SND: Secure Neighbor Discovery for 60 GHz Network with Directional Antenna

Zhiguo Shi[†,‡], Rongxing Lu[‡], Jian Qiao[‡] and Xuemin (Sherman) Shen[‡]
[†]Department of Information and Electronic Engineering, Zhejiang University, Hangzhou 310027, China
[‡]Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada N2L 3G1
Email: shizg@zju.edu.cn; {rxlu, jqiao, xshen}@bbcr.uwaterloo.ca

***Abstract*—In this paper, we propose a wormhole attack resistant secure neighbor discovery scheme, named SND, for 60 GHz directional wireless network with a centralized network controller (NC). In specific, the proposed SND scheme consists of three phases: the NC broadcasting phase, the network node response/authentication phase and the NC time-delay analysis phase. In the broadcasting phase and response/authentication phase, local time information and antenna direction information are elegantly exchanged with signature based authentication techniques between the NC and legislate network nodes, which can prevent most of the wormhole attacks. In the NC time-delay analysis phase, the NC can further detect the possible attack by using the time-delay information from the network node. To solve the transmission collision problem in the response/authentication phase, an RD-TDMA protocol is also proposed. Both simulation results and security analysis demonstrate that the proposed SND scheme can effectively resist wormhole attack for the 60 GHz communication network with directional antenna.**

***Index Terms*—60 GHz network, secure neighbor discovery, wormhole attack.**

I. Introduction

Communications in the unlicensed 57-66 GHz band (60 GHz for short) have recently attracted great attention from both academy and industry [1], [2]. Especially, with the development of using SiGe and CMOS technologies to build inexpensive 60 GHz transceiver, there have been growing interest in standardizing and drafting specifications for applications in this frequency band. In October 2009, IEEE 802.15.3c was introduced for wireless personal area networks (WPAN) [3], [4], and the IEEE 802.11ad is being finalized for wireless local area networks (WLAN) [5].

One distinguishing feature of 60 GHz communication is its high propagation loss due to the extremely high carrier frequency and the oxygen absorption peaks at this frequency band [1]. To combat this, directional antenna with high directivity gain can be adopted to obtain sufficient link budget for multi-Gbps data rate. However, though the directional antenna offers many advantages for the 60 GHz communications, the antenna beam should be allied in the opposite direction for a communication pair before their communication starts. This poses many special challenges for higher layer protocol design [6]–[9], and one of which is the neighbor discovery.

For a wireless node, neighbor discovery is to determine the total number and identities of other nodes in its communication range. It is a fundamental building block of many protocols in communication systems and enables different types of system functionalities, such as physical access control, network access control, routing [10]. In traditional communication system with ommi-directional antenna, the neighbor discovery process is very straightforward. However, in the 60 GHz communication system with directional antenna, the neighbor discovery becomes much more difficult.

In recent years, several neighbor discovery approaches have been proposed from different aspects for 60 GHz network with directional antenna [6], [11]–[13]. A basic assumption in all these approaches is that messages between nodes are communicated in a blind way, which means that the neighbor discovery process is executed without the pre-knowledge of the locations of the neighbors. Generally, neighbor discovery protocols can be categorized into direct neighbor discovery protocols and gossip-based neighbor discovery protocols [14]. In direct neighbor discovery, both the neighbors scan their beams in the space and when they detect each other, execute certain handshakes, then recognize each other as neighbors. According to the beam scan manner, the direct neighbor discovery protocols can be further divided into two categories, namely *randomized* direction neighbor discovery and *scan-based*. In this work, we will focus on the study on the *scan-based* direct neighbor discovery.

Through extensive survey on the neighbor discovery in 60 GHz network with directional antenna, very few works consider the security problem in the neighbor discovery process. In fact, the very nature of wireless networks make it easy to abuse neighbor discovery and therefore compromise the overlying protocols and applications. Thus, it is necessary to provide methods to mitigate this vulnerability and guarantee the neighbor discovery security.

One particular insidious threat to 60-GHz wireless networks is the wormhole or relay attack [15]–[17]. The wormhole attack will cause unauthorized physical access, selective dropping of packets and even denial of services [10]. The 60-GHz wireless networks is prone to this attack, because when a malicious node equipped with directional antenna conducts illegal operations, the probability of being detected by other nodes is much less than that equipped with ommi-directional antenna. Therefore, this is a very critical issue for the 60-GHz wireless networks with directional antenna.

To address the aforementioned challenge, in this paper, we propose a wormhole attack resistant secure neighbor discovery scheme, called SND, for 60 GHz wireless networks with

978-1-4673-5939-9/13/$31.00 ©2013 IEEE

directional antenna. We only consider the infrastructure mode where there exists one network controller (NC) for access control and resources management of the network. The main contributions of this work can be summarized as follows.

- First, we propose a secure neighbor discovery scheme, called SND, which establishes the communications with signature based authentication techniques, and achieves secure neighbor discovery by utilizing the information of antenna direction, local time information and carefully designed broadcast message length.
- Second, we propose an RD-TDMA protocol to solve the transmission collision problem in the response/authetication phase where each node in the same sector does not have information of others and can not listen to the others' transmissions due to the directional antenna limitation.
- Third, we conduct secure analysis and simulations to demonstrate the effectiveness of the proposed SND scheme.

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

II. Problem Formulation

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

A. Network Model

Although different standards of 60 GHz networks may support infrastructure mode, ad hoc network mode and hybrid mode, in this paper, 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 $\mathbb{N} = \{N_1, N_2, N_3, \cdots\}$ and a single NC, which may be AP 802.11.ad based WLAN or PNC in 802.15.3c based WPAN, as shown in Fig. 1. Wireless nodes are randomly distributed in the area for study with the node density ρ per square meter. Each of the wireless nodes and the NC are equipped with an directional antenna. An ideal "flat-top" model [18] for the directional antenna is used here. For this antenna model, the antenna has L beams, each of which spans a fixed beamwidth with angel of $\alpha = 2\pi/L$ radians. All the L beams can collectively maintain the seamless coverage of the entire direction.

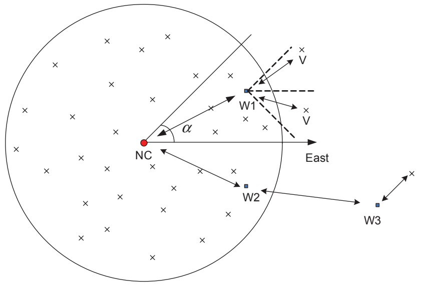

Fig. 1: Network model under consideration

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. The normalized pattern function of the directional antenna when it selects the i-th $(1 < i \leqslant L)$ beam is defined as:

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

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. We assume that all the links between 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 the node A. All the mobile nodes do not have specialized hardware such as 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 direction sector.

B. Attack Model

In this work, we mainly consider one kind of active attack named wormhole attack, in which the malicious node(s) relay packets for legislate node 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 such attack is that, there is a malicious node, e.g., W1, between NC and the distant node. 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 cooperate 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 ρ_m per square meter.

C. Design Goal

Our design goal is to design a wormhole attack resistant secure neighbor discovery scheme for 60-GHz network with centralized NC for further network resource managements.

D. Assumptions

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 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 $Y_c = g^{x_c} \bmod p$ [19]; and each node $N_i \in \mathbb{N}$ also has its private-public key pair $(x_i \in \mathbb{Z}_q^*, Y_i = g^{x_i} \bmod p)$. The malicious nodes have the same level of computation power as the legislate nodes, but they cannot obtain legislate nodes' key materials.
- 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.

III. Proposed Wormhole Attack Resistant Scheme

A. Main Idea of The Proposed Scheme

To illustrate the main idea of the proposed scheme clearly, we plot one sample of the simulated network scenario in Fig. 2, 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) and the direct communication range R is 50 meters. The radius area around the NC is seamless covered by $L = 8$ beams. In this sample, there exist three attackers marked with red star. Though the region that each attacker can attack can be a radium area, sectors other than the plotted red sector can be easily protected from wormhole attack by using directional authentication, as described in the following. The aim of the proposed SND scheme is to find whether there are malicious nodes in each sector.

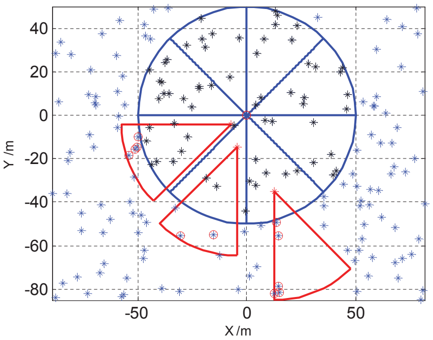

Fig. 2: One sample of simulated network scenario

The flowchart of the proposed wormhole attack resistant scheme is shown in Fig. 3. The NC discovers its neighbor 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 to the specific direction. This period is called "NC broadcasting (BC) phase". The legislate node in this sector scans its neighbor sector in a counter-clockwise manner starting from a random sector, staying in each sector for T_n second. 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 $L * T_n$ seconds.

After the NC broadcast its "hello" message in a specific sector and all the nodes in this sector hear the "hello" message, the node "response/authentication (RA) phase" starts. 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, which is referred as the "NC time analysis (TA) phase", as shown in Fig. 3.

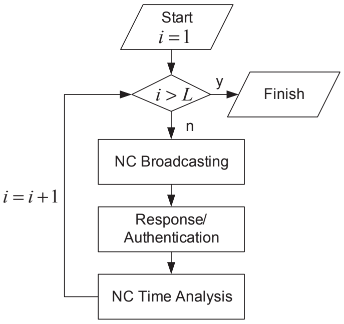

Fig. 3: Flow chat of the proposed scheme

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 NC TA phase. Note that for the NC BC phase, the "hello" message is transmitted in each of the $T_n/2$ time slot and the length of the "hello" message is larger than $T_n/4$ for security reason, which will be explained in the security analysis section.

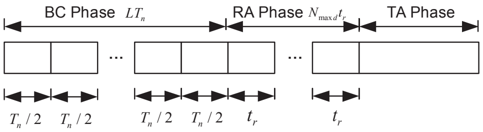

Fig. 4: Time domain observation of the proposed scheme

B. NC BC Phase

For this phase, the NC broadcasts its existence to its neighbor in a specific sector by continuously sending "hello" message. The frame format of the "hello" message is shown in TABLE I.

TABLE I: The BC Frame Format Sent by the NC

DEVID	θ_{NC}	T_{nc}	T_r	t_r	N_{maxd}	σ_c	padding

The main information body M_c of the "hello" message contains six fields, namely DEVID, θ_{NC}, T_{nc}, T_r, t_r and N_{max}. DEVID is the unique device id of the NC. θ_{NC} is the direction sector id that the NC broadcasts. T_{nc} denotes the local NC time. T_r denotes the time that NC stops broadcasting in the sector and legislate node 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 node can send a packet to the NC and wait for the NC's acknowledgment. N_{max} denotes the maximum delayed slot number that a node uses to generate random number of time slot to wait for a transmission, which will be explain later in the RD-TDMA protocol.

The signature σ_c is generated by the following method. 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

$$\begin{cases} R_c = g^{r_c} \bmod p \\ S_c = r_c + x_c \cdot H(R_c||M_c) \bmod q \end{cases} \tag{2}$$

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

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

$$g^{S_c} \overset{?}{=} R_c \cdot Y_c^{H(R_c||M_c)} \bmod p \tag{3}$$

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

$$\begin{aligned} g^{S_c} &= g^{r_c + x_c \cdot H(R_c||M_c)} \\ =&g^{r_c} \cdot g^{x_c \cdot H(R_c||M_c)} = R_c \cdot Y_c^{H(R_c||M_c)} \bmod p \end{aligned} \tag{4}$$

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 N_{max} for further communication with the NC. The θ_{NC} is used to check whether there is possible wormhole attack.

C. RA Phase

After the NC BC phase, the nodes in the specific sector could response in two different manners according to two different situations. The first situation is that the node(s) in this sector knows that they have received frame 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 to the same direction as the NC, as shown in Fig. 2. Under 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 the nodes in this sector have received "hello" message without frame collision. Under this situation, the nodes will send 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 is malicious node in this sector.

The RA frame from the nodes to the NC to report malicious node or to authenticate itself is defined in Table II, where the "TYPE" field is to represent whether this frame a "response" frame or an "authentication" frame, the "DEVID" filed represents the unique device id of node N_i, and the θ_{N_i} denotes the direction from the node N_i to the NC, and the σ_c is used as the signature of node N_i. The fields before the signature field σ_c is denoted as the main body M_i for the node N_i.

TABLE II: The RA Frame Format Sent by Node N_i

TYPE	DEVID	θ_{N_i}	T_{N_i}	σ_c	padding

The signature is generated by the node N_i in the following way. A 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

$$\begin{cases} R_i = g^{r_i} \bmod p \\ S_i = r_i + x_i \cdot H(R_i||M_i) \bmod q \end{cases} \tag{5}$$

After that, the N_i returns $M_i||\sigma_i$ to the NC. In addition, 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

$$g^{S_i} \overset{?}{=} R_i \cdot Y_i^{H(R_i||M_i)} \bmod p \tag{6}$$

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 $sk_{ic} = H(NC||N_i||R_i^{r_c})$ to establish an encrypted channel for future communication between NC and N_i. The correctness is due to $R_i^{r_c} = g^{r_i r_c} = R_c^{r_i} \bmod p$.

When the NC gets the contents of the authentication frame, it will check whether $\theta_{NC} + \theta_{N_i} = L$ to see whether there is a possible malicious node.

After the NC has received either the response frame or the authentication frame from the nodes in the sector, it will acknowledge them with an acknowledgement frame, as defined in Table III. Note that this frame is encrypted with session key sk_{ic} shared by the NC and the node N_i.

TABLE III: The Ack Frame Format Sent by the NC

TYPE	DEVID	θ_{N_i}	T_{N_i}	σ_c	padding

D. NC TA Phase

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

When the NC broadcasts its "hello" message, the local time T_{NC} of the NC starting transmission is also broadcasted. When the neighbor nodes receive the "hello" message, they will use the T_{NC} as the local time. Suppose the transmission time from the NC to a node is $t_{NC2node}$, then the local time difference between this node and the NC is $t_{NC2node}$. When this 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 node and itself. The local time of the NC and the node is shown in Table IV.

When there is a malicious node to attack the 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 which equals the frame transmission time of more than $T_n/4$. In addition, 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 V.

TABLE IV: Local time of 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 V: Local time of NC and 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}

As reported in [20], there exists a kind of high frequency timer 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 show the effectiveness of the time analysis of the NC, we show in Fig. 5 the time delay data obtained by the NC for the sample of the simulated scenario of Fig. 2. In this simulation, the total sector number $L = 8$, 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 the victim node outside the communication region of the NC, the NC can easily detect the attack by using the time analysis.

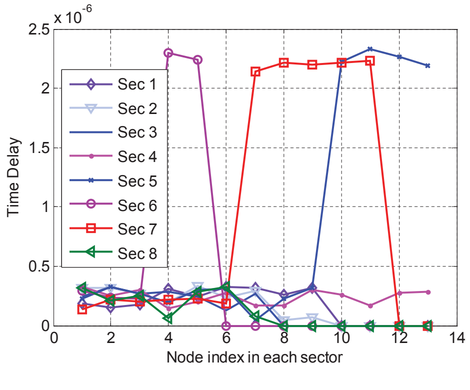

Fig. 5: Time delay data obtained by the NC

E. RD-TDMA protocol

When the RA Phase starts, if all the nodes in this sector start to transmit RA frame to the NC, it is inevitable that the frame will collide with each other. Thus, in this phase, a properly designed scheduling algorithm is required to allocate network resources 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 in this phase, it is difficult to implement carrier sense type multiple access techniques. In this work, we propose a novel random delay time division multiple access (RD-TDMA) protocol for each node in the same sector to communicate with the NC, as described below. For the "hello" message, the response start time is T_r, the response slot time length is t_r, and the maximum number of delaying slot for generating random delay slot number is N_{maxd}. When time T_r starts, each node executes the following protocol.

Algorithm 1 Backoff Mechanism for RD-TDMA

```
BEGIN:
1: Step 1: Generate a random number $n_w$ between 0 and $N_{maxd}$.
   The random number $n_w$ denotes the slot number the node should
   wait until it can send its communication/authentication frame.
2: Step 2: Wait until the starting time of slot $n_w + 1$ and send its
   frame to the NC.
3: Step 3:During the remaining time of slot $n_w + 1$, wait for the
   acknowledgement frame from the NC. If the acknowledgement
   frame from the NC is successfully received, that means it has suc-
   cessfully communicated/authenticated with the NC. Otherwise,
   redo step 1 to step 3.
END;
```

To show the effectiveness of the proposed RD-TDMA protocol, Fig. 6 plots the ratio of successful transmission node versus the number of time slots of the RA phase for different values of N_{maxd}. In this figure, the parameter "$NodeNum$" denotes the average node number in the interested sector under the assumption that the node is uniformly distributed. In the simulation, $NodeNum = 10$. It is found that the proposed RD-TDMA protocol has a rapid convergence time to approach the ratio of 100%. Also the optimal value of the N_{max} is $NodeNum$ when considering the convergence time.

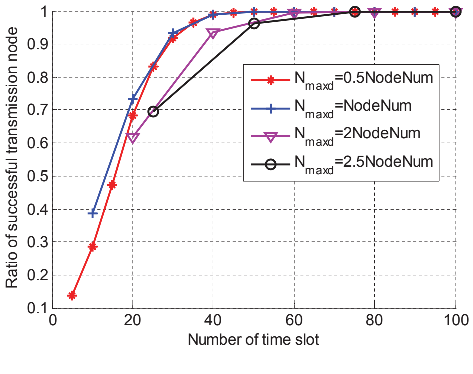

Fig. 6: Ratio of successful transmission nodes

IV. Security Analysis

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

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

Second, by using the directional authentication, the potential attacked region by malicious nodes is significantly reduced. In the BC phase, the NC broadcasts the direction θ_{NC}, and in the RA phase, the node reports the direction θ_{N_i}, then the NC can check whether $\theta_{NC} + \theta_{N_i} = L$. 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 θ_{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 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 node will detect the attack because the malicious node has no chance to relay a frame without collision with the broadcast frame from the NC.

Last, the NC time analysis prevents the remaining possible wormhole attacks. The security analysis above shows that only malicious nodes, which attack legislate nodes outside the circular communication region that can not hear the NC's broadcast, can launch the wormhole attack. However, the NC time analysis can easily detect these malicious nodes by utilizing the timing information.

V. Conclusions

In this paper, we have proposed a wormhole attack resistant secure neighbor discovery scheme, called SND, which consists of three elegantly designed phases, namely the NC BC phase, the RA phase and the NC TA phase. By using antenna direction information, transmission time information and carefully designed BC frame length, the proposed SND scheme can effectively prevent and detect wormhole attack, which has been demonstrated by the simulation results and security analysis. In addition, the proposed RD-TDMA protocol is very effective to solve the transmission collision problem in the RA phase when there are many nodes need to transmit frame to the NC without knowing each other and unable to listen to each other limited by antenna directions. This work is valuable when the security requirements are critical for the 60 GHz network with directional antenna.

Acknowledgment

This work is supported by National Science Foundation of China (No. 61171149, No. 60801004), Zhejiang Province Commonweal Technique Research Project (No. 2010C31069), Research Foundation of State Key Laboratory of Industrial Control Technology (No. ICT1119), China and ORF-RE, Ontario, Canada.

References

[1] R. Daniels and R. Heath, "60 ghz wireless communications: emerging requirements and design recommendations," *IEEE Vehicular Technology Magazine*, vol. 2, no. 3, pp. 41–50, 2007.

[2] J. Foerster, J. Lansford, J. Laskar, T. Rappaport, and S. Kato, "Realizing gbps wireless personal area networks-guest editorial," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 8, pp. 1313–1317, 2009.

[3] H. Singh, S. Yong, J. Oh, and C. Ngo, "Principles of ieee 802.15. 3c: Multi-gigabit millimeter-wave wireless pan," in *Proceedings of 18th Internatonal Conference on Computer Communications and Networks*. Ieee, 2009, pp. 1–6.

[4] 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 Communications Magazine*, vol. 49, no. 7, pp. 114–121, 2011.

[5] C. Cordeiro, D. Akhmetov, and M. Park, "Ieee 802.11 ad: introduction and performance evaluation of the first multi-gbps wifi technology," in *Proceedings of the 2010 ACM international workshop on mmWave communications: from circuits to networks*. ACM, 2010, pp. 3–8.

[6] X. An, R. Prasad, and I. Niemegeers, "Neighbor discovery in 60 ghz wireless personal area networks," in *IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2010, pp. 1–8.

[7] L. Cai, L. Cai, X. Shen, and J. Mark, "Resource management and qos provisioning for iptv over mmwave-based wpans with directional antenna," *Mobile Networks and Applications*, vol. 14, no. 2, pp. 210–219, 2009.

[8] ——, "Rex: a randomized exclusive region based scheduling scheme for mmwave wpans with directional antenna," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 113–121, 2010.

[9] J. Qiao, L. Cai, X. Shen, and J. Mark, "Enabling multi-hop concurrent transmissions in 60 ghz wireless personal area networks," *IEEE Transactions on Wireless Communications*, no. 99, pp. 1–10, 2011.

[10] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J. Hubaux, "Secure neighborhood discovery: A fundamental element for mobile ad hoc networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, 2008.

[11] F. Yildirim and H. Liu, "A cross-layer neighbor-discovery algorithm for directional 60-ghz networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, pp. 4598–4604, 2009.

[12] X. An, R. Prasad, and I. Niemegeers, "Impact of antenna pattern and link model on directional neighbor discovery in 60 ghz networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1435–1447, 2011.

[13] J. Ning, T. Kim, S. Krishnamurthy, and C. Cordeiro, "Directional neighbor discovery in 60 ghz indoor wireless networks," *Performance Evaluation*, 2011.

[14] S. Vasudevan, J. Kurose, and D. Towsley, "On neighbor discovery in wireless networks with directional antennas," in *Proceedings IEEE INFOCOM 2005*, vol. 4, 2005, pp. 2502–2512.

[15] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Network and Distributed System Security Symposium (NDSS)*. San Diego, 2004.

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

[17] 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 Transactions on Vehicular Technology*, no. 99, pp. 1–1, 2011.

[18] R. Mudumbai, S. Singh, and U. Madhow, "Medium access control for 60 ghz outdoor mesh networks with highly directional links," in *IEEE INFOCOM 2009*. IEEE, 2009, pp. 2871–2875.

[19] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology*. Springer, 1985, pp. 10–18.

[20] J. Jansson, A. Mantyniemi, and J. Kostamovaara, "A delay line based cmos time digitizer ic with 13 ps single-shot precision," in *IEEE ISCAS 2005*. IEEE, 2005, pp. 4269–4272.