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

Zhiguo Shi, Member, IEEE, Ruixue Sun, Rongxing Lu, Member, IEEE, Jian Qiao, Jiming Chen, Senior Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE

Abstract—In this paper, we propose a wormhole attack resistant secure neighbor discovery (SND) scheme for a centralized 60 GHz directional wireless network. In specific, 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 legislate network nodes, which can prevent most of the wormhole attacks. In the NC time analysis phase, the NC can further detect the possible attack by 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 \( \Delta t \) periods, within which the unsuccessfully transmitting nodes randomly select a time slot to transmit. The optimal parameter setting of the RDMA protocol and the optimal 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.

1 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 legislate 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 cannot listen to the others’ transmissions due to the limitation of directional antenna.
- Third, we conduct extensive secure analysis and neighbor discovery 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.

## 2 Problem Formulation

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

### 2.1 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 $N = \{N_1, N_2, N_3, \cdots\}$ and a single NC, which may be an access point (AP) in 802.11.ad-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 angel 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.

![Fig. 1: Network model under consideration](image_url)

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:

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

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]:

$$P_R = k_1 G_T G_R d^{-\alpha} P_T,$$

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...
2.2 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.

2.3 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 $Y_c = g^{x_c} \mod p$; 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.

3 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 $R$.
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.

![Flow chat of the proposed SND scheme](image)

![Time domain observation of the proposed scheme](image)

### 3.1 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>
<thead>
<tr>
<th>DEVID</th>
<th>$\theta_{NC}$</th>
<th>$T_{NC}$</th>
<th>$T_r$</th>
<th>$t_r$</th>
<th>$\text{RA}_r\text{TIMING}$</th>
<th>$\sigma_r$</th>
<th>padding</th>
</tr>
</thead>
</table>

The main information body $M_r$ of the "hello" message contains six fields, namely DEVID, $\theta_{NC}$, $T_{NC}$, $T_r$, $t_r$ and $\text{RA}_r\text{TIMING}$. 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 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, 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 $\sigma_r$ is generated as follows. The NC chooses a random number $r_c \in Z_q^*$, and uses its private key $x_c$ to compute the signature $\sigma_c = (R_c, S_c)$ on $M_c$, where

\[
R_c = g^{r_c} \mod p \\
S_c = r_c + x_c \cdot H(R_c || M_c) \mod q
\]

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

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

\[
g^{S_c} = R_c \cdot Y_c^H(R_c || M_c) \mod p
\]

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

\[
g^{S_c} = g^{r_c + x_c \cdot H(R_c || M_c)} = g^{r_c} \cdot g^{x_c \cdot H(R_c || M_c)} = R_c \cdot Y_c^H(R_c || M_c) \mod p
\]

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.

### 3.2 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, 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 $\sigma_r$ is used as the signature of node $N_i$. The fields before the signature field $\sigma_r$ is denoted as the main body $M_i$ for node $N_i$.

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DEVID</th>
<th>$\theta_{N_i}$</th>
<th>$T_{N_i}$</th>
<th>$\sigma_r$</th>
<th>padding</th>
</tr>
</thead>
</table>

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

\[
R_i = g^{r_i} \mod p \\
S_i = r_i + x_i \cdot H(R_i || M_i) \mod q
\]

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

### Table 1: The BC Frame Format Sent by the NC

<table>
<thead>
<tr>
<th>DEVID</th>
<th>$\theta_{NC}$</th>
<th>$T_{NC}$</th>
<th>$T_r$</th>
<th>$t_r$</th>
<th>$\text{RA}_r\text{TIMING}$</th>
<th>$\sigma_r$</th>
<th>padding</th>
</tr>
</thead>
</table>

### Table 2: The RA Frame Format Sent by Node $N_i$

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DEVID</th>
<th>$\theta_{N_i}$</th>
<th>$T_{N_i}$</th>
<th>$\sigma_r$</th>
<th>padding</th>
</tr>
</thead>
</table>

Copyright (c) 2013 IEEE. Personal use is permitted. For any other purposes, permission must be obtained from the IEEE by emailing pubs-permissions@ieee.org.
Upon receiving $M_i||\sigma_i$ from $N_i$, the NC can verify its validity by checking $g^{\sigma_i} = R_i \cdot Y_i^{H(R_i||M_i)} \text{mod}~p$. 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 $sk_{ic} = H(\{NC||N_i||R_i^c\})$ to establish an encrypted channel for future communication with node $N_i$. The correctness is due to $R_i^c = g^{sr_c} = R_i^c \text{mod}~p$.

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 filed 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 $N_i$.

### 3.3 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>
<thead>
<tr>
<th>TABLE 3: Local time of the NC and the node (No attack)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC</td>
</tr>
<tr>
<td>RA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE 4: Local time of the NC and the node (With attack)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BC</td>
</tr>
<tr>
<td>RA</td>
</tr>
</tbody>
</table>

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.

### 4 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.

#### 4.1 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
Period 1

| Period 2 |
|---|---|
| 1 | 2 | ... |
| t | t | ... |

Fig. 6: Detailed timing of the RDMA protocol in RA phase

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 $\text{rand}()$ to randomly generate an integer number $N_k^k$ 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 $N_k^k$-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 $N_k^k$-th slot. If the node has successfully received the acknowledgement frame from the NC, it will set $S_{suc} = 1$, which means 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 ($k = 1, 2, ..., M$) 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 $N_{max}^k$.

### 4.2 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

$$p_1 = \left(\frac{1}{N_{max}^k}\right)\left(\frac{N_{max}^k - 1}{N_{max}^k}\right)^{m_k-1}. \tag{7}$$

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

$$p_2 = m_k\left(\frac{1}{N_{max}^k}\right)\left(\frac{N_{max}^k - 1}{N_{max}^k}\right)^{m_k-1}. \tag{8}$$

Because each node independently generates its random waiting slot number $N^k_w$, 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

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

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

$$m_{k+1} = m_k - \Delta_{m_k}. \tag{10}$$

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 legislate nodes is $\rho$, we have

$$m_0 = N_{nd} = \rho \pi R^2 / L. \tag{11}$$

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:

$$\Delta_{m_k} = m_k\left(\frac{N_{max}^k - 1}{N_{max}^k}\right)^{m_k-1}. \tag{12}$$

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

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

Therefore, we have

$$N_{max}^k = m_k, \tag{14}$$

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 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 (9) is correct. In addition, it can be seen that when equal \( N_{\text{max}}^k \) is used in successive periods, setting \( N_{\text{max}}^k = N_{nd} \) achieves the best scheduling performance, where the convergence of \( R_{\text{suc}} \) to unit is the fastest.

Further more, from Fig. 7, in comparison with the case of using equal \( N_{\text{max}}^k \) in successive periods, adaptively using different \( N_{\text{max}}^k \) in successive periods can have much better scheduling performance when considering the convergence time of \( R_{\text{suc}} \). The time slots required when using adaptive \( N_{\text{max}}^k \) is much less than that of using equal \( N_{\text{max}}^k \) 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 \( N_{\text{max}}^k = N_{nd} \), while the curves marked with squares are that using adaptive slot number \( N_{\text{max}}^k = m_k \). 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 (9) again. From this figure, using adaptive slot number \( N_{\text{max}}^k = m_k \) can saves approximately 30% of the total number of time slots in the RA phase in comparison with the case of using equal number of slots.

Fig. 8: Number of slots required for successful transmission of all nodes in an interested sector

### 4.3 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 \( N_{\text{max}}^k = m_k \). 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 \( N_{\text{max}}^k \).

For a given value of \( N_{nd} \), the NC can theoretically calculate the value of \( M \) and \( N_{\text{max}}^k \) by using Algorithm 2, where \( N_{RA} \) denotes the number of total slots in the RA phase, and the function \( \text{ceil()} \) 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 (9) and (10). 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.

The NC can also get the statistical values of \( M \) and \( N_{\text{max}}^k \) by using Algorithm 3, where \( N_{\text{sim}} \) denotes the total Monte Carlo simulation rounds, \( N_{\text{slot}}(S_{\text{ind}}, k) \) records the slot number used in period \( k \) in the \( S_{\text{ind}} \)-th round of simulation. \( N_{\text{ave}}(k), N_{\text{Std}}(k), \) and \( N_{\text{Max}}(k) \) 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

1. In this algorithm, some Matlab system functions are invoked: \texttt{rand()}, \texttt{find()}, \texttt{size()}, \texttt{sum()}, \texttt{std()}, and \texttt{max()}. For their operations, please refer to the Matlab help file.
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:    $M = M + 1$;
8:    $N_{RA} = N_{RA} + N_{max}^k$;
9:    $m_{k+1} = m_{k}(1 - \frac{N_{max}^k}{N_{max}^k - 1}m_{k-1})$
10:   $N_{max}^k = \text{ceil}(N_{max}^{k+1})$;
11:   $k = k + 1$;
12: end while
13: SET $M = M + 1$;
14: SET $N_{RA} = N_{RA} + 1$;
15: SET $N_{max}^k = 1$;

END;

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 $S_{nd} = 1:1:N_{sim}$ 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 $N_{slot}(S_{nd}, k) = N_{max}^k$;
8:        for $i = 1:1:N_{max}^k$ do
9:            SET $i_{slot}(i) = \text{ceil}(N_{max}^k \text{rand}())$;
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 $m_{k+1} = m_{k} - \text{size(find}(M_{slot} \neq 0)))$;
21:     $k = k + 1$;
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;

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.

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

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 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.

5 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 legislate nodes falling in both the communication range of the NC and the malicious node, the legislate 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 legisate 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.

6 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 propose 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:

\[
T_{SND} = L(T_{BC} + T_{RA} + T_A),
\]

(15)

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

\[
N_{RA} = N_{norm}N_{nd}
\]

(16)

So (15) becomes

\[
T_{SND} = L(Lt_n + N_{norm}\rho \pi R^2 t_d / L + t_d).
\]

(17)
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:

$$G_R = G_T = LG_0,$$  \hspace{1cm} (18)

where $G_0$ is the antenna gain of omni-directional antennas. From (2), we have

$$P_R,t_h = k_1L^2G_0^2R^{-\alpha}P_T.$$  \hspace{1cm} (19)

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

$$R = KL^{\frac{2}{\alpha}}$$  \hspace{1cm} (20)

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

$$T_{SND} = t_nL^2 + N_{norm}\rho\pi L^{\frac{2}{\alpha}}t_r + t_dL.$$  \hspace{1cm} (21)

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

$$T_{SND} = t_nL^2 + N_{norm}\rho\pi L^2t_r + t_dL.$$  \hspace{1cm} (22)

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 $N_{norm}\rho\pi L^2t_r$ 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 $\rho R^2L^{\frac{2}{\alpha}}$, the average time for a node to be discovered by the NC is:

$$T_{A_{SND}} = \frac{t_n}{\rho L^{\frac{2}{\alpha}} - 2\pi K^2} + N_{norm}\rho\pi L^{\frac{1}{\alpha}}K^2 + \frac{t_d}{\rho\pi L^{\frac{2}{\alpha}}K^2}.$$  \hspace{1cm} (23)

When $\alpha = 2$,

$$T_{A_{SND}} = \frac{t_n}{\rho\pi K^2} + N_{norm}\rho\pi t_r + \frac{t_d}{\rho\pi K^2L}.$$  \hspace{1cm} (24)

The first item $t_n/\rho\pi K^2$ is the average BC time, and it is inversely proportional to the node density $\rho$. The second item $N_{norm}\rho\pi t_r$ 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.

7 Conclusions

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


Zhiguo Shi (IEEE M’10) received the B.S. degree and Ph.D. degree both 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 visiting to the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include radar data and signal processing, wireless communication and security. He received the Best Paper Award of IEEE WCNC 2013, Shanghai, China, and IEEE WCSP 2012, Huangshan, China. He received the Scientific and Technological Award of Zhejiang Province, China in 2012. He serves as an editor of KSI Transactions on Internet and Information Systems. He also serves as TPC member for IEEE VTC 2013 Fall, IEEE ICC 2013, MSN 2013, IEEE INFOCOM 2014, IEEE ICNC 2014, etc.

Rongxing Lu (IEEE M’10) 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 his B.E. degree in Beijing University of Posts and Telecommunications, China in 2006 and the MSc degree in Electrical and Computer Engineering from University of Waterloo, Canada in 2010. He is currently working toward his PhD degree at the Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research interests include millimeter wave WPANs, medium access control, resource management, and smart grid networks.

Ruixue Sun received the B. Sc degree in communication engineering, Xidian University, Xi’an, China, in 2012. She is pursuing her Master degree in Department of Information and Electronic Engineering, Zhejiang University. Her research interests mainly focus on security and privacy in millimeter wave communication and smart grid.
Xuemin (Sherman) Shen (IEEE M’97 SM’02 F’09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. He was the Associate Chair for Graduate Studies from 2004 to 2008. Dr. Shen’s research focuses on resource management in interconnected wireless/wired networks, wireless network security, wireless body area networks, 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. Dr. Shen served as the Technical Program Committee Chair for IEEE VTC’10 Fall, the Symposia Chair for IEEE ICC’10, the Tutorial Chair for IEEE VTC’11 Spring and IEEE ICC’08, the Technical Program Committee Chair for IEEE Globecom’07, the General Co-Chair for ChinaCom’07 and QShine’06, the Chair for IEEE Communications Society Technical Committee on Wireless Communications, and P2P Communications and Networking. He also serves/served as the Editor-in-Chief for IEEE Network, Peer-to-Peer Networking and Application, and IET Communications; a Founding Area Editor for IEEE Transactions on Vehicular Technology; an Associate Editor for IEEE Transactions on Vehicular Technology, Computer Networks, and ACM/Wireless Networks, etc.; and the Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004, 2007 and 2010 from the University of Waterloo, the Premier’s Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada Fellow, a Canadian Academy of Engineering Fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.