Djuraev et al. EURASIP Journal on Wireless Communications and Networking (2017) 2017:11
DOI 10.1186/s13638-016-0785-z

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Channel hopping scheme to mitigate jamming attacks in wireless LANs

Sirojiddin Djuraev[1], Jin-Ghoo Choi[1], Kyu-Seek Sohn[2] and Seung Yeob Nam[1*]

Abstract

Although a jamming attack is an important problem in Wi-Fi networks, there is no effective solution to this problem yet. In this paper, we propose a new approach to resolve jamming attacks in Wi-Fi networks based on the concept of channel hopping. If we assume that the attacker does not jam all the channels simultaneously, then it might be possible to circumvent a jamming attack by changing the channel. A channel hopping mechanism is designed so that the access point (AP) and a normal user can agree on the next channel with a high probability without pre-sharing of any secret information between the AP and a user node. The proposed scheme is evaluated through experiment in a test bed.

1 Introduction

Wireless local area networks (LANs) are getting more popular nowadays because of easy deployment and the introduction of diverse types of Wi-Fi devices. However, despite all the advantages offered, wireless communication suffers from security vulnerabilities, such as jamming attacks, denial of service (DoS) attacks, or man-in-the-middle (MITM) attacks. One important issue among them is the jamming attack. An attacker with a radio transceiver intercepts a transmission, injects spurious packets, and blocks or jams the legitimate transmission [1–3]. The shared nature of the wireless medium allows the jammer to disable the entire network within the radio range. In this case, the jamming attack is regarded as a wireless version of a DoS attack. As the usage of wireless networks gets more prevalent, the jamming attack might influence a wider range of users, including military or business networks. Jammers can be classified according to their method: constant jammers, deceptive jammers, random jammers, and reactive jammers [2]. A constant jammer continuously sends jamming signals to interfere with the victim. A deceptive jammer constantly injects regular packets and keeps the channel busy all the time. Instead of sending continuous jamming signals, a random jammer sends a jamming signal randomly from time to time. A reactive jammer sends a jamming signal after sensing transmission on the current channel.

Reactive jamming is considered more sophisticated than other methods, because detection of reactive jammers is more difficult, and they can launch different jamming attacks in the physical layer or the medium access control (MAC) layer. Moreover, the reactive jamming method is energy efficient and can be done with any Wi-Fi-equipped device. In this paper, we model the attacker node after the reactive jammer.

Several approaches have been proposed to prevent jamming [4–6]. Channel hopping is one of the most practical approaches, because it might enable packet delivery even in the presence of jammers. One of the critical issues for this method is that the next channel should be determined without prior negotiation. If any prior negotiation is done by exchanging messages between users, those messages might be intercepted by the attackers, resulting in disclosure of the next channel to the attacker. Another problem is, if we consider a Wi-Fi hot spot where users come and go frequently, it may not be easy to exchange messages with the access point (AP) in the presence of an attacker.

In order to overcome the limitations of prior negotiation-based schemes, we propose a channel hopping mechanism that provides channel agreement between user nodes and the AP without prior negotiation. We use transmission power and received signal strength (RSS) to derive a channel number common to both the user and the AP.

* Correspondence: synam@ynu.ac.kr
[1]Information and Communication Engineering, Yeungnam University, Gyeongsan, South Korea
Full list of author information is available at the end of the article

When two APs are within the communication range of each other, a network administrator usually assigns the channel for each AP manually to minimize interference between them, or the APs search for the least congested channel, usually among the non-overlapping channels, by themselves [7]. However, Mishra et al. [8] showed that the total capacity of a wireless LAN can be improved by using partially overlapped channels among adjacent APs, rather than using only non-overlapping channels. When a specific AP is within the communication range of a jammer, even though the AP selects a partially overlapped channel as the next channel, the application traffic throughput may not be zero, depending on the physical distance between the AP and the jammer and the channel separation. Thus, in our proposed scheme we consider any channel except the jammed channel as a candidate for the next channel in order to lower the prediction ability of the jammer.

When the AP and the user select the next channel under a jamming attack, if they know the channel numbers used by other adjacent APs, then it would be better to avoid those channels as the next selection. However, when APs are densely deployed, it may not be easy to find any remaining non-overlapping channel. Furthermore, interfering channels monitored by a specific AP might be different from the channels monitored by a user node due to the hidden terminal problem. Thus, any channel except the jammed channel would be considered a candidate for the next channel in our proposed scheme, as mentioned above.

The contributions of our work can be summarized as follows.

- We propose a new channel hopping scheme that does not require prior negotiation.
- Using transmission power and received signal strength, we determine the next channel, and implementation of the scheme does not require special devices, such as a frequency hopping spread spectrum transmitter and a receiver. Thus, the proposed scheme can be deployed in existing wireless networks.
- We analytically investigate the effect of the proposed channel hopping scheme on throughput.

The rest of this paper is organized as follows. In Section 2, we review the existing approaches. In Section 3, we introduce the signal strength-based channel number generation scheme. In Section 4, we analyze the effect of the channel selection algorithm on throughput. Sections 5 and 6 describe the experiment topology and the experiment results, respectively. Section 7 concludes the paper.

2 Related work

Several channel surfing approaches have been proposed in the past [9–11]. Those approaches can be classified into two types: proactive and reactive.

In proactive approaches, the user node and AP change channels periodically at an interval of fixed length without checking for jammers [4, 10]. One disadvantage to this approach is that the nodes must change channels persistently, even when there is no jammer. This kind of unnecessary channel switching lowers throughput significantly. Moreover, if the next channel is determined according to a specific pattern, the scheme may not work when that pattern is detected by an attacker.

In reactive approaches, the AP and the user nodes start to change their channels after the detection of channel jamming [12, 13]. Several techniques have been proposed to detect channel jamming [14–19]. However, the main issue in this approach is to derive a new channel number that is common to both APs and users. If a jamming attack starts, it may not be possible to exchange messages between the APs and users. Most approaches rely on prior channel negotiation.

In order to implement a reactive approach, it is first necessary to detect jamming. Well-known jamming detection methods usually use packet delivery ratio, packet loss rate, packet latency, and signal strength [2, 14, 17]. Jamming detection schemes can be classified into two categories: the signal strength consistency-based approach and the location consistency-based approach. In the signal strength consistency-based approach, a low packet delivery ratio and a high received signal strength usually indicate a jamming attack. A location consistency-based approach determines the location of a node and measures throughput. If the throughput is low for a node that is close by, it might be due to a jamming attack. The signal strength consistency-based approach of Xu et al. [2] is used to detect a jamming attack in our proposed scheme.

Navda et al. [4] proposed a proactive channel hopping protocol with pseudo-random channels to avoid jamming. They assumed that the sequence of hopping channels is pseudo-random, and it is difficult to predict the next channel. However, a pseudo-randomly generated sequence is not truly random, because it is completely determined by a relatively small set of initial values. Thus, using a previous channel hopping sequence, the attacker might calculate or predict the next channel. They assumed that the channel sequence is only known to legitimate users and the AP. Another limitation of this approach is that it may not work in public Wi-Fi hot spots, where people come and leave frequently. If the users do not know the seed for the pseudo-random scheme, they cannot predict the next channel.

Frequency hopping is similar to channel surfing in that both of them change frequency during communications,

but frequency hopping is a physical-layer technology, which requires more advanced transceivers, while channel hopping is a link-layer technology that can be applied to existing wireless devices without a frequency hopping feature. Lee et al. [5] proposed a frequency hopping method that does not require pre-key establishment before data transmission. Although they introduced a scheme to make different nodes meet on the same channel without any pre-shared information under a jamming attack, they do not discuss how different nodes can change channels in a synchronized manner afterwards. The quorum rendezvous channel hopping scheme [5] guarantees at least one rendezvous between two different nodes within c time slots, where c is the total number of available channels. Thus, if the channel hopping scheme proposed in [5] is used repeatedly, even after the first channel agreement, the throughput is likely to remain low for a large c. Contrarily, we design a channel hopping scheme carefully so as to maintain the agreement of the channels between the AP and a user node over adjacent time slots.

Yang et al. [20] and Tang et al. [21] investigated the issue of optimal power control for a user in the presence of a smart jammer. They modeled the power control problem with a smart jammer as a Stackelberg game [22] and investigated an optimal strategy to control the transmission power of the user with a utility defined based on the signal-to-interference-plus-noise ratio (SINR) reward and power consumption penalty. However, the utility did not include the factor of throughput between the legitimate transmitter and receiver, which is an important performance metric in wireless LAN environments. When the channel of an AP is fixed, if an attacker jams that channel continuously, simple power control on that channel may not be enough to overcome a low-throughput problem. Channel switching might be needed in this case. However, channel switching, i.e., coordinated channel switching between the AP and a user node, has not been specifically discussed in those game theory-based approaches yet.

3 Signal strength-based channel number generation

Wireless channel signal strength is measured as a negative number in decibel-milliwatts (dBm). In 802.11 wireless networks, clear channel assessment (CCA) is defined as a lower bound of energy for decoding of a wireless signal. Energy detection is based on receiving a valid signal at the start of a transmission slot, with a signal power of −76 dBm or greater for the 802.11g standard. If the signal strength of the frames is less than −76 dBm, then a user usually disconnects [23]. Table 1 describes the major parameters and variables required to explain our proposed scheme.

The received signal strength depends on the distance between the user and the AP. If two user nodes stay at two different positions from the AP, they have different signal strength values for the frames coming from the AP. That means we can measure different signal strengths from different locations around the AP. Even though an attacker is located near a user, the signal strength measured by the attacker might be different from that of the user. Thus, it is not easy to measure signal strength between two remote nodes. We will use this feature as a key to determine the next channel [24, 25].

Table 1 Major parameters and variables

Notations	Meaning
δ_0	Clear channel assessment (CCA) level for 802.11g
S	Adjusted RSS value, i.e., summation of its own transmission power and received signal strength
δ	Group size, i.e., a margin to determine the similarity between two different RSS values
$Tx(i,j)$	Transmission power of node i for the jth packet
$Rx(k,l)$	Received signal strength of the lth packet measured at node k
Δ	Channel switching time (= channel sojourn time = time slot)
C_n	Channel number in the nth time slot
c	Number of available channels in 802.11g
r_{on}	Average traffic rate during the time slot where the AP and a user node stays on the same channel
r_a^{ran}	Average throughput when the AP and the user node randomly select the next channel
r_a^{sel}	Average throughput when the AP and the user node select the next channel according to our proposed scheme
p_e	Channel disagreement probability, i.e., probability that the AP and a user node select different next channel numbers under the condition they stay on the same channel in the current time slot
p_a	Probability that the AP and the user node select the same next channel number under the condition that they stay on different channels in the current time slot

According to Chen et al. [26], the property of reciprocity declares that bidirectional wireless channel states should be identical between two transceivers at a given instant of time. However, this may not always be true in a real environment.

Let us assume that the AP and a user node exchange two frames, one in each direction, and measure the signal strength at the same time. Let S_1 and S_2 denote the signal strength (in dBm) measured by the AP and by the user node, respectively. If we compare S_1 and S_2 as floating point numbers, they might be close to each other, but a complete agreement between them will be a very rare event. This means that if each node attempts to generate the next channel number using S_1 or S_2 at floating point precision, then they are not likely to agree on the same channel number.

Thus, it is necessary to design the channel number generation algorithm based on the similarity between S_1 and S_2, but not based on equality between them, even to floating point precision. To resolve this issue, we divide a possible range of signal strengths into subintervals of a fixed length, as shown in Fig. 1.

In Fig. 1, if the measured signal strength belongs to the interval $[\delta_0 + (i-1)\delta,\ \delta_0 + i\delta]$, then that signal strength belongs to group G_i, and the next channel is generated using group index i instead of the signal strength value itself to induce the same next channel number, assuming the measured signal strength values are similar between the AP and user node. The group size δ determines the resolution for signal strength comparison.

3.1 Next channel number generation scheme

If a legitimate client and the AP communicate on a static channel, jammers can easily identify the channel and can jam that channel indefinitely. Hopping methods usually require legitimate users to move to another channel in order to avoid the jammer. There are two approaches to avoid jamming: proactive and reactive. Our proposed scheme follows the reactive approach, and in our scheme, each user node and the AP move to another channel only after finding that the current channel is jammed.

When a jamming signal is detected, the AP and the user node choose the next channel to move based on the symmetry of signal strength over the bidirectional wireless channel between them. We consider the packet transmissions between two arbitrary nodes, node A and node B, in Fig. 2. In the figure, $Tx(i,k)$ denotes the transmission power of node i for the kth packet, and similarly, $Rx(j,k)$ indicates the received signal strength of the kth packet measured at node j. We denote the channel gain from node A to B as $H(\mathrm{A},\mathrm{B},k)$ for the kth packet transmission. Then, the following equations hold:

$$Rx(B,1)=Tx(A,1)+H(A,B,1),$$

$$Rx(A,2)=Tx(B,2)+H(B,\mathrm{A},2),$$

where every power and channel gain are in dBm. Thus, assuming that $H(A,B,1) = H(B,A,2)$, we obtain

$$Tx(A,1)\text{-}Rx(B,1) = Tx(B,2)\text{-}Rx(A,2). \quad (1)$$

If node B can receive the value of $Tx(A,1)$ from node A and node A can receive the value of $Tx(B,2)$ from node B, then these two nodes can use $(Tx(A,1) - Rx(B,1))$ or $(Tx(B,2) - Rx(A,2))$ as a seed to generate the next channel number because of the equality between them in Eq. (1). However, in this case, there will be an additional communication overhead to deliver the transmission power information to the other side. This communication overhead issue can be resolved in the following way. Equation (1) can be rearranged to

$$Tx(A,1)+Rx(A,2)=Tx(B,2)+Rx(B,1). \quad (2)$$

$Tx(A,1)$ on the left-hand side of the above equation is the packet transmission power at node A. Because the transmission power at node A is determined by node A, node A knows the value of $Tx(A,1)$. $Rx(A,2)$ is the received signal strength measured by node A for the second packet. Thus, node A knows this value as well. Node B knows the values of $Tx(B,2)$ and $Rx(B,1)$ for similar reasons. Equation (2) can be summarized as follows. Even when the transmission power is different between two communicating nodes, if they add their own transmission power (in dBm) to the received signal strength (in dBm), then the two communicating nodes can obtain the same summation value by Eq. (2), which is referred to as *adjusted RSS value* in this paper, in case of path loss symmetry on the bidirectional channel. S denotes the most recent value of adjusted RSS, and this

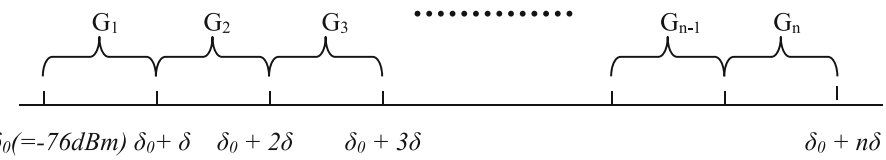

Fig. 1 Division of a signal strength range into intervals of fixed width δ

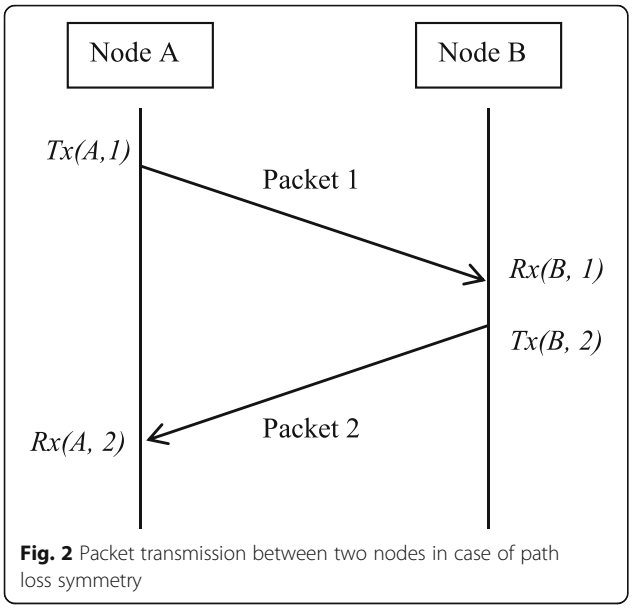

Fig. 2 Packet transmission between two nodes in case of path loss symmetry

can be used as a seed to generate the next channel number.

In order to calculate the next channel, we build a formula. As input values, we use the previous channel number C_{n-1} and the adjusted RSS value S. If there is no previous channel, then $C_{n-1} = 0$. We generate the next channel number according to the following equation:

$$C_n = h(\lfloor (S - \delta_0)/\delta \rfloor \| C_{n\text{-}1}) \% c, \quad (3)$$

where c is the number of available channels, $h()$ is a uniform random hash function, and $x||y$ means bit-level concatenation of x and y, and we use MD5 for $h()$ in this paper. $\lfloor x \rfloor$ is the largest integer that is less than or equal to x. The outcome of the hash function will be a non-negative integer, but it can be a large number, although the number of available channels is usually limited to a small number. In this paper, we consider IEEE 802.11g, and, thus, the number of channels is 11. We apply the modular operator % to map a large integer, the outcome of the hash function, to one of the available channel numbers with c of 11. We use $\lfloor (S - \delta_0)/\delta \rfloor$, which is referred to as the *quantized RSS value* in this paper, instead of the adjusted RSS value (S) itself in order to increase the channel agreement probability between the AP and the user, as explained in Fig. 1.

According to Eq. (3), the next channel number C_n is determined based on the previous channel number C_{n-1} and the adjusted RSS value S. Thus, the AP and the user node that share the same previous channel number are likely to share the same next channel number as long as they observe a similar signal strength.

Our scheme is based on the reciprocity of wireless channels, meaning that the channel gain between two nodes is identical when the role of each node changes, i.e., the transmitter becomes the receiver while the receiver becomes the transmitter. It is well known that channel reciprocity holds even in multipath fading channels with slow/fast fading [27, 28]. In practice, however, channel reciprocity may not always be true, since the channel measurement times are not identical at each node, and the noise level depends on the transceiver circuit. Indeed, there are many approaches to ensure channel reciprocity in wireless systems, such as interpolation and filtering [28]. The interpolation methods emulate the identical channel measurement times at the nodes [29, 30] and the filtering methods eliminate the high frequency components in noise [31, 32]. Unfortunately, these techniques are not perfect. That is the reason we use the quantized RSS value in Eq. (3) instead of the adjusted RSS value, as is. As the signal strength group size δ increases, our scheme becomes more robust to imperfect channel reciprocity. However, when δ increases, the attacker might easily obtain the quantized RSS value of the user node or the AP from its own signal strength measurement. If the attacker can calculate the next channel from Eq. (3) in this case, the throughput will be lowered again. We analyze the effect of δ on throughput through experiment in Section 6.

3.2 Attacker model

We assume that the attacker is fully aware of our proposed protocol. We assume that the jammer node also has the same performance as a usual node, and the jammer cannot jam all channels at the same time. We consider a reactive jammer model in this paper. In more detail, the attacker first attempts to guess the channel number of the AP according to the formula of our proposed protocol, i.e., Eq. (3). If there is a hit on the channel number, then the attacker launches a jamming attack. Otherwise, the attacker scans the busy channel and launches a jamming attack on the detected busy channel until the AP leaves the channel. If the AP changes channels, then the attacker repeats the same attack pattern of channel guessing, scanning, and jamming. The attacker uses a MAC layer jamming attack method.

4 Effect of channel selection scheme on throughput

In this section, we analyze the effect of the proposed channel selection scheme on throughput. We considered packet exchange between an AP and a specific user node. According to the channel switching model considered in this paper, each AP and user node change channels periodically at an interval of Δ after detection of a

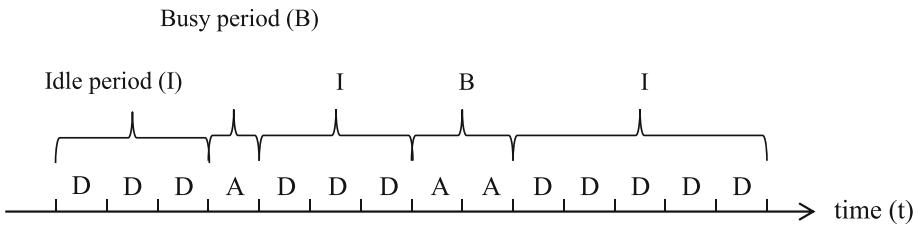

Fig. 3 Alternating idle and busy periods over time, under channel hopping

jamming attack. Thus, we can say that each node will stay on the selected channel during a fixed interval of Δ, also called a time slot. If the AP and the user node select the same channel number in a given time slot, then that time slot is called the A (agreement) slot. If the selected channel numbers do not agree with each other, then that time slot is called a D (disagreement) slot. Consecutive D slots constitute an idle (I) period, and consecutive A slots constitute a busy (B) period. Figure 3 describes the relation among A/D slots and I/B periods again with an example. We can easily find that the I and B periods always alternate. If r_{on} represents the average traffic rate from the user node to the AP during an A slot, the average throughput (r_{a}) can be expressed as

$$r_{\text{a}} = \frac{E[\text{B}] \times r_{\text{on}}}{E[\text{I}] + E[\text{B}]}. \tag{4}$$

Let us first consider the average throughput (r_a^{ran}) when the AP and the user node randomly select the next channel. If the number of available channels is c, then the probability that the AP and the user node select the same channel the next time is $1/c$. In this case, the busy period (B) is geometrically distributed, since the channel agreement probabilities for two consecutive time slots are independent of each other. Thus, B has the following distribution:

$$\Pr(\text{B} = n\Delta) = \left(\frac{1}{c}\right)^n \left(1-\frac{1}{c}\right), \quad n = 1, 2, 3,$$

Then, the expectation of B (E[B]) can be obtained as

$$\begin{aligned} E[\text{B}] &= \sum_{n=1}^{\infty} n\Delta \cdot \Pr(\text{B} = n\Delta) = \Delta \sum_{n=1}^{\infty} n \left(\frac{1}{c}\right)^n \left(1-\frac{1}{c}\right) \\ &= \left(\frac{1}{1-1/c} - 1\right)\Delta = \frac{\Delta}{c-1}. \end{aligned} \tag{5}$$

The idle period (I) has the following geometric distribution:

$$\Pr(\text{I} = n\Delta) = \left(1-\frac{1}{c}\right)^n \left(\frac{1}{c}\right), \; n = 1, 2, 3,$$

Then, the expectation of I (E[I]) can be obtained as

$$\begin{aligned} E[\text{I}] &= \sum_{n=1}^{\infty} n\Delta \cdot \Pr(\text{I} = n\Delta) = \Delta \sum_{n=1}^{\infty} n \left(1-\frac{1}{c}\right)^n \left(\frac{1}{c}\right) \\ &= \left(\frac{1}{1/c} - 1\right)\Delta = (c-1)\Delta. \end{aligned} \tag{6}$$

Combining Eqs. (4), (5), and (6) yields

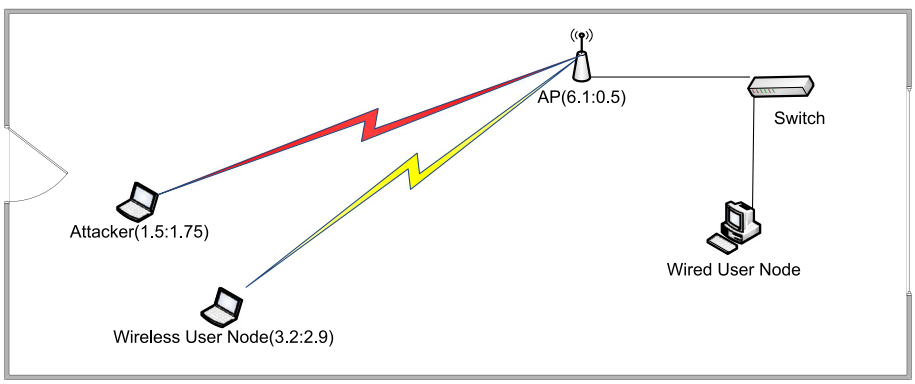

Fig. 4 Experiment topology

Table 2 Specification of each node involved in the experiment

	CPU	RAM	OS	Network adapter
AP	2.3 GHz Quad Core	2 GB	Ubuntu 12.04 LTS	3Com a/b/g
Attacker	1.4 GHz Intel Celeron	2 GB	Ubuntu 12.04 LTS	Atheros AR5822
Wireless user node	1.4 GHz Intel Celeron	2 GB	Ubuntu 12.04 LTS	Atheros AR5822
Wired user node	1.4 GHz Intel Celeron	2 GB	Ubuntu 12.04 LTS	Netlink BCM5778

$$r_a^{\text{ran}} = \frac{r_{\text{on}}}{(c-1)^2 + 1}. \tag{7}$$

We next consider the average throughput (r_a^{sel}) when the AP and the user node select the next channel according to our proposed scheme. In our scheme, the probability that the AP and the user node select the same next channel can be different, depending on whether they are currently on the same channel. If the AP and the user node stay on the same channel in the current time slot, then they can select the same channel again with a very high probability of $1 - p_e$, according to the algorithm described in Section 3, where p_e is the channel disagreement probability between the AP and a user node from inconsistent signal strength measurement. However, they may select a different channel with a low probability of p_e if the adjusted RSS values are significantly different between those two nodes.

Let p_a denote the probability that the AP and the user node select the same next channel number under the condition that they stay on different channels in the current time slot. If the AP and the user node stay on a different channel in the current time slot, then the user node first detects the discrepancy between its own channel number and the channel number of the AP and actively scans the channels to find the channel of the AP. The user node can find the next channel correctly only when it acquires the channel number of the AP in a given time slot, and the quantized RSS value of the node agrees with that value of the AP by Eq. (3). Although the user node attempts to search for the channel of the AP in this case, that search may not always be successful, that is, p_a may not always be equal to 1 because the channel scanning time can vary dynamically, on the order of hundreds of milliseconds in 802.11 networks [33].

We now investigate the distribution of the busy period (B) and the idle period (I) in detail. The time slot just before the idle period is always A slot from the explanation given for Fig. 3. There will be no idle period if another A slot comes after the previous A slot. Two consecutive A slots occur with a probability of $1 - p_e$ by the definition of p_e. Thus, we can obtain the following distribution of I:

$$\begin{aligned} &\Pr(\mathrm{I} = 0) = 1 - p_e, \\ &\Pr(\mathrm{I} = n\Delta) = p_e(1-p_a)^{n-1} p_a, \quad n = 1, 2, 3, \ldots \end{aligned}$$

From the distribution of I, $E[\mathrm{I}]$ can be obtained as

$$\begin{aligned} E[\mathrm{I}] &= \sum_{n=1}^{\infty} n\Delta \cdot \Pr(\mathrm{I} = n\Delta) \\ &= \Delta \sum_{n=1}^{\infty} n \cdot (p_e p_a)(1-p_a)^{n-1} = \frac{p_e}{p_a}\Delta \end{aligned} \tag{8}$$

In a similar manner, we can obtain the distribution of B as

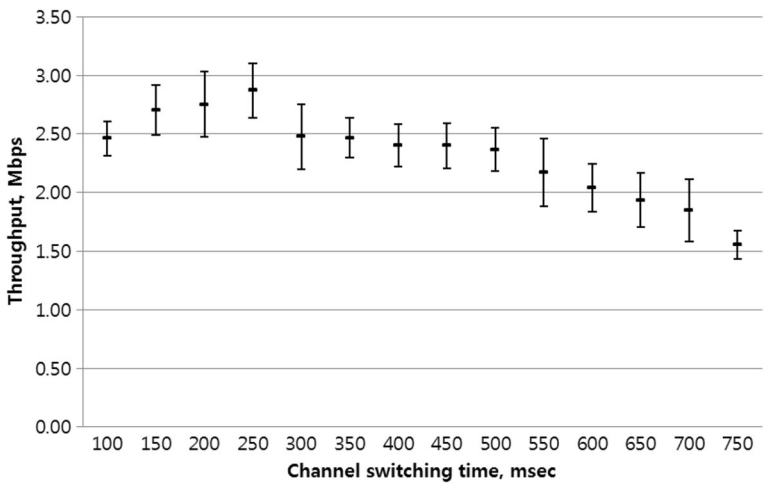

Fig. 5 Throughput of the proposed scheme for various channel switching times (or channel sojourn times) in the presence of a jammer

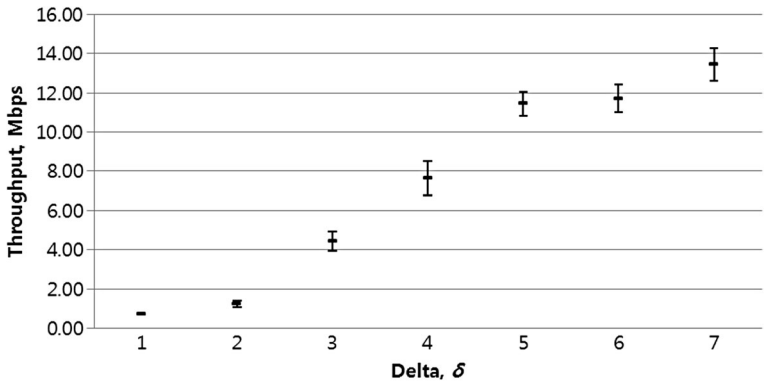

Fig. 6 Throughput of the proposed scheme for different values of δ when there is no attacker

$$\Pr(\mathrm{B}=0)=1-p_a,$$
$$\Pr(\mathrm{B}=n\Delta)=p_a(1-p_e)^{n-1}p_e,\quad n=1,2,3,\ldots$$

From the above distribution of B, $E[\mathrm{B}]$ can be obtained as

$$E[\mathrm{B}]=\sum_{n=1}^{\infty}n\Delta\cdot\Pr(\mathrm{B}=n\Delta)=\Delta\sum_{n=1}^{\infty}n\cdot(p_ap_e)(1-p_e)^{n-1}=\frac{p_a}{p_e}\Delta \tag{9}$$

Combining Eqs. (4), (8), and (9) yields

$$r_a^{\mathrm{sel}}=\frac{p_a^2\cdot r_{\mathrm{on}}}{p_e^2+p_a^2}. \tag{10}$$

If we compare r_a^{ran} in Eq. (7) and r_a^{sel} in Eq. (10), it is possible to show that $r_a^{\mathrm{sel}}>r_a^{\mathrm{ran}}$ when $c\geq 2$ and $p_e<p_a$, which is likely to be valid for a sufficiently large value of δ, because p_e tends to decrease as δ increases by the definition of p_e. Specifically, when p_e (i.e., the channel disagreement probability) is negligibly small, r_a^{sel} gets close to r_{on}, the theoretical upper bound of throughput, by Eq. (10).

5 Experiment topology

There are four nodes in the experiments: two user nodes (one wired node and one wireless node), one access point, and an attacker, as shown in Fig. 4. User nodes and the attacker use machines at the same level of performance, with an Atheros Wi-Fi chipset. We implemented channel switching in the kernel space for user nodes, and the attacker was implemented as a user space application. We modified an ath9k Wi-Fi driver and the hostapd open source code on the AP side. Table 2 shows the parameters of the nodes used for the experiments. All the experiments are done in an IEEE 802.11g environment (Table 2).

6 Experiment results

We measured the signal strength of the frames from the user node at the AP and that of the frames from the AP at the user node. Each user node generates the next channel independently and moves to that channel. If a

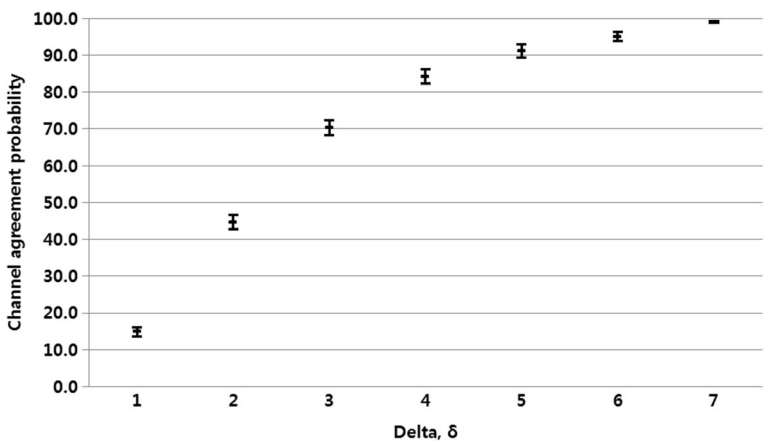

Fig. 7 Channel agreement probability between two communicating nodes for various values of δ when there is no attacker

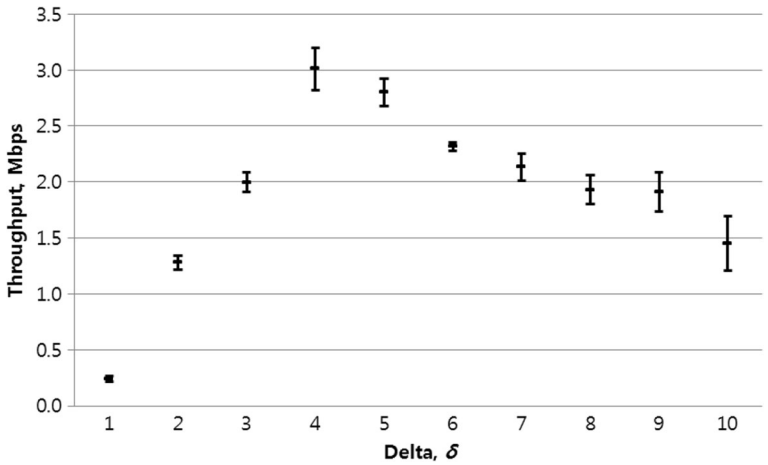

Fig. 8 Throughput of the proposed scheme for different values of δ when there is an attacker

user node cannot find the AP on that channel, then that user node searches other channels, one by one. We performed an experiment to investigate the effect of channel switching time on throughput for our proposed scheme when there is a jammer. Figure 5 shows throughput of the proposed scheme for various switching times. We found that a channel sojourn time of 250 ms gives the highest throughput in the presence of an attacker in our experiment.

In Fig. 5, when channel switching (channel sojourn) time increases, the throughput tends to decrease. As we stay on the selected channel longer, the attacker has a higher chance of jamming the channel after finding it, resulting in lower throughput. On the other hand, the channel switching time should not be too small. There must be enough time to reconfigure the connection between the user and the AP. Even though users do not authenticate and associate after changing channels, MAC layer access delay might lead to low throughput, especially when the channel sojourn time is very short [34]. The channel switching time will be fixed at 250 ms hereafter, considering the result of Fig. 5.

We next investigate the effect of the group size δ on throughput through experiment. We first measure the throughput of the proposed channel switching scheme for various values of δ when there is no attacker. Figure 6 shows the measurement results. We found that throughput increases as the value of δ increases. This trend can be explained as follows. According to Eq. (3), i.e., the next channel generation formula, δ is a margin in deciding the similarities between two adjusted RSS values measured between two communicating nodes. Thus, when the value of δ increases, the channel agreement probability tends to increase, as shown in Fig. 7, which was also obtained from experiment. When the channel agreement probability is high, the AP and the user node

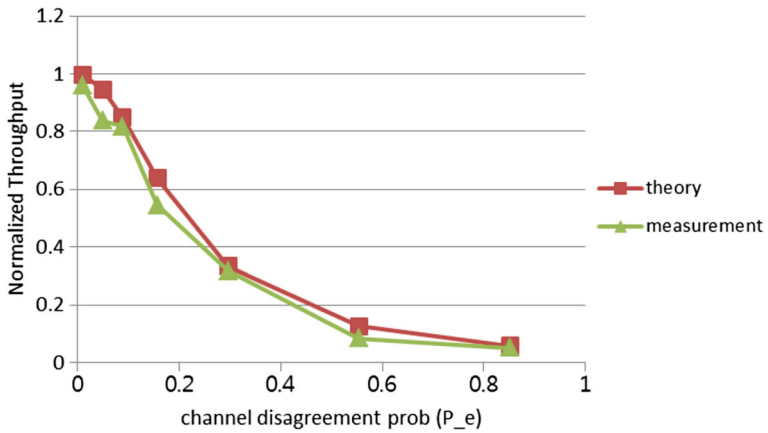

Fig. 9 Comparison of analysis result by Eq. (10) with the measurement result when there is no attacker

Table 3 Experiment scenarios

Scenario	Test environment
1	Random channel selection without an attacker
2	Proposed scheme without an attacker
3	Random channel selection scheme with an attacker
4	Proposed scheme with an attacker

are likely to stay on the same channel, even after switching channels, leading to higher throughput according to the analysis in Section 4.

Figure 8 shows the throughput of the proposed scheme for various values of δ when there is an attacker. The difference between the results of Figs. 6 and 8 can be summarized as follows. When there is no attacker (Fig. 6), the throughput increases monotonically when δ increases, due to improvement of the channel agreement probability. However, in Fig. 8, the throughput reaches a peak point when $\delta = 4$ and decreases afterwards. This trend can be explained as follows. δ is a margin in deciding the similarities between two adjusted RSS values between two communicating nodes. If the value of δ gets too large, the probability that the attacker obtains the correct channel number based on the formula of Eq. (3) using its own signal strength measurement might increase due to a large margin in the similarity check part of Eq. (3). Thus, throughput might degrade for large values of δ, especially when there is an attacker. The value of δ is fixed at 4 hereafter, based on the experiment result of Fig. 8.

Figure 9 compares the analysis results obtained by Eq. (10) with the measurement results when there is no attacker. The horizontal axis represents the channel disagreement probability, p_e, and the vertical axis, the normalized throughput, i.e., throughput divided by maximum throughput. For Eq. (10), r_{on} is the maximum throughput. Probability p_a was measured to be 0.21, and this value was used for p_a in Eq. (10). We find that our analysis result agrees closely with the experiment data.

Our goal is to improve throughput between a user node and the AP during the jamming period. We will compare our proposed scheme with a scheme that randomly selects the next channel. Table 3 explains the scenarios considered for subsequent experiments.

We measured the throughput for the random channel hopping scheme and the throughput for the proposed scheme and compared them with the throughput for the normal situation when there is no jammer. There is no channel hopping under normal circumstances. As we can see in Fig. 10, the throughput for the random channel hopping scheme stays very low (close to zero) because of the disagreement over channel numbers selected by the AP and the wireless user node.

Figure 10 shows that the proposed scheme yields much higher throughput compared to the random channel selection scheme. In the proposed scheme, the throughput sometimes goes down to zero due to disagreement over channel numbers selected by the AP and the user node. However, we find that the idle period due to such disagreements is usually shorter than the busy period with higher throughput.

Figure 11 compares the throughput of the proposed scheme with the throughput of the random channel selection scheme when there is a jammer, which behaves according to the attacker model described in subsection 3.2. We find that the random channel selection scheme does not effectively resolve the low-throughput issue when there is a reactive jammer. The throughput of the proposed scheme is higher than that of the random channel selection scheme, because the AP and the user node can select the same next channel with a higher probability, according to the channel selection scheme

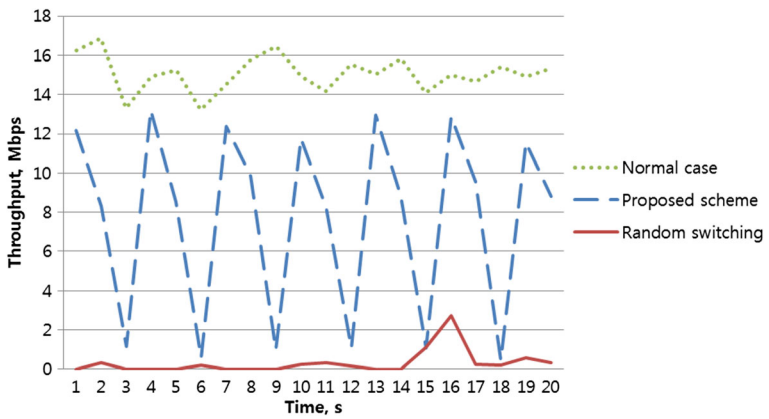

Fig. 10 Comparison of the throughput of the random channel selection scheme and the throughput of the proposed scheme when there is no jammer (scenarios 1 and 2)

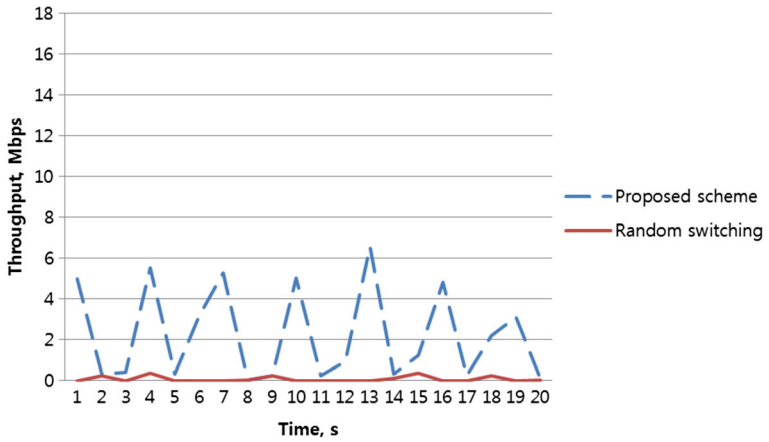

Fig. 11 Comparison of the throughput of the random channel selection scheme and the throughput of the proposed scheme when there is a jammer (scenarios 3 and 4)

described in subsection 3.1. If we compare Figs. 10 and 11, the throughput is lower for Fig. 11 because of the interference from the jammer.

7 Conclusions

We proposed a new channel hopping scheme to mitigate jamming attacks in the wireless LAN environment. The proposed scheme does not require an exchange of secret keys between the AP and user node prior to a jamming attack. This makes it harder for the attacker to guess the next channel number under our proposed scheme. The next channel is determined using the previous channel number and a combination of transmission power and received signal strength between the AP and user node. Since the next channel number generation scheme is designed to exploit the path loss symmetry between the AP and a user node, they are likely to switch to the same next channel as long as they stayed on the same channel previously. In case of an attack, even though the attacker finds the current busy channel number, it cannot easily predict the next channel because the path loss information between the AP and user node is not available. The effect of the proposed channel selection scheme on throughput was investigated analytically, and the experiment results show that meaningful throughput can be achieved with the proposed scheme in the presence of a jammer, compared to nearly zero throughput of the random channel selection scheme.

In this paper, we fixed the number of wireless normal users to one, just to concentrate on the operation of our proposed scheme in an adversarial environment. When there are multiple normal users, we need to consider both the aggregate throughput of normal users and fairness of throughput for each user. This complicated issue will be investigated in our future work.

Acknowledgements
This research was supported by the 2015 Yeungnam University Research Grant.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Information and Communication Engineering, Yeungnam University, Gyeongsan, South Korea. [2]Department of Hacking and Security, Hanyang Cyber University, Seoul, South Korea.

Received: 7 June 2016 Accepted: 5 December 2016
Published online: 09 January 2017

References

1. N Sufyan, NA Saqib and M, Detection of jamming attacks in 802.11b wireless networks, EURASIP Journal on Wireless Communications and Networking 2013:108 (2013). doi:10.1186/1687-1499-2013-208.
2. W Xu, W Trappe, Y Zhang, T Wood, *The feasibility of launching and detecting jamming attacks in wireless networks*. ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) (Urbana-Champaign, IL, USA, 2005)
3. DJ Thuente and M Acharya, Intelligent jamming in wireless networks with applications to 802.11b and other networks, in *Proceedings of IEEE Communication Society Military Communications Conference (MILCOM)*, Washington, DC, USA, pp. 1075–1081, Oct. 2006.
4. V Navda, A Bohra, S Ganguly, D Rubenstein, Using channel hopping to increase 802.11 resilience to jamming attacks, in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, Anchorage, AK, USA, pp. 2526–2530, May 2007.
5. EK Lee, SY Oh, M Gerla, Randomized channel hopping scheme for anti-jamming communication, in *Proceedings of IFIP Wireless Days (WD)*, Venice, Italy, pp. 1–5, Oct. 2010.
6. K Bicakci, B Tavli, Denial-of-service attacks and countermeasures in IEEE 802.11 wireless networks. Comput. Stand. Interfaces **31**(5), 931–941 (2009)
7. J Geier, Assigning 802.11b access point channels, Wi-Fi Planet, http://www.wi-fiplanet.com/tutorials/article.php/972261/Assigning-80211b-Access-Point-Channels.htm. Accessed 16 Aug 2016.
8. A Mishra, V Shrivastava, S Banerjee, W Arbaugh, Partially overlapped channels not considered harmful, in *Proc. of ACM SIGMETRICS*, Saint-Malo, France, pp. 63–74, June 2006.
9. K Pelechrinis, M Iliofotou, SV Krishnamurthy, Denial of service attacks in wireless networks: the case of jammers. IEEE Commun. Surv. Tutorials **13**(2), 245–257 (2011)

10. W Xu, T Wood, W Trappe, and Y Zhang, Channel surfing and spatial retreats: defenses against wireless denial of service, in *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, Philadelphia, PA, USA, pp. 80–89, Oct. 2004.
11. L Wang, AM Wyglinski, A combined approach for distinguishing different types of jamming attacks against wireless networks, in *Proceedings of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PacRim)*, Victoria, BC, Canada, pp. 809–814, Aug. 2011.
12. SR Gummadi, D Wetheral, B Greenstein, S Seshan, Understanding and mitigating the impact of RF interference on 802.11 networks, in *Proceedings of ACM SIGCOMM*, Kyoto, Japan, pp. 385–396, Aug. 2007.
13. W Hu, K Ma, W Trappe, Y Zhang, Jamming sensor networks: attacks and defense strategies. IEEE Netw. **20**(3), 41–47 (2006)
14. A Hamieh, J Ben-Othman, Detection of jamming attacks in wireless ad hoc networks using error distribution, *Communications, in Proceedings of IEEE International Conference on Communications (ICC)*, Dresden, Germany, pp. 1 – 6, June 2009.
15. AL Toledo, X Wang, Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks. IEEE Trans. Inf. Forensics Secur. **3**(3), 347–358 (2008)
16. K Pelechrinis, C Koufogiannakis, SV Krishnamurthy, On the efficacy of frequency hopping in coping with jamming attacks in 802.11 networks. IEEE Trans. Wirel. Commun. **9**(10), 3258–3271 (2010)
17. G Liu, J Liu, Y Li, L Xiao, Y Tang, Jamming detection of smartphones for WiFi signals, in *Proceedings of IEEE Vehicular Technology Conference (VTC)*, Glasgow, pp. 1–3, May 2015.
18. M Spuhler, D Giustiniano, V Lenders, M Wilhelm, JB Schmitt, Detection of reactive jamming in DSSS-based wireless communications. IEEE Trans. Wirel. Commun. **13**(3), 1593–1603 (2014)
19. O Punal, I Aktas, C Schnelke, G Abidin, K Wehrle, J Gross, Machine learning-based jamming detection for IEEE 802.11: design and experimental evaluation, in *Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Sydney, Australia, pp. 1–10, June 2014.
20. D Yang, G Xue, J Zhang, A Richa, X Fang, Coping with a smart jammer in wireless networks: a Stackelberg game approach. IEEE Trans. Wirel. Commun. **12**(8), 4038–4047 (2013)
21. X Tang, P Ren, Y Wang, Q Du, L Sun, Securing wireless transmission against reactive jamming: a Stackelberg game framework, in *Proceedings of IEEE Globecom*, San Diego, CA, pp. 1–6, Dec. 2015.
22. D Fudenberg and J Tirole, Game Theory, (The MIT Press, Cambridge, MA, 1991)
23. IEEE P802.11-REVmc™/D4.0—part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications, (Revision of IEEE Std 802.11™-2012), Jan. 2015.
24. R Wilson, D Tse, RA Scholtz, Channel identification: secret sharing using reciprocity in ultrawideband channels. IEEE Trans. Inf. Forensics Secur. **2**(3), 364–375 (2007)
25. K Zeng, Physical layer key generation in wireless networks: challenges and opportunities. IEEE Commun. Mag. **53**(6), 33–39 (2015)
26. S Chen, K Zeng, P Mohapatra, Jamming-resistant communication: channel surfing without negotiation, in *Proceedings of IEEE Conference on Communications (ICC)*, Cape Town, South Africa, pp. 1 – 6, May, 2010.
27. J Zhang, TQ Duong, A Marshall, R Woods, Key generation from wireless channels: a review. IEEE Access **4**, 614–626 (2016)
28. Zhang, et. al., "Experimental study on channel reciprocity in wireless key generation," in *Proceedings of IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Edinburgh, UK, 2016.
29. N Patwari, J Croft, S Jana, SK Kasera, High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Trans. Mobile Comput. **9**(1), 17–30 (2010)
30. H Liu, J Yang, Y Wang and Y Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, Orlando, Florida, USA, 2012.
31. H Liu, J Yang, Y Wang and Y Chen, "Fast and practical secret key extraction by exploiting channel response," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, Turin, Italy, 2013.
32. X Zhu, F Xu, E Novak, C C. Tan, Q Li and G Chen, "Extracting secret key from wireless link dynamics in vehicular environments," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, Turin, Italy, 2013.
33. D Murray, M Dixon, T Koziniec, Scanning delays in 802.11 Networks, in *Proceedings of International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST)*, Cardiff, UK, pp, 255–260, Sep. 2007.
34. P Chatzimisios, AC Boucouvalas, V Vitsas, IEEE 802.11 packet delay—a finite retry limit analysis, in *Proceedings of IEEE Globecom*, San Francisco, USA, pp. 950–954, Dec. 2003.