network lifetime, but may need some additional data buffer comparing with RED and P-MPC protocols. Comparing with the LSM protocol, the storage requirements of ERCD, RED and P-MPC protocols do not increase with the growth of node number. This is because the witness number of LSM depends on the node number while other protocols does not, which can achieve lower storage requirement with more node number or node density.

Finally, we study the impact of the duty cycle on the proposed ERCD protocol, and evaluate average delay and routing success rate, i.e., the rate of successful routing over all rounds of transmission, with various duty cycles. Specifically, we consider a WSN located in a 500 m $\times$ 500 m region, where the transmission range of each sensor node is 50 m. In ERCD protocol, a sensor node will forward the message to another awaken sensor when available. If its neighboring sensors are in sleep mode, the sensor will hold the message till at least one relaying sensor wakes up or delay times out. The round of clone detection routing is determined as failure if the delay of any node's transmission is larger than 1 second. We evaluate the impact of duty cycle, denoted as τ, on our protocol in terms of routing success rate. As shown in Fig. 15, based on a WSN with node density of $1.4\sim1.8$ nodes/m^2, the routing success rate increases with the growth of duty cycle and network density in general, due to more awaken sensors ready for forwarding.

The relationship of average delay, duty cycle and node density is shown in Fig. 16. The average delay is very small when node density is larger than 1.8 nodes/m^2, and the

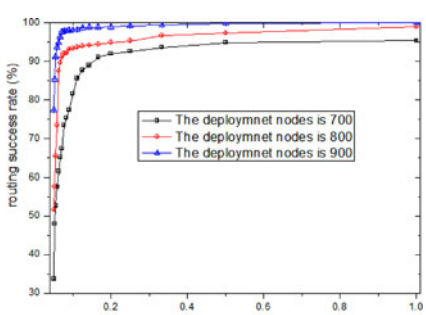
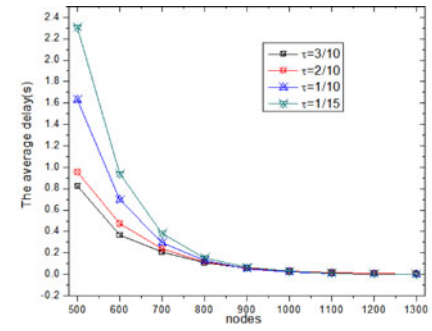
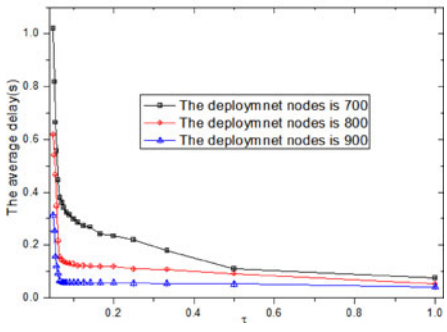


Fig. 15. Routing success rate with various duty cycle.



(a) Different number of nodes



(b) Different duty cycle τ

Fig. 16. Average delay by using ERCD protocol.

average delay of sensor nodes decreases significantly with the increase of duty cycles from 0 to 0.05.

7 Conclusion

In this paper, we have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. In addition, our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended. In our future work, we will consider different mobility patterns under various network scenarios.

Acknowledgments

This work was supported by NSERC Canada, the National Natural Science Foundation of China (61379110, 61073104, 61272149, and 61272494), and the National Basic Research Program of China (973 Program) (2014CB046305). A preliminary version of this paper was presented at the 32nd Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2013), Turin, Italy [1]. Prof. Anfeng Liu is the corresponding author of this work.

References

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," in *Proc. IEEE INFOCOM*, Apr. 14-19, 2013, pp. 2436–2444.

[2] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Commun. Mag.*, vol. 49, no. 4, pp. 28–35, Apr. 2011.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, Mar. 2002.

[4] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, "Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks," *Comput. Netw.*, vol. 56, no. 7, pp. 1951–1967, May. 2012.

[5] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Trans. Mobile Comput.*, vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, "A randomized countermeasure against parasitic adversaries in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 7, pp. 1036–1045, Sep. 2010.

[7] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.

[8] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," *IEEE Netw.*, vol. 25, no. 5, pp. 50–55, May. 2011.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "A dynamic privacy-preserving key management scheme for location based services in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 1, pp. 127–139, Jan. 2012.

[10] M. Conti, R. D. Pietro, L. 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.-Oct. 2011.

[11] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Security Privacy*, Oakland, CA, USA, May. 8-11, 2005, pp. 49–63.

[12] 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. 28, pp. 677–691, Jun. 2010.

[13] 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.

[14] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN," *IEEE Trans. Mobile Comput.*, vol. 11, no. 5, pp. 793–806, May. 2012.

[15] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen., "BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 1, pp. 32–43, Jan. 2012.

[16] J. Li, J. Chen, and T. H. Lai, "Energy-efficient intrusion detection with a barrier of probabilistic sensors," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 25-30, 2012, pp. 118–126.

[17] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE Trans. Syst., Man, Cybern.*, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[18] W. Naruephiphat, Y. Ji, and C. Charnsripinyo, "An area-based approach for node replica detection in wireless sensor networks," in *Proc. IEEE TrustCom*, Liverpool, UK, Jun. 25-27, 2012, pp. 745–750.

[19] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in *Proc. IEEE 17th Int. Conf. Netw. Protocols*, Princeton, NJ, USA, Oct. 13-16, 2009, pp. 284–293.

[20] T. Bonaci, P. Lee, L. Bushnell, and R. Poovendran, "Distributed clone detection in wireless sensor networks: An optimization approach," in *Proc. IEEE IEEE Int. Symp. World of Wireless, Mobile Multimedia Netw.*, Lucca, IT, Jun. 20-23, 2011, pp. 1–6.

[21] Q. Chen, S. S. Kanhere, and M. Hassan, "Analysis of per-node traffic load in multi-hop wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 958–967, Feb. 2009.

[22] A. Liu, P. Zhang, and Z. Chen, "Theoretical analysis of the lifetime and energy hole in cluster based wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 71, no. 10, pp. 1327–1355, Oct. 2011.

[23] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symp. Security Privacy*, Berkeley, CA, USA, May 11-14, 2003, pp. 197–213.
[24] C. Ok, S. Lee, P. Mitra, and S. Kumara, "Distributed routing in wireless sensor networks using energy welfare metric," *Inf. Sci.*, vol. 180, no. 9, pp. 1656–1670, May 2010.
[25] OMNET++ network simulation framework: [Online]. Available: http://www.omnetpp.org/

Zhongming Zheng received the BEng. (2007) and MSc (2010) degrees from the City University of Hong Kong in 2007 and 2010, respectively, and the PhD degree in 2015 from the University of Waterloo. His research interests include green wireless communication, smart grid, and wireless sensor networks. He is a student member of the IEEE.

Anfeng Liu received the MSc and PhD degrees from Central South University, China, in 2002 and 2005, respectively, both in computer science. He is a professor in the School of Information Science and Engineering at Central South University, His major research interests are crowd sensing network and wireless sensor network. He is a member of the IEEE.

Lin X. Cai received the MASc and PhD degrees in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2005 and 2010, respectively. She was a postdoctoral research fellow in the Electrical Engineering Department at Princeton University in 2011. She then worked as a senior engineer at Huawei US Wireless R&D center from 2012 to 2014. She has been an assistant professor with the Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, IL, since August 2014. Her research interests include green communication and networking, broadband multimedia services, radio resource and mobility management, and cognitive radio networks. She is a member of the IEEE.

Zhigang Chen received the BSc, MSc, and the PhD degrees from Central South University, China, 1984, 1987, and 1998, respectively. He is a PhD supervisor and his research interests are in network computing and distributed processing. He is a member of the IEEE.

Xuemin (Sherman) Shen received the BSc degree in 1982 from Dalian Maritime University, China, and the MSc and PhD degrees in 1987 and 1990, respectively, from Rutgers University, New Jersey, all in electrical engineering. He is a professor and university research chair in the Department of Electrical and Computer Engineering, University of Waterloo. He was the associate chair for graduate studies from 2004 to 2008. His research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks. He is a co-author/editor of six books, and has published more than 600 papers and book chapters in wireless communications and networks, control, and filtering. He has served as the technical program committee chair for IEEE VTC 10 Fall, a symposia chair for IEEE ICC 10, a tutorial chair for IEEE VTC 11 Spring and IEEE ICC 08, a technical program committee chair for IEEE GLOBECOM 07, IEEE INFOCOM 14, a general co-chair for Chinacom 07, QShine 06 and ACM MobiHoc 15, a chair for IEEE Communications Societys Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as an editor-in-chief for *IEEE Network*, *Peer-to-Peer Networking and Application*, and *IET Communications*; a founding area editor for the *IEEE Transactions on Wireless Communications*; an associate editor for the *IEEE Transactions on Vehicular Technology*, *Computer Networks*, and *ACM/Wireless Networks*; and as a guest editor for *IEEE Journal on Selected Areas in Communications*, *IEEE Wireless Communications*, *IEEE Communications Magazine*, and *ACM Mobile Networks and Applications*. He received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo, the Premiers Research Excellence Award (PREA) in 2003 from the Province of Ontario, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. He is a registered professional engineer of Ontario, Canada, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of the *IEEE Vehicular Technology and Communications Societies*. He is a fellow of the IEEE.