

Received 1 April 2013; revised 3 June 2013; accepted 29 June 2013. Date of publication 12 July 2013;  
date of current version 21 January 2014.

Digital Object Identifier 10.1109/TETC.2013.2273220

# A Wormhole Attack Resistant Neighbor Discovery Scheme With RDMA Protocol for 60 GHz Directional Network

ZHIGUO SHI<sup>1,3</sup> (Member, IEEE), RUIXUE SUN<sup>1</sup>, RONGXING LU<sup>2</sup> (Member, IEEE), JIAN QIAO<sup>3</sup>,  
JIMING CHEN<sup>4</sup> (Senior Member, IEEE), AND XUEMIN SHEN<sup>3</sup> (Fellow, IEEE)

<sup>1</sup>Department of Information and Electronic Engineering, Zhejiang University, Hangzhou 310027, China

<sup>2</sup>School of Electrical and Electronic Engineering, Nanyang Technological University, 639798, Singapore

<sup>3</sup>Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada

<sup>4</sup>State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China

CORRESPONDING AUTHOR: Z. SHI (shizg@zju.edu.cn)

This work was supported in part by the National Science Foundation of China under Grant 61171149, the Fundamental Research Funds for the Chinese Central Universities under Grant 2013xzzx008-2, and ORF-RE, Ontario, Canada. Part of this paper was presented at the 2013 IEEE Wireless Communications and Networking Conference, Shanghai, China, Apr. 2013.

**ABSTRACT** In this paper, we propose a wormhole attack resistant secure neighbor discovery (SND) scheme for a centralized 60-GHz directional wireless network. Specifically, the proposed SND scheme consists of three phases: the network controller (NC) broadcasting phase, the network nodes response/authentication phase, and the NC time analysis phase. In the broadcasting phase and the response/authentication phase, local time information and antenna direction information are elegantly exchanged with signature-based authentication techniques between the NC and the legitimate network nodes, which can prevent most of the wormhole attacks. In the NC time analysis phase, the NC can further detect the possible attack using the time-delay information from the network nodes. To solve the transmission collision problem in the response/authentication phase, we also introduce a novel random delay multiple access (RDMA) protocol to divide the RA phase into  $M$  periods, within which the unsuccessfully transmitting nodes randomly select a time slot to transmit. The optimal parameter setting of the RDMA protocol and the optional strategies of the NC are discussed. Both neighbor discovery time analysis and security analysis demonstrate the efficiency and effectiveness of the proposed SND scheme in conjunction with the RDMA protocol.

**INDEX TERMS** Cyber physical systems, 60 GHz directional network, secure neighbor discovery, wormhole attack, random delay multiple access.

## I. INTRODUCTION

Communications in the unlicensed 57–66 GHz band (60 GHz for short) have recently attracted great attention from both academic and industry [2]–[4]. Especially, by using SiGe and CMOS technologies to build inexpensive 60 GHz transceivers, there has been growing interest in standardizing and drafting specifications in this frequency band for both indoor and outdoor application scenarios such as “outdoor campus” and “auditorium deployments” [5]. In October 2009, IEEE 802.15.3c was introduced for wireless personal area networks (WPAN) [6], [7], and in January 2013, the formal standard of IEEE 802.11ad was appeared for wireless local area networks (WLAN) [8].

One distinguishing feature of the 60 GHz communication is its high propagation loss due to the extremely high carrier frequency and the oxygen absorption peaks at this frequency band [2]. To combat this, directional antenna with high directivity gain can be adopted to obtain sufficient link budget for multi-Gbps data rate. Although the directional antenna offers many advantages for the 60 GHz communication, the antenna beam should be aligned in the opposite direction for a communication pair before their communication starts. This poses many special challenges for higher layer protocol design [9]–[13], and one of these challenges is the neighbor discovery problem [14]–[16].

For each network node, neighbor discovery is a process to determine the total number and identities of other nodes within its communication range. Since neighbor discovery serves as the foundation of several high layer system functionalities [17], the overlying protocols and applications of a system will be compromised if neighbor discovery is successfully attacked. One type of major attacks to neighbor discovery is wormhole attack, in which malicious node(s) relay packets for two legitimate nodes to fool them believing that they are direct neighbors [18]–[20]. It seems a merit that this kind of attack can enlarge the communication ranges, however, since it causes unauthorized physical access, selective dropping of packets and even denial of services, the wormhole attack is intrinsically a very serious problem especially in case of emergent information transmission. For example, in one of the outdoor application scenarios named “Police/Surveillance Car Upload” as defined in the usage models of 802.11ad [5], this attack may cause very severe consequences. Therefore, it is very important to design a wormhole attack resistant neighbor discovery scheme for 60 GHz directional networks.

Wormhole attack is more difficult to combat in 60 GHz directional networks than in networks with omni-directional antenna. The reason can be explained as follows. In a network with omni-directional antenna, when a malicious node attempts to launch a wormhole attack, nearby nodes around it from all directions can hear it and can co-operate to detect the attack [21]. However, in a 60 GHz network with directional antenna, when a wormhole attack happens, only nodes in the specific direction can hear the data transmission, and consequently the probability of attack detection becomes much less than that with omni-directional antenna.

To address this difficulty, we propose a wormhole attack resistant secure neighbor discovery (SND) scheme for a 60 GHz wireless network operating in infrastructure mode in this paper. All devices in the network are equipped with directional antenna. Although there are some related works [18], [22], [23] on the wormhole attack resistant scheme for wireless networks with directional antenna, the wormhole attack in the 60 GHz infrastructure mode network remains a problem. The main contributions of this work is summarized as follows.

- First, we propose a wormhole attack resistant SND scheme, which establishes the communications with signature-based authentication techniques, and achieves SND by utilizing the information of antenna direction, local time information and carefully designed length of the broadcast message.
- Second, we introduce a random delay multiple access (RDMA) protocol to solve the transmission collision problem in the response/authentication phase when each node in the same sector does not have information of others and can not listen to the others’ transmissions due to the limitation of directional antenna.
- Third, we conduct extensive secure analysis and neighbor discover time analysis to demonstrate the

effectiveness and efficiency of the proposed wormhole attack resistant SND scheme.

The remainder of this paper is organized as follows. In Section II, we provide the network model, attack model, and give some necessary assumptions. Then, we present the detailed design of the proposed wormhole attack resistant SND scheme in Section III, followed by the design and analysis of the proposed RDMA protocol in Section IV. In Section V and Section VI, we conduct security analysis and neighbor discovery time analysis for the proposed scheme, respectively. Finally, we conclude this paper in Section VI.

## II. PROBLEM FORMULATION

In this section, we formalize the network model and the attack model, and make some necessary assumptions.

### A. NETWORK MODEL

For 60 GHz directional networks, from the usage model of both 802.15.3c and 802.11ad, it is known that almost all the application scenarios are based on a centralized network structure, i.e., at least one network controller (NC) is deployed, although concurrent point-to-point transmissions are supported between different pairs of devices. Thus, we only consider the infrastructure mode where there exists one NC for access control and resources management of the network. In particular, we consider a 60 GHz network composed of multiple wireless nodes  $\mathbb{N} = \{N_1, N_2, N_3, \dots\}$  and a single NC, which may be an access point (AP) in 802.11ad-based WLAN or a piconet controller (PNC) in 802.15.3c-based WPAN, as shown in Fig. 1. Wireless nodes are randomly distributed in the area for study with node density  $\rho$  per square meter. Each of the wireless nodes and the NC are equipped with an electronic steering antenna, which can use digital beamforming techniques to span a beamwidth with angle of  $\beta = 2\pi/L$  radians, where  $L$  is the total number of beams. All the  $L$  beams can collectively maintain the seamless coverage of the entire direction.

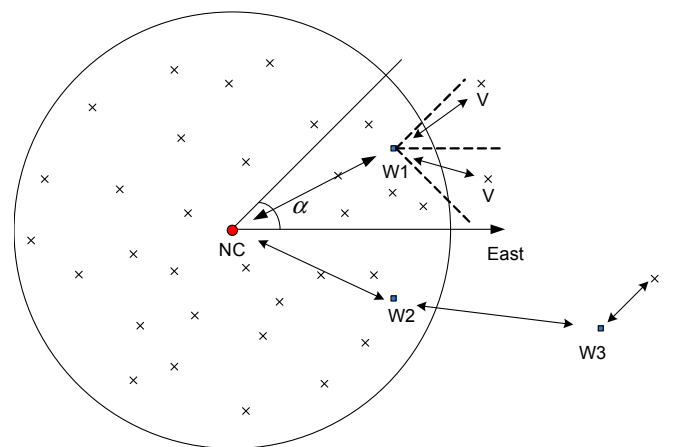


FIGURE 1. Network model under consideration.

The beams of the directional antenna are numbered from 1 to  $L$  in a counter-clockwise manner from the axis pointing to the eastern direction. An ideal “flat-top” model [24] for the directional antenna is applied. The normalized pattern function of the directional antenna when it selects the  $i$ -th ( $1 \leq i \leq L$ ) beam is defined as:

$$g(k) = \begin{cases} 1, & \text{if } k = i \\ 0, & \text{if } k \neq i. \end{cases} \quad (1)$$

When the NC uses its directional antenna to communicate with other nodes, the maximum reachable distance is  $R$ , which is the radius of a circular region that it can cover. With directional antennas used in both transmitters and receivers, the average received power can be modeled as [11]:

$$P_R = k_1 G_T G_R d^{-\alpha} P_T, \quad (2)$$

where  $k_1$  is a constant coefficient dependant on the wavelength,  $G_T$  and  $G_R$  are antenna gain of the transmitter and receiver, respectively,  $d$  is the distance from the transmitter to the receiver,  $\alpha$  is the path loss exponent, and  $P_T$  is the averaged transmitting power. When both the NC and the network nodes employ directional antennas, the maximum reachable distance  $R$  is dependant on the sector number  $L$  and can be determined when the transmitting power is fixed and a minimum threshold value of  $P_{R_{th}}$  is required.

All the links between the network nodes and the NC are bidirectional, i.e., if a wireless node A can hear the NC (or another node B), then the NC (or the node B) can also hear node A. All the wireless nodes do not have specialized hardware such as a GPS module to know its own global position, but they do have a kind of electronic compass which is much cheaper than the GPS module and used to align the beam direction, i.e., different antennas with the same beam number point to the same sector.

## B. ATTACK MODEL

We focus on an active attack named wormhole attack, in which the malicious node(s) relay packets for two legislate nodes to fool them believing that they are direct neighbors. In particular, there are two types of wormhole attack in the network, as shown in Fig. 1. One type of attack is that, there is a malicious node, e.g., W1, between the NC and the distant nodes. In the neighbor discovery procedure, the malicious node relays the packets from the NC to the distant wireless node and vice-versa, to make them believe they are direct neighbor and let the NC offer service to the distant node. Another type of such attack is that, there are two or even more malicious nodes, e.g., W2 and W3, and they collude to relay packets between the NC and a distant legislate wireless node to believe they are direct neighbor. We only consider the first type of wormhole attack, as the proposed SND scheme is also effective for the second attack. In our attack model, we assume there exist several malicious nodes in the networks, and the malicious node density is denoted as  $\rho_m$  per square meter.

## C. ASSUMPTIONS

Our goal is to design a wormhole attack resistant SND scheme for the 60 GHz directional network. The proposed SND scheme is based on some necessary assumptions as follows.

- Assumption 1: The NC is always trusted and responsible for the authentication, neighbor discovery, malicious nodes detection, etc.
- Assumption 2: Both the NC and the legislate nodes are equipped with certain computation capability, and can execute the necessary cryptographic operations. For instance, the NC has its ElGamal-type private key  $x_c \in \mathbb{Z}_q^*$ , and the corresponding public key  $Y_c = g^{x_c} \mod p$  [25]; and each node  $N_i \in \mathbb{N}$  also has its private-public key pair ( $x_i \in \mathbb{Z}_q^*$ ,  $Y_i = g^{x_i} \mod p$ ). The malicious nodes have the same level of computation power as the legislate nodes, but they cannot obtain the key materials of the legislate nodes.
- Assumption 3: The malicious nodes have only one electronic steering antenna, and thus they can only replay the messages between the NC and wireless node at packet level rather than at bit level.

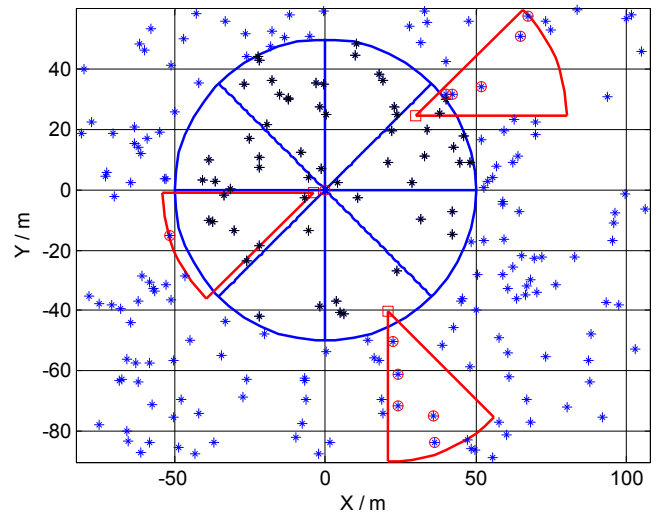


FIGURE 2. The simulated network scenario.

## III. PROPOSED WORMHOLE ATTACK RESISTANT SCHEME

In this section, we first introduce the main idea of the proposed scheme, followed by the detailed description of the three phases in the scheme, namely the NC broadcast (BC) phase, response/authentication (RA) phase and the NA time analysis (TA) phase.

To illustrate the main idea of the proposed scheme clearly, Fig. 2 shows a simulated network scenario, where the average node density  $\rho = 0.002$  per square meter, and the attacker node density  $\rho_m = 0.0004$ . The NC is located at the original point (0,0). The circular area around the NC is seamlessly covered by  $L = 8$  beams, and the direct communication range  $R$  is 50 meters. In this scenario, there exist three attackers marked with hollow square. Though the region that each

attacker can attack could be a circular area, sectors other than the three plotted sectors can be easily protected from the wormhole attack by using directional authentication, as described in the following. The objective of the proposed SND scheme is to detect whether there are malicious nodes in the NC's communication range  $R$ .

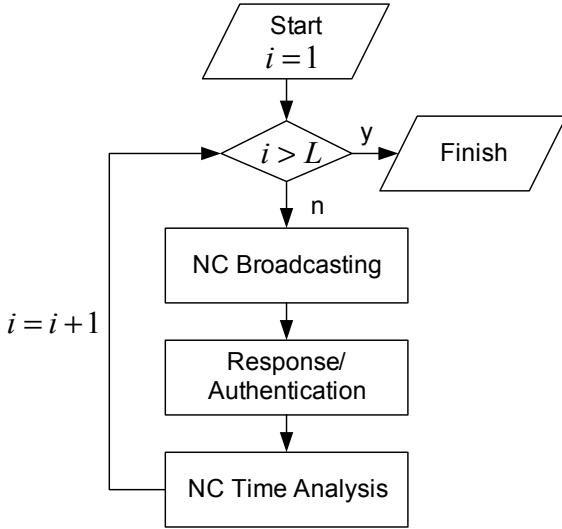


FIGURE 3. Flow chat of the proposed SND scheme.

The flowchart of the SND scheme is shown in Fig. 3. The NC discovers its neighbors in a sector-by-sector scan model, i.e., it scans its neighbor area from sector 1 to sector  $L$ . For the scan of each sector, the NC broadcasts its “hello” message in the specific direction. This period is called “NC BC phase”. The legislate nodes in this sector scan its neighbor sector in a counter-clockwise manner starting from a random sector, staying in each sector for  $t_n$  seconds. Thus, to guarantee that all the nodes in the sector that the NC is scanning can hear the “hello” message, the NC BC phase should last for at least  $Lt_n$  seconds.

After the NC broadcasts its “hello” message in a specific sector and all the nodes in this sector hear the “hello” message, the node “RA phase” launches. In this phase, either the node(s) in this sector hear the transmission collision and report wormhole attack, or they authenticate with the NC and report their local time information, which can be used by the NC for further detection of wormhole attack in the “NC TA phase”, as shown in Fig. 3.

From the time domain, the process of the proposed wormhole attack resistant SND scheme is shown in Fig. 4, which starts with the NC BC phase, followed by the RA phase and the NC TA phase. In the NC BC phase, the “hello” message is transmitted in each time slot of length  $t_n/2$  to guarantee that the nodes in this sector can hear the “hello” message when they enter this sector at a random time and stay there for time duration  $t_n$ . As shown in Fig. 4, the NC TA phase can be pipelined with the RA phase with a delay of  $t_d$ . Note that for the NC BC phase, the length of the “hello”

message is larger than  $t_n/4$  for security reason, which will be explained in the security analysis section.

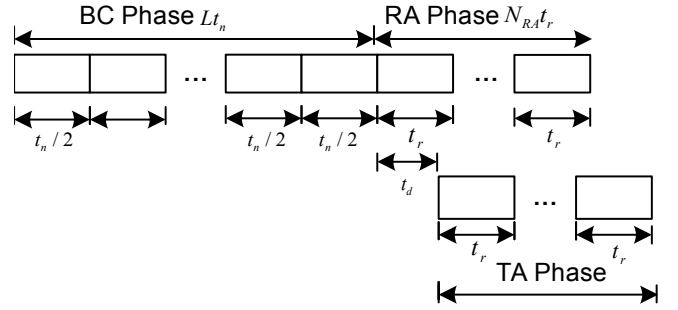


FIGURE 4. Time domain observation of the proposed scheme.

#### A. NC BC PHASE

In this phase, the NC broadcasts its existence to its neighbors in a specific sector by continuously sending “hello” messages. The frame format of the “hello” message is shown in Table 1.

TABLE 1. The BC frame format sent by the NC.

DEVID	$\theta_{NC}$	$T_{NC}$	$T_r$	$t_r$	RA_TIMING	$\sigma_c$	padding
-------	---------------	----------	-------	-------	-----------	------------	---------

The main information body  $M_c$  of the “hello” message contains six fields, namely DEVID,  $\theta_{NC}$ ,  $T_{NC}$ ,  $T_r$ ,  $t_r$  and RA\_TIMING. DEVID is the unique device identification (ID) of the NC.  $\theta_{NC}$  is the sector ID of direction that the NC broadcasts.  $T_{NC}$  denotes the local NC time.  $T_r$  denotes the time that the NC stops broadcasting in the sector and legislate nodes can begin to send response/authentication frame to the NC. The time after  $T_r$  is divided into several slots of length  $t_r$ . In each slot, legislate nodes can send a packet to the NC and wait for the NC's acknowledgment. RA\_TIMING contains information about how network nodes select time slot for frame transmission in the RDMA protocol. Details of the RA\_TIMING fields will be described in Section IV.

The signature  $\sigma_c$  is generated as follows. The NC chooses a random number  $r_c \in \mathbb{Z}_q^*$ , and uses its private key  $x_c$  to compute the signature  $\sigma_c = (R_c, S_c)$  on  $M_c$ , where

$$\begin{cases} R_c = g^{r_c} \bmod p \\ S_c = r_c + x_c \cdot H(R_c || M_c) \bmod q \end{cases} \quad (3)$$

and  $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$  is a secure hash function.

When the node in this specific sector receives the  $M_c || \sigma_c$ , it will first check

$$g^{S_c} \stackrel{?}{=} R_c \cdot Y_c^{H(R_c || M_c)} \bmod p \quad (4)$$

If it holds,  $M_c$  is accepted, otherwise  $M_c$  is rejected, since

$$g^{S_c} = g^{r_c + x_c \cdot H(R_c || M_c)} \quad (5)$$

$$= g^{r_c} \cdot g^{x_c \cdot H(R_c || M_c)} = R_c \cdot Y_c^{H(R_c || M_c)} \bmod p \quad (6)$$



Once  $M_c$  is accepted, the node will record the NC's local time  $T_{NC}$  for clock synchronization, and record  $T_r$ ,  $t_r$  and RA\_TIMING for further communication with the NC.  $\theta_{NC}$  is used to check whether there is a possible wormhole attack.

### B. RA PHASE

After the NC BC phase, the nodes in the specific sector could respond to the "hello" message in two different manners according to two different situations. The first situation is that some nodes in this sector know that they have received frame(s) by observing their received signal strength indicator (RSSI), but they cannot recognize or decode what the frame is. This happens when there exist malicious nodes which replay what they received in the same direction as the NC, as shown in Fig. 2. In this situation, the nodes will respond to the NC and report the existence of malicious nodes with a "response" frame. The second situation is that some nodes in this sector have received the "hello" message without any frame collision. In this situation, the nodes will send an acknowledgement frame to conduct directional authentication with the NC by using an "authentication" frame. Note that this situation does not mean that there is no possible malicious node. Actually, it is then the NC's responsibility to detect whether there are malicious nodes.

The RA frame from the nodes to the NC to report malicious nodes or to authenticate itself is given in Table 2, where the "TYPE" field represents whether this frame is a "response" frame or an "authentication" frame, DEVID represents the unique device ID of node  $N_i$ ,  $\theta_{N_i}$  denotes the direction from node  $N_i$  to the NC, and  $\sigma_c$  is used as the signature of node  $N_i$ . The fields before the signature field  $\sigma_c$  is denoted as the main body  $M_i$  for node  $N_i$ .

TABLE 2. The RA frame format sent by node  $N_i$ .

TYPE	DEVID	$\theta_{N_i}$	$T_{N_i}$	$\sigma_c$	padding
------	-------	----------------	-----------	------------	---------

The signature is generated by node  $N_i$  in the following way. Node  $N_i \in \mathbb{N}$  chooses a random number  $r_i \in \mathbb{Z}_q^*$ , and uses its private key  $x_i$  to compute the signature  $\sigma_i = (R_i, S_i)$  on  $M_i$ , where

$$\begin{cases} R_i = g^{r_i} \bmod p \\ S_i = r_i + x_i \cdot H(R_i || M_i) \bmod q \end{cases} \quad (7)$$

After that, node  $N_i$  returns  $M_i || \sigma_i$  to the NC. In addition, node  $N_i$  can calculate the session key  $sk_{ic} = H(NC || N_i || R_i^{r_i})$ .

Upon receiving  $M_i || \sigma_i$  from  $N_i$ , the NC can verify its validity by checking  $g^{S_i} \stackrel{?}{=} R_i \cdot Y_i^{H(R_i || M_i)} \bmod p$ . If it holds, the NC accepts  $M_i || \sigma_i$ , otherwise rejects it. If  $M_i || \sigma_i$  is accepted, the NC can calculate the same session key  $sk_{ic} = H(NC || N_i || R_i^{r_i})$  to establish an encrypted channel for future communication with node  $N_i$ . The correctness is due to  $R_i^{r_i} = g^{r_i r_c} = R_c^{r_i} \bmod p$ .

When the NC gets the contents of the authentication frame, it will check whether  $|\theta_{NC} - \theta_{N_i}| = L/2$  to see if there is a possible malicious node. After the NC has received either

the response frame or the authentication frame from a node in the sector, it will send back an acknowledgement frame, which has the same frame structure of the RA frame but the DEVID field is replaced with the NC's DEVID. The same contents are sent back to the node to verify that the frame has been successfully received by the NC. Note that the acknowledgement frame is encrypted with the session key  $sk_{ic}$  shared by the NC and node  $N_i$ .

### C. NC TA PHASE

In the above two phases of the proposed SND scheme, most of the wormhole attacks by malicious nodes can be prevented. However, there is still one situation that the malicious node can launch an attack, i.e., most probably the malicious node is near the boundary of the NC's communication range, and the legislate nodes attacked can not hear the broadcast message of the NC, and will not know they have been cheated. To combat the wormhole attack in this situation, in the NC TA phase, the NC will conduct time analysis.

When the NC starts to broadcast its "hello" message, the exact local time  $T_{NC}$  is broadcasted. When neighbor nodes receive the "hello" message, they will use  $T_{NC}$  as their local time. Denote the transmission time from the NC to a node as  $t_{NC2node}$ , the local time difference between the node and the NC is  $t_{NC2node}$ . When the node replies to the NC, it will also send its local time  $T_{NC}$  to the NC, but when the NC receives the RA frame, its local time is actually  $T_{NC} + 2t_{NC2node}$ . The NC can then obtain the time difference of the distant node and itself. The local time of the NC and the node are shown in Table 3.

TABLE 3. Local time of the NC and the node (No attack).

	NC local time	node local time
after BC	$T_{NC} + t_{NC2node}$	$T_{NC}$
after RA	$T_{NC} + 2t_{NC2node}$	$T_{NC}$

TABLE 4. Local time of the NC and the node (With attack).

	NC local time	node local time
after BC	$T_{NC} + t_{NC2node} + T_{rl}$	$T_{NC}$
after RA	$T_{NC} + 2t_{NC2node} + 2T_{rl}$	$T_{NC}$

When there is a malicious node to attack a legislate node outside the communication range of the NC, the legislate node sets its local time to be  $T_{NC}$ , while the local time of the NC is  $T_{NC} + T_{NC2Node} + T_{rl}$ , where  $T_{rl}$  is the relay time of the malicious node and equals the frame transmission time of more than  $T_n/4$ . When the attacked node replies to the NC, their time difference becomes  $T_{NC} + 2T_{NC2Node} + 2T_{rl}$ . The local time of the NC and the node attacked is shown in Table 4.

As reported in [26], there exists some kind of high frequency timers with resolutions of as high as 13 ps, which is enough to detect the time difference listed in the above tables. Thus, it is feasible for the NC to detect the possible malicious nodes by analyzing the time delay.

To see the effectiveness of the time analysis of the NC, Fig. 5 shows the time delay data obtained by the NC for the simulated scenario of Fig. 2. In this simulation, the broadcast frame length is 1000 bit, and the bit rate is 1 Gbps. The time slot for broadcast frame  $t_n = 3 \times 10^{-6}$ , which satisfies the requirement that  $t_n/4 < 1000/10^6 < t_n/2$ . From Fig. 5, it can be seen that when there are malicious nodes that attack victim nodes outside the communication range of the NC, the NC can easily detect the attack by conducting the time analysis.

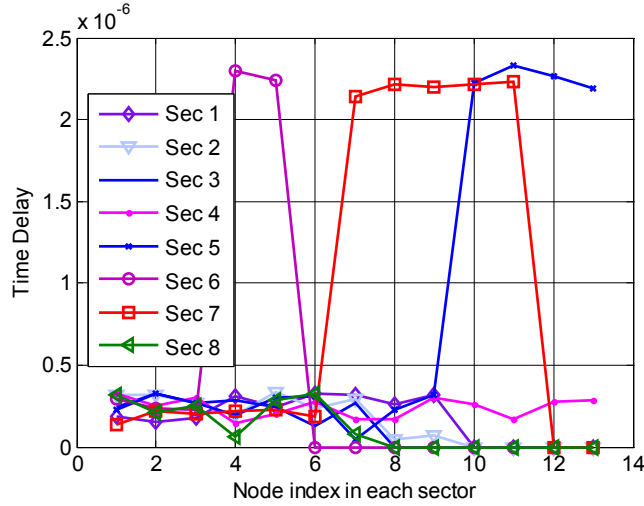


FIGURE 5. Time delay data obtained by the NC.

#### IV. RDMA PROTOCOL

When the RA phase starts, if all the nodes in the specific sector start to transmit RA frames to the NC, it is inevitable that the frames will collide with each other. Thus, in the RA phase, a properly designed scheduling protocol is required to allocate time slot to each node to communicate with the NC successfully. Since all nodes in the same sector will point their antenna toward the same direction, i.e., the NC, it is difficult to implement types of carrier sense multiple access techniques. In this section, we propose the novel RDMA protocol for the nodes to communicate with the NC, and then conduct mathematical analysis and simulation study to optimally select the parameter  $N_{max}^k$  in the protocol. Finally, we discuss optional strategies of the NC on the protocol parameter setting.

Although some random multiple-access algorithms have been proposed and analyzed in literatures, e.g., [27], [28], they assume that the cumulative packet arrival process by busy user is Poisson with intensity  $\lambda_p$  per time slot. Thus, the problem studied here is fundamentally different from those works.

##### A. BACKOFF MECHANISM OF THE RDMA PROTOCOL

The detailed timing of the proposed RDMA protocol is shown in Fig. 6. The whole RA phase is divided into  $M$  periods, and the  $k$ -th period contains  $N_{max}^k$  time slots with slot length of  $t_r$ . When the NC BC finishes and the RA phase starts at time

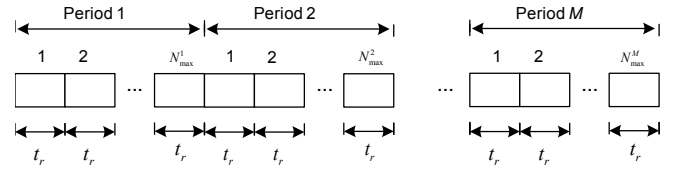


FIGURE 6. Detailed timing of the RDMA protocol in RA phase.

##### Algorithm 1 Backoff Mechanism of the RDMA Protocol

```

BEGIN:
1: Set  $S_{suc} = 0$ ;
2: for  $k=1,2,\dots,M$  do
3:   if ( $S_{suc} == 1$ ) then
4:     break;
5:   else
6:     Generate waiting slot number:  $N_w^k = \text{rand}(N_{max}^k)$ ;
7:     Wait for the  $N_w^k$ -th time slot in period  $k$ ;
8:     Send its frame to the NC;
9:     Wait for ACK frame from the NC until the end of the  $N_w^k$ -th
    time slot;
10:    if (ACK frame is received) then
11:      Set  $S_{suc} = 1$ ;
12:    else
13:      Set  $S_{suc} = 0$ ;
14:    end if
15:  end if
16: end for
END;
```

$T_r$ , each node executes the backoff mechanism of the RDMA protocol, as shown in Algorithm 1.

In the algorithm,  $S_{suc}$  denotes whether a node has successfully sent its RA frame to the NC. When a new period, e.g., period  $k$  starts, if a node has not successfully sent its frame to the NC, it will use the function **rand()** to randomly generate an integer number  $N_w^k$  uniformly distributed from 1 to  $N_{max}^k$ , where  $N_{max}^k$  is the total number of slot in period  $k$  designated by the NC. Then, the node will wait until the  $N_w^k$ -th slot and start to send its frame to the NC. After the node finishes transmission, it will wait for an acknowledgement frame from the NC until the end of the  $N_w^k$ -th slot. If the node has successfully received the acknowledgement frame from the NC, it will set  $S_{suc} = 1$ , which means that it will not send further frame to the NC in the remaining periods of the RA phase. Otherwise, it will set  $S_{suc} = 0$ .

In Algorithm 1, there are two key parameters, namely the number of period,  $M$ , and the number of slot in the  $k$ -th ( $k = 1, 2, \dots, M$ ) period,  $N_{max}^k$ . The two parameters are set by the NC and broadcasted to distant nodes in the “hello” messages. The NC has to decide the optimal values for the two parameters to achieve good scheduling performance. In the following, we will conduct mathematical analysis and simulation to find the optimal values of  $M$  and  $N_{max}^k$ .

##### B. OPTIMAL PARAMETER VALUE FINDING

Suppose that at the end of period  $k$ , the number of nodes that have not been scheduled is  $m_k$ . Then for each slot in period

$k + 1$ , the probability that the slot is selected only by one node is

$$p_1 = \left( \frac{1}{N_{\max}^k} \right) \left( \frac{N_{\max}^k - 1}{N_{\max}^k} \right)^{m_k - 1}. \quad (8)$$

Since there are  $m_k$  nodes at the beginning of period  $k + 1$ , the probability that the slot is successfully scheduled to one node is

$$p_2 = m_k \left( \frac{1}{N_{\max}^k} \right) \left( \frac{N_{\max}^k - 1}{N_{\max}^k} \right)^{m_k - 1}. \quad (9)$$

Because each node independently generates its random waiting slot number  $N_w^k$ , the probability  $p_2$  for all the time slots in period  $k$  is the same. Then, the number of the expected successfully scheduled nodes in period  $k + 1$  is

$$\Delta_{m_k} = m_k \left( \frac{N_{\max}^k - 1}{N_{\max}^k} \right)^{m_k - 1}. \quad (10)$$

Then, we can have the iterative relationship of  $m_k$  at two consequent periods:

$$m_{k+1} = m_k - \Delta_{m_k}. \quad (11)$$

Denote the number of nodes at the beginning of the RA phase as  $m_0$ . The expected value of  $m_0$  equals the average number  $N_{nd}$  of legislated nodes in the specific sector. Since the node density of legislature nodes is  $\rho$ , we have

$$m_0 = N_{nd} = \rho \pi R^2 / L. \quad (12)$$

To find the optimal value of  $N_{\max}^k$ , we examine the physical meaning of  $\Delta_{m_k}$ , which denotes the number of the successfully scheduled nodes in period  $k$ . The objective of the scheduling is to achieve the maximum number of successfully scheduled nodes in each slot, which is:

$$\frac{\Delta_{m_k}}{N_{\max}^k} = m_k \frac{(N_{\max}^k - 1)^{m_k - 1}}{N_{\max}^k}. \quad (13)$$

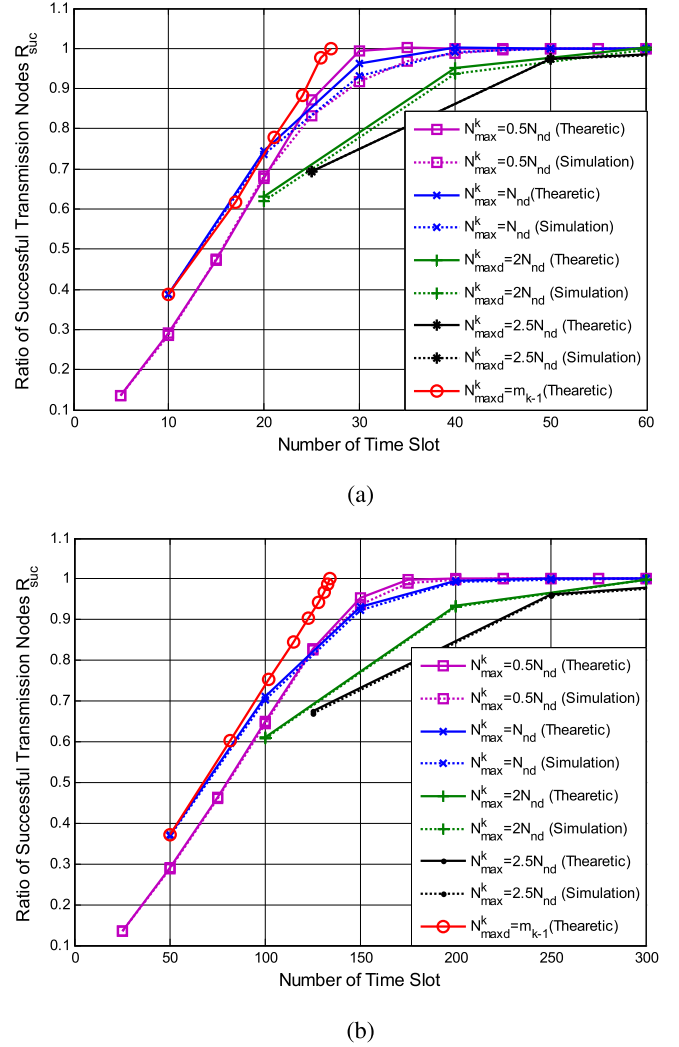
Set  $\frac{d}{dN_{\max}^k} \left( \frac{\Delta_{m_k}}{N_{\max}^k} \right) = 0$ , we have

$$(m_k - 1)N_{\max}^k = m_k(N_{\max}^k - 1). \quad (14)$$

Therefore, we have

$$N_{\max}^k = m_k, \quad (15)$$

i.e., the optimal value of the slot number in period  $k$  equals the expected number of nodes that have not been scheduled at the beginning of the period. In Fig. 7, we plot the ratio of successful transmission nodes,  $R_{suc}$ , when using equal and adaptive  $N_{\max}^k$  in successive periods in the RA phase. Fig. 7(a) and Fig. 7(b) are results for different number of nodes at the beginning of the RA phase in the interested antenna sector, namely  $N_{nd} = 10$  and  $N_{nd} = 50$ , respectively. In each subfigure, simulation results and theoretical results of  $R_{suc}$  for equal  $N_{\max}^k$  in successive period are plotted, where  $N_{\max}^k$  is independent of period  $k$ . Each of the simulation results is obtained by averaging 1000 Monte Carlo simulations. For comparison, the theoretical results of using adaptive slot



**FIGURE 7. Ratio of successful transmission nodes  $R_{suc}$  for different  $N_{\max}^k$  in successive periods of the RA phase. (a) Ratio of successful transmission nodes  $R_{suc}$  with  $N_{nd} = 10$ . (b) Ratio of successful transmission nodes  $R_{suc}$  with  $N_{nd} = 50$ .**

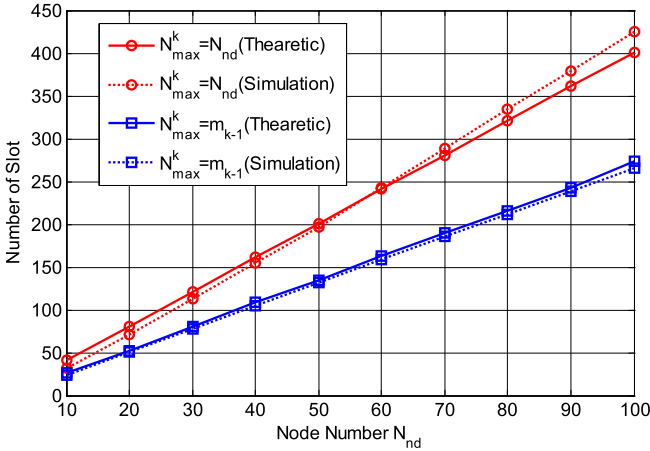
numbers in successive periods are also plotted in each subfigure.

It can be seen from Fig. 7 that for the case that equal  $N_{\max}^k$  is used in successive periods, the simulation results matches the theoretical results very well in both the subfigures. This indicates that (10) is correct. In addition, it can be seen that when equal  $N_{\max}^k$  is used in successive periods, setting  $N_{\max}^k = N_{nd}$  achieves the best scheduling performance, where the convergence of  $R_{suc}$  to unit is the fastest.

Further more, from Fig. 7, in comparison with the case of using equal  $N_{\max}^k$  in successive periods, adaptively using different  $N_{\max}^k$  in successive periods can have much better scheduling performance when considering the convergence time of  $R_{suc}$ . The time slots required when using adaptive  $N_{\max}^k$  is much less than that of using equal  $N_{\max}^k$  in successive periods.

To further verify that using adaptive slot numbers in successive periods is better than using equal slot

number, in Fig. 8, we plotted the number of slots required for successful transmission of all  $N_{nd}$  nodes in an interested sector in the RA phase versus the number of nodes  $N_{nd}$ . The curves marked with circles are results when using equal slot number  $N_{max}^k = N_{nd}$ , while the curves marked with squares are that using adaptive slot number  $N_{max}^k = m_k$ . The simulation results are obtained by averaging 1000 Monte Carlo simulations. It is seen that the simulation results match well with the theoretical results, which validates (10) again. From this figure, using adaptive slot number  $N_{max}^k = m_k$  can save approximately 30% of the total number of time slots in the RA phase in comparison with the case of using equal number of slots.



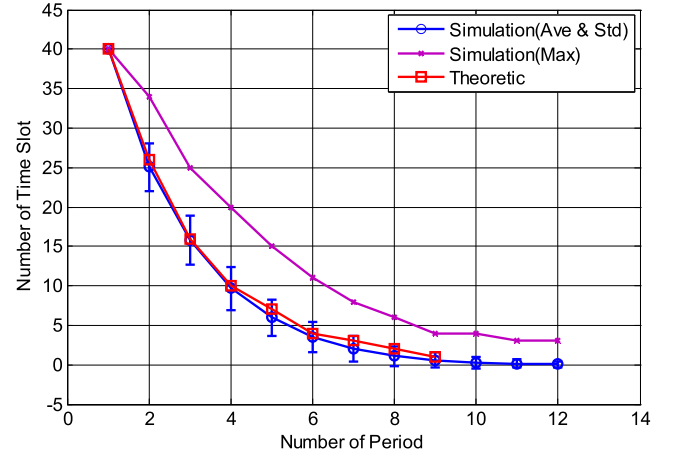
**FIGURE 8.** Number of slots required for successful transmission of all nodes in an interested sector.

### C. NC'S STRATEGIES

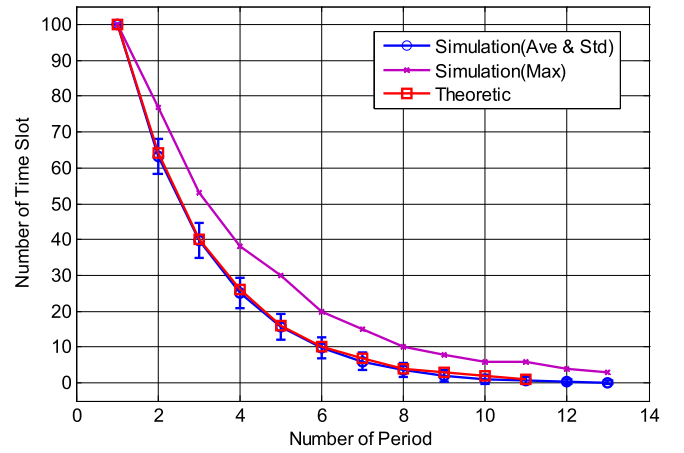
In the above subsection, we have shown by theoretical analysis and simulation that, the optimal value of the number of slots used in periods of the RA phase is  $N_{max}^k = m_k$ . However, in the network shown in Fig. 1, it is impractical for nodes in a specific sector to know the total number of nodes  $N_{nd}$ . Thus, it is the responsibility of the NC to broadcast the strategies that how many periods  $M$  are allowed in the RA phase and in each period how many time slots are allocated to the nodes. In the following, we investigate the strategies of the NC to set up proper values of  $M$  and  $N_{max}^k$ .

For a given value of  $N_{nd}$ , the NC can theoretically calculate the value of  $M$  and  $N_{max}^k$  by using Algorithm 2, where  $N_{RA}$  denotes the number of total slots in the RA phase, and the function `ceil()` rounds its input to the nearest integers towards infinity. In each step of the WHILE loop, the number of remaining unscheduled nodes  $m_k$  is calculated by using (10) and (11). Every time the period number  $M$  increases, the number of total slot  $N_{RA}$  is accumulated. The close of the WHILE loop means that only one more period with one time slot is needed to schedule all the nodes.

<sup>1</sup>In this algorithm, some Matlab system functions are invoked: `rand()`, `find()`, `size()`, `sum()`, `std()`, and `max()`. For their operations, please refer to the Matlab help file.



(a)



(b)

**FIGURE 9.** Number of time slots used in successive periods in RA phase. (a) Number of time slots used in successive periods in RA phase with  $N_{nd} = 40$ . (b) Number of time slots used in successive periods in RA phase  $N_{nd} = 100$ .

The NC can also get the statistical values of  $M$  and  $N_{max}^k$  by using Algorithm 3, where  $N_{sim}$  denotes the total Monte Carlo simulation rounds,  $N_{slot}(S_{ind}, k)$  records the slot number used in period  $k$  in the  $S_{ind}$ -th round of simulation.  $N_{Ave}(k)$ ,  $N_{Std}(k)$ , and  $N_{Max}(k)$  denote the average, standard deviation and maximum value of slot number in period  $k$  of the RA phases, respectively.

By using Algorithms 2 and 3, with a given  $N_{nd}$ , the NC can get the number of time slots in successive periods in a RA phase for the nodes in a specific sector. In Fig. 9(a) and Fig. 9(b), we plot the number of time slots used in different periods with  $N_{nd} = 40$  and  $N_{nd} = 100$ , respectively. From Fig. 9, it can be seen that for a given  $N_{nd}$ , the average value of  $N_{max}^k$  obtained by simulation roughly equals the corresponding theoretical value for every period, and both of them are smaller than the corresponding maximum values obtained by using Monte Carlo method.



**Algorithm 2** Theoretical Calculation of  $M$  and  $N_{max}^k$  With Given  $N_{nd}$

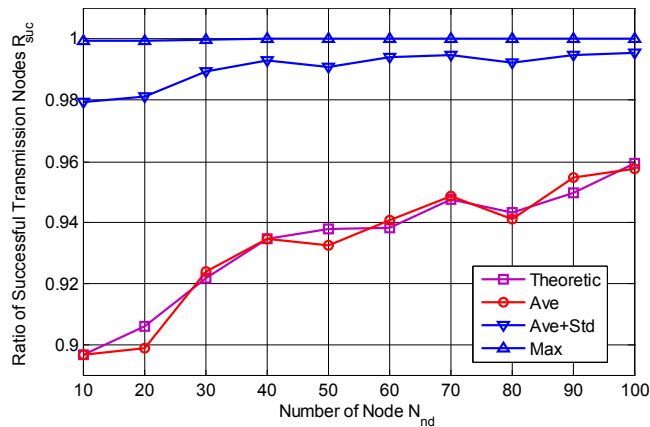
```

BEGIN:
1: Set  $k = 1$ ;
2: Set  $N_{RA} = 0$ ;
3: Set  $N_{max}^k = N_{nd}$ ;
4: Set  $M = 0$ ;
5: Set  $m_k = N_{nd}$ ;
6: while  $N_{max}^k \geq 1$  do
7:   SET  $M = M + 1$ ;
8:   SET  $N_{RA} = N_{RA} + N_{max}^k$ ;
9:   SET  $m^{k+1} = m^k (1 - (\frac{N_{max}^k - 1}{N_{max}^k})^{m^k - 1})$ 
10:  SET  $N_{max}^{k+1} = \text{ceil}(N_{nd}^{k+1})$ ;
11:  SET  $k = k + 1$ ;
12: end while
13: SET  $M = M + 1$ ;
14: SET  $N_{RA} = N_{RA} + 1$ ;
15: SET  $N_{max}^k = 1$ ;
END;

```

Therefore, it is important to determine the value of  $M$  and  $N_{max}^k$ . First, we can calculate the  $N_{nd}$  from the node density  $\rho$  and the size of the sector area by (12). Then, three strategies can be used to determine the value of  $M$  and  $N_{max}^k$ :

- 1) Strategy 1: Using Algorithm 2 to calculate the value of  $M$  and  $N_{max}^k$ ;
- 2) Strategy 2: Using the same value of  $M$  as in strategy 1, and setting  $N_{max}^k = N_{Ave}(k) + N_{Std}(k)$  ( $k = 1, 2, \dots, M$ );
- 3) Strategy 3: Using the same value of  $M$  as in strategy 1, and setting  $N_{max}^k = N_{Max}(k)$  ( $k = 1, 2, \dots, M$ ).



**FIGURE 10.** Ratio of successful transmission nodes  $R_{suc}$ .

Note that different strategies have different scheduling performance, along with different computational complexity for the NC. To investigate the scheduling performance of different strategies, in Fig. 10, we plot the ratio of successful transmission nodes  $R_{suc}$  versus different  $N_{nd}$  when the three different strategies are used by the NC. The results of using  $N_{max}^k = N_{Ave}(k)$  are also shown in this figure, and its performance is at the same level of strategy 1. In Fig. 10, all the results are

**Algorithm 3** Calculation of  $M$  and  $N_{max}^k$  With Given  $N_{nd}$  by Using Monte Carlo Method

```

BEGIN:
1: SET  $N_{sim} = 1000$ ;
2: for  $S_{ind}=1:1:N_{sim}$  do
3:   SET  $k = 1$ ;
4:   SET  $m_k = N_{nd}$ ;
5:   SET  $N_{max}^k = N_{nd}$ ;
6:   while  $m_k > 0$  do
7:     SET  $N_{slot}(S_{ind}, k) = N_{max}^k$ ;
8:     for  $i=1:1:N_{max}^k$  do
9:       SET  $I_{slot}(i) = \text{ceil}^1(N_{max}^k \text{ rand}());$ 
10:    end for
11:    SET  $M_{slot}(1 : N_{max}^k) = 1$ ;
12:    for  $i=1:1:N_{max}^k$  do
13:      for  $j=i+1:1:N_{max}^k$  do
14:        if  $I_{slot}(i) == I_{slot}(j)$  then
15:          SET  $M_{slot}(i) = 0$ ;
16:          SET  $M_{slot}(j) = 0$ ;
17:        end if
18:      end for
19:    end for
20:    SET  $m_{k+1} = m_k - \text{size}(\text{find}(M_{slot} \neq 0))$ ;
21:    SET  $k = k + 1$ ;
22:  end while
23: end for
24: for  $k=1:1:M$  do
25:   SET  $N_{Ave}(k) = \text{sum}(N_{slot}(:, k)) / N_{sim}$ ;
26:   SET  $N_{Std}(k) = \text{std}(N_{slot}(:, k))$ ;
27:   SET  $N_{Max}(k) = \text{max}(N_{slot}(:, k))$ ;
28: end for
END;

```

obtained by averaging 1000 Monte Carlo simulations. It is seen that with strategy 3,  $R_{suc}$  always equals unit, indicating that in all Monte Carlo simulations, all nodes in the interested sector can be successfully scheduled to transmit their frames. Thus, strategy 3 is the best one when only considering the scheduling performance. For comparison, strategy 2 keeps  $R_{suc}$  between 0.98 to 0.995 when  $N_{nd}$  varies from 10 to 100, and has the medium scheduling performance among the three strategies. With strategy 1,  $R_{suc}$  varies from 0.89 to 0.96. The lowest ratio and the rapid variation over  $N_{nd}$  make strategy 1 the worst strategy in terms of scheduling performance. For the NC, the computational complexity of strategies 2 and 3 are much higher than strategy 1.

To further compare the delay of the three strategies, the normalized number of total time slots required in the RA phase are shown in Fig. 11. Note that the number  $N_{norm}$  is normalized to the corresponding value of  $N_{nd}$  to give a more meaningful and intuitive comparison. It can be seen that strategy 1 requires the least normalized number of total time slots and strategy 3 requires the largest normalized number of total time slots. Therefore, if better scheduling performance is required, much more total time slots are required. The NC can select the strategy by considering the scheduling performance requirements and the total slots required. Generally, when discovery of all nodes is required, the NC can use strategy 3, otherwise, the NC is recommended to use strategy 2 by jointly

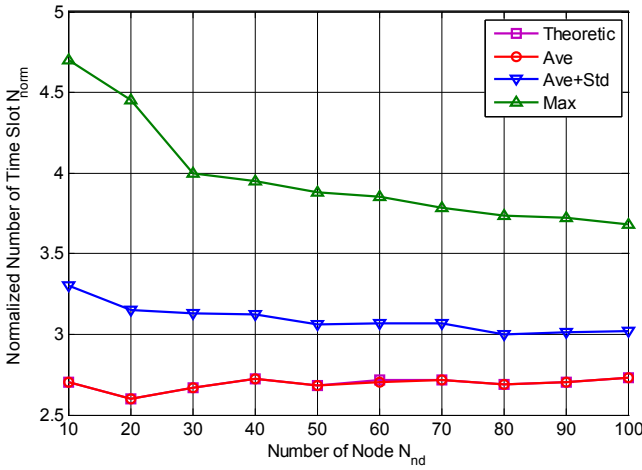


FIGURE 11. Total number of time slots in a RA phase.

considering the scheduling performance and the total time slots required.

## V. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed SND scheme.

First, when the NC broadcasts the “hello” messages to the nodes and when the nodes response/authenticate with the NC, they use their signatures to guarantee the data integrity and establish their session keys. In this way, in the NC BC phase and the RA phase, the attacker can not modify the data, and further more, after the two phases, the attacker can not even know what they are talking about.

Second, by using the directional authentication, the potentially attacked region by malicious nodes is significantly reduced. In the BC phase, the NC broadcasts its direction  $\theta_{NC}$ , and in the RA phase, the node reports its direction  $\theta_{N_i}$ , then the NC can check whether  $|\theta_{NC} - \theta_{N_i}| = L/2$ . In this way, if a malicious node wants to launch a wormhole attack to its neighbor, it can only attack the node in the same direction of  $\theta_{NC}$  rather than nodes in all the directions around it.

Third, by carefully designing the length of the time slot and broadcast frame length in the BC phase, most of the malicious nodes will be detected when they launch the wormhole attack if they are not near the circular communication range boundary. As shown in Fig. 4, the broadcast frame is transmitted every  $T_n/2$  with a frame length of longer than  $T_n/4$ . In this way, if a malicious node launches the wormhole attack when there are legitimate nodes falling in both the communication range of the NC and the malicious node, the legitimate nodes will detect the attack because the malicious node has no chance to relay a frame without collision with the broadcast frames from the NC.

Finally, the NC time analysis prevents the remaining possible wormhole attacks. The security analysis above indicates that only malicious nodes, which attack legitimate nodes outside the circular communication region where the NC's

broadcast can not be heard, can launch the wormhole attack. However, the NC time analysis can easily detect these malicious nodes by analyzing the timing information in the TA phase.

## VI. NEIGHBOR DISCOVERY TIME ANALYSIS

In this section, we conduct neighbor discovery time analysis of the proposed SND scheme with the RDMA protocol.

As shown in Fig. 4, the proposed SND scheme contains three phases, namely the NC BC phase, the RA phase and the NC TA phase when the NC stays in a specific sector. Since totally there are  $L$  sectors in the whole region, the total neighbor discovery time is:

$$T_{SND} = L(T_{BC} + T_{RA} + T_{TA}), \quad (16)$$

where  $T_{BC}$ ,  $T_{RA}$  denote the time of the NC BC phase and the RA phase, respectively, and  $T_{TA}$  denotes the extra time caused by the NC TA phase. From Fig. 4,  $T_{BC} = Lt_n$ ,  $T_{RA} = N_{RA}t_r$  and  $T_{TA} = t_d$ . From Fig. 11, the total number in a RA phase can be written as:

$$N_{RA} = N_{norm}N_{nd} \quad (17)$$

So (16) becomes

$$T_{SND} = L(Lt_n + N_{norm}\rho\pi R^2t_r/L + t_d). \quad (18)$$

As discussed in Section II, the maximum reachable distance  $R$  from the NC to its surrounding nodes depends on the number of sector  $L$ . According to (1), when both the transmitter and the receiver use directional antennas, the antenna gain is:

$$G_R = G_T = LG_0, \quad (19)$$

where  $G_0$  is the antenna gain of omni-directional antennas.

From (2), we have

$$P_{R_{th}} = k_1L^2G_0^2R^{-\alpha}P_T. \quad (20)$$

Thus, the relationship between  $R$  and  $L$  can be written as

$$R = KL^{\frac{2}{\alpha}} \quad (21)$$

where  $K = \left(\frac{k_1G_0^2P_T}{P_{R_{th}}}\right)^{\frac{1}{\alpha}}$ . Then, we have

$$T_{SND} = t_nL^2 + N_{norm}\rho\pi L^{\frac{4}{\alpha}}K^2t_r + t_dL. \quad (22)$$

When  $\alpha = 2$ , i.e.,  $R = KL$ ,

$$T_{SND} = t_nL^2 + N_{norm}\rho\pi L^2K^2t_r + t_dL. \quad (23)$$

The first item  $t_nL^2$  denotes the total NC BC time, and it is proportional to the square of the sector number  $L$ . The second item  $N_{norm}\rho\pi L^2K^2t_r$  is the total RA time for nodes to authenticate with the NC, and it is proportional to the square of  $L$  and the node density  $\rho$ . The last item  $t_dL$  increases linearly with  $L$ . Since  $t_d$  is much smaller than  $t_n$  and  $t_r$ , the last item contributes little to the total neighbor discovery time.

Besides the total neighbor discovery time, the average time for a node to be discovered is also an important parameter.

Since the total number of nodes presenting in the range  $R$  is  $\rho\pi K^2 L^{\frac{4}{\alpha}}$ , the average time for a node to be discovered by the NC is

$$T_{A\_SND} = \frac{t_n}{\rho L^{\frac{4}{\alpha}-2}\pi K^2} + N_{norm}t_r + \frac{t_d}{\rho\pi L^{\frac{4}{\alpha}-1}K^2} \quad (24)$$

When  $\alpha = 2$ ,

$$T_{A\_SND} = \frac{t_n}{\rho\pi K^2} + N_{norm}t_r + \frac{t_d}{\rho\pi K^2 L}. \quad (25)$$

The first item  $\frac{t_n}{\rho\pi K^2}$  is the average BC time, and is inversely proportional to the node density  $\rho$ . The second item  $N_{norm}t_r$  can be regarded as a constant when the NC's strategy is selected. The last item is also inversely proportional to the node density  $\rho$ . Thus, the average time per node decreases with the node density, which indicates that the proposed neighbor discovery scheme is suitable for networks with high node density.

## VII. CONCLUSION

In this paper, we have proposed a wormhole attack resistant SND scheme. By using antenna direction information, transmission time information and carefully designed broadcast frame length, the proposed SND scheme can effectively prevent and detect wormhole attack, which has been demonstrated by security analysis and simulation. In addition, we have introduced the RDMA protocol to effectively solve the transmission collision problem when there are many nodes transmitting frames to the NC without knowing each other and unable to listen to each other limited by directional antennas. Our work is valuable since the security requirements are ever-increasing for the 60 GHz network with directional antenna, especially in some outdoor application scenarios. In our future work, we will consider how to identify the security problem in neighbor discovery of ad hoc 60 GHz networks by extending the scheme and protocol proposed in this paper.

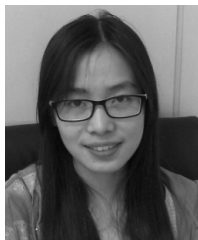
## REFERENCES

- [1] Z. Shi, R. Lu, J. Qiao, and X. Shen, "Snd: Secure neighbor discovery for 60 ghz network with directional antenna," in *Proc. IEEE WCNC*, Feb. 2013, pp. 1–6.
- [2] R. Daniels and R. Heath, "60 ghz wireless communications: Emerging requirements and design recommendations," *IEEE Veh. Technol. Mag.*, vol. 2, no. 3, pp. 41–50, Sep. 2007.
- [3] J. Foerster, J. Lansford, J. Laskar, T. Rappaport, and S. Kato, "Realizing Gbps wireless personal area networks-guest editorial," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 8, pp. 1313–1317, Oct. 2009.
- [4] Z. Shi, R. Lu, J. Chen, and X. S. Shen, "Three-dimensional spatial multiplexing for directional millimeter-wave communications in multi-cubicle office environments," in *Proc. Globecom*, 2013, pp. 1–6.
- [5] A. Myles and R. de Vegt, (Mar. 2008). *Wi-Fi Alliance (WFA) VHT Study Group Usage Models* [Online]. Available: <https://mentor.ieee.org/802.11/dcn/07/11-07-2988-04-0000-liaison-from-wi-fi-allian-to-802-11-regarding-wfa-vht-study-group-consolidation-of-usage-models.ppt>
- [6] H. Singh, S. Yong, J. Oh, and C. Ngo, "Principles of IEEE 802.15.3c: Multigigabit millimeter-wave wireless PAN," in *Proc. 18th IEEE Int. Conf. Comput. Commun. Netw.*, Aug. 2009, pp. 1–6.
- [7] T. Baykas, C. Sum, Z. Lan, J. Wang, M. Rahman, H. Harada, and S. Kato, "IEEE 802.15.3c: The first IEEE wireless standard for data rates over 1 Gb/s," *IEEE Commun. Mag.*, vol. 49, no. 7, pp. 114–121, Jul. 2011.
- [8] C. Cordeiro, D. Akhmetov, and M. Park, "Ieee 802.11 ad: Introduction and performance evaluation of the first multi-gbps wifi technology," in *Proc. ACM Int. Workshop mmWave Commun., Circuits Netw.*, 2010, pp. 3–8.
- [9] X. An, R. Prasad, and I. Niemegeers, "Neighbor discovery in 60 Ghz wireless personal area networks," in *Proc. IEEE Int. Symp. World Wireless Mobile Multimedia Netw.*, Jun. 2010, pp. 1–8.
- [10] L. X. Cai, L. Cai, X. Shen, and J. Mark, "Resource management and QoS provisioning for IPTV over mmwave-based WPANs with directional antenna," *Mobile Netw. Appl.*, vol. 14, no. 2, pp. 210–219, Apr. 2009.
- [11] L. X. Cai, L. Cai, X. Shen, and J. Mark, "Rex: A randomized exclusive region based scheduling scheme for mmwave WPANs with directional antenna," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 113–121, Jan. 2010.
- [12] J. Qiao, L. X. Cai, X. Shen, and J. W. Mark, "Enabling multi-hop concurrent transmissions in 60 GHz wireless personal area networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3824–3833, Nov. 2011.
- [13] R. Sun, Z. Shi, R. Lu, J. Qiao, and X. Shen, "A lightweight key management scheme for 60 GHz WPAN," in *Proc. WCSP*, Oct. 2012, pp. 1–6.
- [14] S. Vasudevan, J. Kurose, and D. Towsley, "On neighbor discovery in wireless networks with directional antennas," in *Proc. 24th Annu. Joint Conf. IEEE INFOCOM*, vol. 4, Mar. 2005, pp. 2502–2512.
- [15] X. An, R. Prasad, and I. Niemegeers, "Impact of antenna pattern and link model on directional neighbor discovery in 60 GHz networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 5, pp. 1435–1447, May 2011.
- [16] J. Ning, T. Kim, S. Krishnamurthy, and C. Cordeiro, "Directional neighbor discovery in 60 GHz indoor wireless networks," *Perform. Evaluation*, vol. 68, no. 9, pp. 897–915, 2011.
- [17] P. Papadimitratos, M. Poturlalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J. Hubaux, "Secure neighborhood discovery: A fundamental element for mobile ad hoc networking," *IEEE Commun. Mag.*, vol. 46, no. 2, pp. 132–139, Feb. 2008.
- [18] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. Netw. Distrib. Syst. Security Symp.*, Feb. 2004, pp. 1–11.
- [19] 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.
- [20] R. Lu, X. Lin, T. 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. 1–16, Jan. 2011.
- [21] J. Du, E. Kranakis, and A. Nayak, "Cooperative neighbor discovery protocol for a wireless network using two antenna patterns," in *Proc. 32nd IEEE Int. Conf. Distrib. Comput. Syst. Workshops*, Jun. 2012, pp. 178–186.
- [22] R. Zhao, A. Wen, Z. Liu, and J. Yang, "A trustworthy neighbor discovery algorithm for pure directional transmission and reception in MANET," in *Proc. IEEE 9th Int. Conf. Adv. Commun. Technol.*, vol. 2, Feb. 2007, pp. 926–931.
- [23] H. Park, Y. Kim, I. Jang, and S. Pack, "Cooperative neighbor discovery for consumer devices in mmwave ad-hoc networks," in *Proc. IEEE Int. Conf. Consum. Electron.*, Jan. 2012, pp. 100–101.
- [24] R. Mudumbai, S. Singh, and U. Madhow, "Medium access control for 60 GHz outdoor mesh networks with highly directional links," in *Proc. IEEE INFOCOM*, Apr. 2009, pp. 2871–2875.
- [25] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Proc. Adv. Cryptol.*, 1985, pp. 10–18.
- [26] J. Jansson, A. Mantyniemi, and J. Kostamovaara, "A delay line based CMOS time digitizer IC with 13 ps single-shot precision," in *Proc. IEEE ISCAS*, May 2005, pp. 4269–4272.
- [27] L. Georgiadis, L. Merakos, and P. Papantoni-Kazakos, "A method for the delay analysis of random multiple-access algorithms whose delay process is regenerative," *IEEE J. Sel. Areas Commun.*, vol. 5, no. 6, pp. 1051–1062, Jul. 1987.
- [28] A. Burrell and P. Papantoni-Kazakos, "Random access algorithms in packet networks—a review of three research decades," *Int. J. Commun. Netw. Syst. Sci.*, vol. 5, no. 10, pp. 691–707, 2012.



**ZHIGUO SHI** (M'10) received the B.S. and Ph.D. degrees in electronic engineering from Zhejiang University, Hangzhou, China, in 2001 and 2006, respectively. From 2006 to 2009, he was an Assistant Professor with the Department of Information and Electronic Engineering, Zhejiang University, where currently he is an Associate Professor. From September 2011, he begins a two-year visit with the Broadband Communications Research Group, University of Waterloo, Waterloo, ON, Canada.

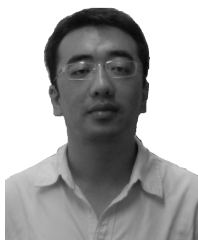
His current research interests include radar data and signal processing, wireless communication, and security. He received the Best Paper Award of the IEEE WCNC in 2013, Shanghai, China, and the IEEE WCSP in 2012, Huangshan, China. He received the Scientific and Technological Award of Zhejiang, China, in 2012. He serves as an Editor of the *KSII Transactions on Internet and Information Systems*. He serves as TPC member for IEEE VTC in 2013, the IEEE ICC in 2013, MSN in 2013, IEEE INFOCOM in 2014, IEEE ICNC in 2014.



**RUIXUE SUN** received the B.Sc degree in communication engineering, Xi'an University, Xi'an, China, in 2012. She is currently pursuing the master's degree with the Department of Information and Electronic Engineering, Zhejiang University, Hangzhou, China. Her current research interests include security and privacy in millimeter wave communication and smart grid.



**RONGXING LU** (M'10) Rongxing Lu received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China in 2006, and the Ph.D. degree (with Governor General's Gold Medal) in electrical and computer engineering from the University of Waterloo, Canada in 2012. He is currently an assistant professor at School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. His research interests include wireless network security, applied cryptography, trusted computing, and target tracking.



**JIAN QIAO** received the B.E. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2006, and the M.A.Sc. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2010. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo. His current research interests include millimeter wave WPANs, medium access control, resource management, and smart grid networks.



**JIMING CHEN** (M'08–SM'11) received the B.Sc. and Ph.D. degrees in control science and engineering from Zhejiang University, Hangzhou, China, in 2000 and 2005, respectively. He was a Visiting Researcher with INRIA in 2006, the National University of Singapore, Singapore, in 2007, and University of Waterloo, Waterloo, ON, Canada, from 2008 to 2010. Currently, he is a Full Professor with the Department of Control Science and Engineering, and the Coordinator of Group of

Networked Sensing and Control, State Key laboratory of Industrial Control Technology, the Vice Director of Institute of Industrial Process Control, Zhejiang University. He currently serves an Associate Editor for several international journals, including the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM, the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, the *IEEE Network*, *IET Communications*. He was a Guest Editor of the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, *Computer Communication* (Elsevier), *Wireless Communication and Mobile Computer* (Wiley), and *Journal of Network and Computer Applications* (Elsevier). He served/serves as an Ad hoc and Sensor Network Symposium Co-Chair, the IEEE Globecom in 2011, General Symposia Co-Chair of ACM IWCMC in 2009 and ACM IWCMC in 2010, WiCON in 2010 MAC Track Co-Chair, IEEE MASS in 2011 Publicity Co-Chair, the IEEE DCOSS in 2011 Publicity Co-Chair, IEEE ICDCS in 2012 Publicity Co-Chair, IEEE ICC in 2012 Communications QoS and Reliability Symposium Co-Chair, the IEEE SmartGridComm The Whole Picture Symposium Co-Chair, the IEEE ASS in 2013 Local Chair, Wireless Networking and Applications Symposium Co-Chair, IEEE ICC in 2013 and TPC Member for IEEE ICDCS in 2010, 2012, and 2013, the IEEE MASS in 2010, 2011, 2013, the IEEE SECON in 2011 and 2012, the IEEE INFOCOM from 2011 to 2013.



**XUEMIN SHEN** (M'97–SM'02–F'09) received the B.Sc.(1982) degree from Dalian Maritime University, Dalian, China, and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Brunswick, NJ, USA, all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. His current

research interests include resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, vehicular ad hoc, and sensor networks. He is the co-author and editor of six books, and has published more than 600 papers, and book chapters in wireless communications and networks, control, and filtering. He served as the Technical Program Committee Chair for IEEE VTC in 2010, the Symposia Chair for IEEE ICC in 2010, the Tutorial Chair for IEEE VTC in 2011 and the IEEE ICC in 2008, the Technical Program Committee Chair for IEEE Globecom in 2007, the General Co-Chair for Chinacom in 2007 and QShine in 2006, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He serves/served as the 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 the Guest Editor for the *IEEE JSAC*, *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 from the University of Waterloo in 2004, 2007, and 2010, the Premier's Research Excellence Award from the Province of Ontario, Canada, in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, in 2002 and 2007. 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 Society and Communications Society.