Ad Hoc Networks 11 (2013) 2648–2660

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Spoofing detection in IEEE 802.15.4 networks based on received signal strength

Paria Jokar *, Nasim Arianpoo, Victor C.M. Leung

Department of Electrical and Computer Engineering, The University of British Columbia, Vancouver, BC, Canada V6T 1Z4

ARTICLE INFO

Article history:
Received 15 October 2012
Received in revised form 10 March 2013
Accepted 2 April 2013
Available online 20 May 2013

Keywords:
Spoofing
IDS
IEEE 802.15.4

ABSTRACT

The shared medium used in wireless networks makes them vulnerable to spoofing attacks, in which an adversary masquerades as one or more legitimate nodes to disturb normal operation of the network. In this paper we present a novel spoofing detection method for static IEEE 802.15.4 networks based on spatial correlation property of received signal strength (RSS). While most existing RSS based techniques directly process RSS values of the received frames and rely on multiple traffic air monitors (AMs) to provide an acceptable detection performance, we extract features of RSS streams to reduce data redundancy and provide a more distinguishable representation of the data. Our algorithm employs two features of RSS streams, summation of detailed coefficients (SDCs) in discrete Haar wavelet transform (DHWT) of the RSS streams and the ratio of out-of-bound frames. We show that in a typical scenario, a single AM with SDC as detection parameter, can theoretically outperform a system with 12 AMs which directly applies RSS values as detection parameter. Using ratio of out-of-bound frames facilitates detection of high rate attacks. In addition, we suggest adaptive learning of legitimate RSS values which enhances the robustness of the attack detector against environmental changes. Using both magnitude and frequency related features, we achieved high detection performance with a single AM; this enables development of preventive measures for spoofing attacks. The performance of our approach was evaluated through an IEEE 802.15.4 testbed in an office environment. Experimental results along with theoretical analysis show that the proposed method outperforms the existing RSS-based spoofing detection solutions. Using a single AM, we were able to attain 94.75% detection rate (DR) with 0.56% false positive rate (FPR). For 4 AMs, the results improved to 99% DR and 0% FPR.

1. Introduction

The shared medium used in wireless networks makes them inherently vulnerable to many cyber security threats. Identity spoofing is an important class of attacks which by exploiting the openness property of transmission medium is launched more easily in wireless networks compared to wired networks. In a spoofing attack, an adversary masquerades as one or more legitimate nodes, and by forging their identities, injects malicious traffic to affect the normal operation of the network. Spoofing is a basis for several other types of attacks, including various types of denial of service (DoS), session hijacking, etc. Therefore, designing appropriate spoofing detection and prevention mechanisms is of crucial importance and an open research topic.

Most existing systems rely on cryptographic methods to prevent spoofing attacks. However, the long history of breaking the authentication and encryption mechanisms employed in wireless networks shows the inadequateness of such approaches in guaranteeing a spoof-free network [1]. Furthermore, a variety of DoS attacks work in layers

* Corresponding author.
E-mail addresses: pariaj@ece.ubc.ca (P. Jokar), nasima@ece.ubc.ca (N. Arianpoo), vleung@ece.ubc.ca (V.C.M. Leung).

1570-8705/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2013.04.015

1 and 2 of the network protocol stack, while encryption usually covers the upper layers. In addition, resource limitations of many wireless devices, such as wireless sensors, hinder implementation of strong cryptographic schemes.

To determine whether an identity belongs to a legitimate entity or has been counterfeited by a malicious node, forge-resistant qualities are exercised. One commonly used characteristic is sequence number of data-link layer frames [2,3]. Sequence numbers are a linear chain of numbers assigned to the frames by network card. It was assumed that since sequence numbers are allotted by network cards, attackers cannot create a stream of packets that match the sequence number of the legitimate traffic. Therefore, the gap between sequence numbers could be employed to detect the presence of the sybil nodes. However, nowadays myriad of free packet generator tools exist which enable the attackers to manipulate the desired fields of every frame.

Another property that has recently attracted the attention of the body of researchers is received signal strength (RSS). According to the physics laws, the signal strength in a receiver antenna is proportional to the spatial distance between the receiver and the sender. Assuming that the sybil and legitimate nodes are located in different places, the RSS spatial correlation can be used to discriminate the entities applying the same identity. Beside distance, RSS depends on wireless environment features, such as absorption and multipath effect, which makes it hard to predict the power level of frames collected by a given receiver. Thus, sybil nodes cannot simply adjust their power levels to match the RSS of the legitimate nodes.

On the other hand, the RSS value is a random variable with Gaussian distribution [4]. While effective for long spatial distances and large differences between RSS, time varying nature of RSS, confines the resolution of RSS-based detection methods. To address this problem, multiple air monitors (AMs) are employed [4–6,9]. Increasing the number of AMs facilitates finer differentiation between entities located in closer distances and/or have close RSS values. The downsides of using multiple AMs are the extra cost required for excessive devices, as well as secure and reliable connections between several AMs and a central server. Moreover, relying on multiple AMs complicates the development of preventive measures. The main contribution of this work is the design of a novel robust RSS-based spoofing detection mechanism with low computational and resource overhead. While existing methods rely on multiple AMs for accurate attack detection, the proposed approach provides a high detection performance with a single AM, and a superior performance over other methods using multiple AMs. In theory, we prove that a single AM that employs the proposed algorithm can outperform a system with 12 AMs that directly uses RSS values such as [5,6,9].

The focus of this work is spoofing detection in static IEEE 802.15.4 networks. Unlike IEEE 802.11b, IEEE 802.15.4 nodes usually do not support technologies like automatic radio management (ARM) and antenna diversity. Therefore, RSS-based techniques can effectively be employed to detect and prevent spoofing attacks. The increasing use of ZigBee (IEEE 802.15.4 defines the physical and medium access control (MAC) layer protocols of the ZigBee standard) networks in sensitive applications necessitates development of appropriate intrusion detection/prevention systems (IDS/IPSs). As a major example, in North America and many other countries, ZigBee has become the dominant technology for home area networks (HANs) within the smart grids. The importance of designing appropriate IDS/IPS for such networks has been emphasized in many literatures [7,8].

In this paper we survey the existing RSS-based spoofing mechanisms, and discuss their weaknesses. Further, we present a novel RSS-based detection method which provides a higher detection performance using less number of AMs. Unlike most existing solutions that directly process the RSS values of the packet stream, we employ feature extraction techniques to reduce data redundancy, and obtain a better representation of the data. We extract two features of RSS streams, ratio of out-of-bound frames, and the summation of detailed coefficients (SDCs) in discrete Haar wavelet transform (DHWT) of the RSS streams. Through theoretical analysis and experiment we show that the SDC distributions of benign and spoofed stream are more separable than RSS distributions; this leads to a better detection performance. In addition, we suggest adaptive learning of RSS mean values, which reduces the false positives imposed by environmental changes.

Finally, we evaluate the performance of our proposed method through an IEEE 802.15.4 testbed in an office building environment. Consistent with theoretical analysis, experimental results show that parallel application of magnitude and frequency features of the RSS stream, along with adaptive learning of mean values, yields a detection method which significantly outperforms the existing approaches. Using a single AM, we were able to achieve 94.75% detection rate (DR) with 0.56% false positive rate (FPR). With four AMs the DR and FPR improved to 99% and 0% when the distance between the legitimate node and attacker was more than one meter.

The remainder of the paper is organized as follows: In Section 2 we survey previous works in related area and discuss the shortcomings and advantageous of each method. The threat model of a spoofing attack is provided in Section 3. Section 4 explains the proposed spoofing detection algorithm. In Section 5 the performance of our approach is analyzed theoretically. Experimental results are described in Section 6. Section 7 includes a discussion on the proposed method and comparison with previous approaches, and Section 8 concludes the paper.

2. Related work

In [4] a method for detecting spoofing attacks in wireless networks based on signalprints was proposed. Signalprint was defined as a vector containing RSS readings in multiple AMs. Signalprints of the traffic generated by a single node are expected to be similar. Dissimilar samples suggest the presence of an attacker. As a dissimilarity measure, number of vector elements differing from a mean value more than a predefined threshold was counted. The threshold value directly depended on the variance of RSS

values. When the out-of-bound elements of a vector exceeded a specific number, an attack alert was raised. For an IEEE 802.11 testbed and 6 AMs, the authors reported 95% DR without mentioning the rate of false positives. This approach requires a high number of AMs to achieve a desirable performance. The authors did not provide any updating mechanism for mean values of the RSS stream in AMs, which may cause a high false positive rate over long term due to the environmental changes.

Spoofing detection in IEEE 802.11 transmitters with antenna diversity was targeted in [5]. The authors showed that as a result of antenna diversity, the RSS distribution function tends to a multi-Gaussian model, instead of the single Gaussian assumed in other literature. They further showed that the difference between the mean RSS values of the traffic generated with different antennas of the same node is more than 5 dB (5 dB is the variance of the RSS Gaussian model used in other literature, which is an important factor in defining threshold values for classifiers.). For each AM, an RSS profile was built; then for a sequence of RSS samples, likelihood-ratio test was performed to detect deviations from the AM profiles. One or two times updating of RSS profiles per day was suggested to deal with the effect of environmental changes on distribution function. In an IEEE 802.11 testbed in an office building, using a single AM they achieved 73.4% DR with 3% FPR. For the same FPR, by increasing the number of AMs to 20, detection rate improved to 97.8%. This work is valuable in that it is the only method effective for multi-antenna transmitters. However, this approach is not efficient for single antenna, since it requires a high number of AMs, high computation and resources. Besides, one or two time profile updates might not be adequate to avoid false positives.

In [6] a technique for detecting spoofing attacks and localizing the position of adversaries was introduced. The authors used *k*-means clustering [6] for attack detection. For each frame, an *N*-dimensional vector of RSS readings in *N* different AMs was defined. Then, utilizing *k*-means algorithm, *M* vectors corresponding to a stream of *M* frames were divided into two clusters. Assuming a Gaussian distribution with 5 dB standard deviation, a threshold was defined for the distance between the centers of the clusters under normal condition. When the distance exceeded the threshold value, a spoofing alert was raised. The performance of the method was tested in both IEEE 802.11 and IEEE 802.15.4 network testbeds, each with four AMs. For FPR less than 10%, [6] achieved a detection rate above 95%. Moreover, [6] studied the effect of the distance between the spoofing and original nodes on detection performance, and concluded that the further away is the spoofer from the original node, the higher is the detection rate. For IEEE 802.11, the detection rate was reported to be more than 90% when the distance is about 13 feet, while for IEEE 802.15.4 the same detection rate was obtained for distances about 20 feet.

The most recent work in the area of RSS-based spoofing detection is [9] which presents methods for spoofing detection, finding the number of attackers, and locating multiple adversaries. For detection phase, they used partitioning around mediod (PAM) algorithm. PAM clustering is similar to *k*-means, yet it is more robust against noise and outliers. For discovering the number of attackers, two methods were suggested, Sillhouette plot and SILENCE. Both methods were based on finding the number of clusters in a clustering problem, where each cluster contains samples of a same distribution. This approach is effective, as long as the adversary node does not change its transmission power. A single attacker utilizing different power levels, can present multiple clusters. The performance of the spoofing detection method was assessed in IEEE 802.11 and IEEE 802.15.4 testbeds, with 5 and 4 AMs orderly. For 5% false positive rate, the detection rate was above 90%, when the distance between the malicious and genuine nodes was less than 15 feet and 20 feet for IEEE 802.11 and IEEE 802.15.4 networks respectively.

The major drawback of clustering-based approaches such as *k*-means and PAM is that when the ratio of malicious traffic significantly outweighs the benign traffic, benign frames are treated by the clustering algorithm as outliers. In this case malicious traffic is divided into two clusters; since both clusters belong to the same origin, the attack will not be detected. Therefore, clustering-based methods cannot detect high traffic rate spoofing attacks which include most of the denial of service (DoS) attacks, such as back-off manipulation attack. In addition, the attacker and the genuine nodes do not necessarily communicate with the victim at the same time. Attack can happen when the genuine node is silent or have a very low traffic rate. Fig. 1 shows the result of *k*-means clustering, when malicious frames constitute 90% of the traffic. The mean value of benign and malicious traffic are (15,15) and (58,58) orderly. As Fig. 1 suggests, in this scenario malicious traffic is divided into two clusters which have close centers, while benign traffic is included in one of the attack clusters.

The only work that by converting the time series of RSS values into frequency domain, tries to provide a more proper representation of the data is [10]. In [10], signal strength Fourier analysis (SSFA) was utilized to detect spoofing attacks. The intuition behind the method was the fact that under normal condition only low-frequency

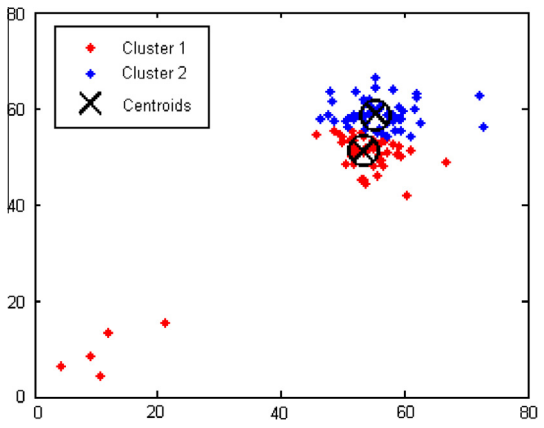

Fig. 1. *k*-Means clustering result when traffic of the attacker constitute 90% of the total number of frames.

oscillations exist. On the other hand, during spoofing attacks, the genuine frames are interleaved with malicious frames which generate high-frequency components. Using fast Fourier transform (FFT), the energy of high-frequency components were compared to a threshold. Passing the threshold value was interpreted as a spoofing attack. The advantage of this method is, using a single AM it can achieve a better detection performance compared to other methods. However, when the traffic rate of the original and spoofing nodes surpasses a specific range, this method will not be effective. Besides, relying on high frequency component of the Fourier transform introduced 0.2 s delay in detection process.

The goal of this work is to provide a resource and time efficient algorithm which detects a vast range of spoofing attacks. While most of the previous works, [4–6,9], tried to improve the detection performance by applying different classification techniques on the raw RSS values, and achieved almost similar results, we focus on providing a thorough and more distinctive representation of the data. We show that projecting the data into a feature space that includes both magnitude and frequency related components, can overcome the limitations of [4–6,9], and allows a high detection performance even with one AM.

Our work is motivated by [10] in leveraging the fluctuations in RSS stream for attack detection. Yet, we take a different approach; instead of FFT and energy of high frequency component, we employ DHWT which is more time and resource efficient. Accordingly we introduce SDC parameter which is highly separable for benign and malicious traffic. In [10] only high frequency components are used for attack detection, which not only imposes a high detection delay, but also is ineffective in detecting high rate attacks. In addition to the fact that DHWT is faster than FFT, by avoiding the reliance on frequency feature for highly separable attacks (high differences between RSS values or high attack ratio), we further improve the detection delay.

Another advantage of the proposed method compared to [4–6,9] is robustness against environmental changes achieved through adaptive learning of legitimate RSS values. Overall, as we show in the rest of the paper, the proposed algorithm provides a significantly higher performance in terms of resources, detection accuracy and false alarms compared to previous works.

3. Threat model

In a spoofing attack, at least three entities are involved: a legitimate node, an attacker, and a victim. The legitimate node is allowed to exchange information and command massages with the victim. The victim uses identity of the legitimate node to decide whether the traffic comes from a genuine node. For instance, MAC address and node ID usually represent the identities in IEEE 802.11 and IEEE 802.15.4 networks. The attacker eavesdrops the network traffic to extract identity of the legitimate node; then, by forging its identity, sends malicious traffic to the victim. Spoofing is used by attackers for a variety of objectives, including but not limited to stealing information, sending falsified data, and gaining access to limited resources. In IEEE 802.15.4, spoofing is the basis of several other types of attacks such as DoS against data transmission during contention free period (CFP), false data injection in guaranteed time slot (GTS) mode, DoS against GTS requests [11], stealing network bandwidth [9], back-off manipulation [12], replay protection, ACK attack and man in the middle [13].

Some capabilities required by an adversary before and during a spoofing attack are:

- Adversary must be able to monitor the network traffic and identify the legitimate users.
- In an encrypted communication, attacker must be able to encrypt/decrypt packets. However, in a variety of DoS attacks this is not necessary, since usually encryption is performed on data packets rather than control signals.
- Adversary needs to adjust the address field and sequence number of the frames using appropriate tools.
- Adversary must be able to inject packets to the network. Therefore, it must be in the proper vicinity of the network nodes dictated by the maximum coverage range according to the physical and MAC layer protocols.

4. Spoofing detection algorithm

Spoofing detection can be formulated as a statistical significance testing problem. The null hypothesis is defined as:

H_0. Benign traffic (no attack)

Test statistics are then used to decide if the observed data belongs to the null hypothesis.

In order to achieve high detection performance in terms of number of AMs, false positive/negative and detection rate, we utilize two parameters to represent the features of the stream of RSS values. We use the ratio of out-of-bound frames, which deals with the magnitude of RSS values. Further, we apply DHWT on time series of RSS values and use SDC to measure the oscillations in the data stream. In a spoofing attack, when both genuine and attacker nodes communicate to the victim during the same period, RSS time series have more fluctuations since the legitimate packets are interleaved by forged packets with possibly different RSS values. In Section 5 we show that under a variety of attack scenarios, SDC provides a more separable distribution function (compared to RSS) which allows an accurate attack detection, even when the genuine and attacker nodes are in close proximity.

4.1. Operation phase

The data stream is divided into windows containing 2^n frames. Selection of the window size is related to the required number of samples as inputs of a DHWT. Following [4–6,9,10] we assume a Gaussian distribution for RSS.

Step 1: For each captured frame, the RSS is compared with the mean value, μ_{global}, of the Gaussian distribution. A counter keeps track of the number of RSS values

differing from the μ_{global} more than a threshold, th_{RSS}. th_{RSS} is related to the variance (σ) of the Gaussian distribution. At the end of each window, the ratio of out-of-bound frames is calculated, $R = n_{out}/n$, where n_{out} is the number of out-of-bound frames. If R lies in the range $R_{\min} < R < R_{\max}$, the algorithm stops at this step and raises an alarm declaring the presence of a spoofing attack. R greater than $R_{\min}$ shows that the number of frames having an out-of-bound RSS value is more than normal; this with a high probability is due to the presence of another entity calming the same identity. However, $R_{\max} < R$ might be the result of alteration of the mean value of the RSS distribution due to the environmental changes rather than a malicious activity. For instance, changing the position of the legitimate node, or putting an object in the communication path can change the RSS distribution. If an attack is not detected at this step, the algorithm continues in step 2.

Step 2: Next step is evaluation of the SDC. SDC is calculated using DHWT; in Section 5 we will briefly introduce DHWT and explain the rational behind using this transformation for feature extraction. Like RSS, SDC has a Gaussian distribution. Knowing the mean value and variance of SDC for a given node under normal condition, for each window SDC is compared with a threshold, th_{SDC}; if the threshold is exceeded, an attack alert is triggered. In addition to SDC, DHWT calculates the mean value of the frames inside the window, μ_w.

Step 3: As the final step, if $R_{\max} < R$ and step 2 did not detect a spoofing attack, an extra check is performed. $R_{\max} < R$ can be a result of two conditions, shift of the mean value due to the environmental changes, or presence of an attacker with a much higher traffic rate compared to the genuine node. Therefore, in order to decide whether an attack alarm should be raised, or the mean value requires update, detection system sends a sequence of packets to the receiver, for instance a stream of data packets that require acknowledgment or internet control message protocol (ICMP) massages such as PING, if ICMP is supported. Using this method, the detection system forces the genuine node to transmit packets with the traffic rate comparable to the traffic rate of the attacker. We assume that the attacker does not block the genuine node from replying to the messages. This can be monitored through secure hello messages. An alternative and more secure method which in computationally more expensive is to exchange a series of challenge responses. The detection system then can be sure that a sufficiently large portion of the received frames comes from the genuine node. After passing an expected time for receiving the replies, the algorithm is repeated from the first step. This time if still $R_{\max} < R$ and an attack has not been detected until this step, the algorithm decides that the traffic is benign and the mean value is updated by replacing μ_{global} with μ_w.

4.2. Training phase

To effectively detect spoofing attacks, the algorithm uses four threshold values, th_{RSS}, th_{SDC}, $R_{\min}$, $R_{\max}$. Except $R_{\max}$ which is a fixed parameter close to one, other thresholds are learnt through a training phase in which the network is assumed to be spoof-free. First the mean, μ_{RSS}, and variance, σ_{RSS}, of the RSS stream over the whole training duration are calculated. th_{RSS} is defined as $th_{RSS} = \sigma_{RSS}$.

In the next step, the RSS stream is divided into windows of 2^n frames. For each window, R (using μ_{RSS} and σ_{RSS}) and SDC are calculated. According to the distribution of R and SDC over several windows, the following parameters are extracted:

- Mean value and variance of R (μ_R and σ_R).
- Mean value and variance of SDC (μ_{SDC} and σ_{SDC}).
- Ten largest values of R ($R_{MAX} = \{R_{MAX1}, \ldots, R_{MAX10}\}$ in descending order)
- Ten largest values of SDC ($SDC_{MAX} = \{SDC_{MAX1}, \ldots, SDC_{MAX10}\}$in descending order)

Numerical values are assigned to $R_{\min}$ and th_{SDC} using the above parameters. $R_{\min}$ and th_{SDC} dictate the trade-off between DR and FPR. When very low FPR is required, R_{MAX} and SDC_{MAX} are used. (application of R_{MAX1} and SDC_{MAX1} results in close to 0% FPR) Otherwise, the threshold values can be defined according to the parameters of Gaussian distributions. One option is the combination in (1) which minimizes the FPR at the first step of the algorithm and provides a good detection rate for the second step; however, depending on the application and security policy, appropriate balance between DR and FPR are achievable by adjusting the thresholds:

$$\begin{cases} R_{\min} \in R_{MAX} \\ th_{SDC} = \mu_{SDC} + 3\sigma_{SDC} \end{cases} \quad (1)$$

A pseudo code of the above algorithm is provided in the following:

Training Phase:

Input: $\{RSS_i\}$ with $i = \{1, \ldots, l\}$, n;
Output: th_{RSS}, th_{SDC}, $R_{\min}$, μ_{global};
μ_{global} = mean of $\{RSS_i\}$;
σ_{RSS} = variance of $\{RSS_i\}$;
$th_{RSS} = \sigma_{RSS}$;
for $j = 1$ to $i < \lfloor l/2^n \rfloor$ do
  //calculate and store R for each window.
  for $i = 1$ to 2^n do
    if $|RSS_i - \mu_{global}| > th_{RSS}$
      n_{out}++;
    end if;
  end for;
  $R[j] = \frac{n_{out}}{n}$;
  $n_{out} = 0$;
  //calculate and store SDC for each window.
  apply DHWT and find detailed coefficients $\{dc_k\}$
  $SDC[j] = \sum_{k=1}^{2^n-1} dc_k$;
end for;
sort $R[j]$ and find $R_{MAX} = \{R_{MAX1}, \ldots, R_{MAX10}\}$;
$\mu_{SDC} = Mean\{SDC_j\}$
$\sigma_{SDC} = Variance\{SDC_j\}$
$R_{\min} \in R_{MAX}$;
$th_{SDC} = \mu_{SDC} + 3\sigma_{SDC}$;

Operation Phase:

Input: $\{RSS_i\}$, n, th_{RSS}, th_{SDC}, $R_{\min}$, $R_{\max}$, μ_{global};
Output: attack (Boolean variable initialized as false);
for $i = 1$ to 2^n do
  if $|RSS_i - \mu_{global}| > th_{RSS}$
    n_{out}++;
  end if;
end for;
$R = \frac{n_{out}}{n}$;
$n_{out} = 0$;
if $R_{\min} < R < R_{\max}$ do
  attack = true;
  end of the algorithm;
else
  apply DHWT and find detailed coefficients $\{dc_k\}$ and μ_w;
  $SDC[j] = \sum_{k=1}^{2^n-1} dc_k$;
  if $SDC > th_{SDC}$ do
    attack = true;
    end of the algorithm;
  end if
end if;
if $R > R_{\max}$ and attack==false
  if flag = 1 do
    $\mu_{global} = \mu_w$;
    flag = 0;
    end of the algorithm;
  else
    send a packet stream to the node and wait for response;
    flag = 1;
    repeat the algorithm;
  end if
else
  attack = false;
end if
end

4.3. Multiple AMs

When the detection system contains more than one AM, the RSS readings of the AMs are transferred to a central server (CS). All computations are performed in the CS and the AMs are only responsible for reading the RSS values of the receiving frames from the target nodes, as well as sending packets to a given node for mean update. Based on the AM reports, the CS makes a global decision about the health or malice of traffic. Using the RSS readings of different AMs, the CS makes an RSS vector for each frame. Reports of different AMs might be received by CS with different delays. The CS assumes that the reports within a predefined time interval (according to the delay estimation) belong to the same frame. If a report from a specific AM is not received by the CS in the expected time, the mean RSS of that AM is used in the RSS vector.

The detection algorithm for multi-AM scheme is summarized as follow:

1. For each AM, the thresholds and algorithm parameters are learnt through a training phase similar to what was described in the above.
2. During the operation phase, for each window, CS calculates the ratio of out-of-bound frames. This time a frame is considered to be out-of-bound if (2) is true,

$$\left\| \overrightarrow{RSS} - \overrightarrow{\mu_{RSS}} \right\| > \left\| \overrightarrow{\sigma_{RSS}} \right\| \tag{2}$$

where $\overrightarrow{RSS}, \overrightarrow{\mu_{RSS}}, \overrightarrow{\sigma_{RSS}}$ are vectors with n components, containing the RSS readings, mean and variance of RSS (learnt in the training phase) of n AMs. $\|\cdot\|$ denotes the Euclidean distance. If $R_{\min} < R < R_{\max}$ attack is detected and the algorithm ends for the current window. $R_{\min}$ is learnt in the training phase similar to the single AM method.

1. For each AM the SDC of the current window is calculated. An attack is detected if (3) is true,

$$\left\| \overrightarrow{SDC} - \overrightarrow{\mu_{SDC}} \right\| > 3 \left\| \overrightarrow{\sigma_{SDC}} \right\| \tag{3}$$

where $\overrightarrow{SDC}, \overrightarrow{\mu_{SDC}}, \overrightarrow{\sigma_{SDC}}$ are vectors with n components, containing the SDC, mean and variance of SDC for n AMs.

1. If $R > R_{\max}$ a notification is sent to the AMs. In response, each AM transmits a packet stream to the target node and mean update mechanism is initiated.

The communication between AMs and the CS can be wired or wireless; either way, it must be highly secure, for instance through implementation of secure authentication and encryption algorithms. Especially, for wireless communication, the attack detection system must not be subject to spoofing attacks itself. Therefore, in multi-AM scheme, not only several AMs are required, but also AMs need high resources to ensure the security of the spoofing detection system.

When the CS detects an attack, it can send a notification to the victim to inform it about the illegitimacy of the traffic. The victim then can discard the received frames during the attack. However, in multi-AM scheme once the attack is detected, informing the victim that which frames are legitimate and which are not, without implementing a complementary algorithm in the victim node, if not impossible is very hard. At the same time, discarding all frames during an attack will lead to DoS. Therefore, while multi-AM provides high detection performance and is suitable when there is an administrator who reacts upon intrusion detection alarms, it is not appropriate for automatic preventive measures. On the other hand, in a single AM detector, the victim can be the detector; therefore, it knows which frames are benign and which are illegitimate; thus, during the attack it only discards frames that with a high probability are malicious.

The above discussion highlights the advantages of designing a high performance single-AM spoofing detector which is the major contribution of this work.

5. Theoretical analysis

In the proposed spoofing detection approach, we exploit the spatial correlation of RSS values to determine whether the incoming frames, carrying the same identity,

belong to a single genuine node, or are originated from different sources. The RSS of a frame measured in a given location (landmark) is affected by parameters such as environmental condition, random noise and multipath effect; still it strongly depends on the distance between the sender and the receiver. As a result, RSS of devices located at different physical places are expected to be distinctive. The spatial dependency of RSS is formulated as.

$$RSS = P_0 - 10\gamma \log\left(\frac{d_1}{d_0}\right) + X \tag{4}$$

where P_0 is the transmission power in a reference point, d_0 and d_1 are the distance from the sender to the reference point and to the receiver, γ is the path loss exponent and X is the shadow fading with a Gaussian distribution $N(0,\sigma)$.

Having the configuration in Fig. 2a, and assuming an equal transmission power for nodes 1 and 2, the difference between RSS values of the two nodes, sensed by node 3 is:

$$\Delta RSS = 10\gamma \log\left(\frac{d1}{d2}\right) + \Delta X \tag{5}$$

where ΔX has a Gaussian distribution $N(0,\sqrt{2}\sigma)$.RSS values in a landmark also follow a Gaussian distribution $N(\mu,\sigma)$; while σ depends on environmental condition, its average in an indoor location is reported to be about 5 dB [4–6,9].

Knowing the above physical properties, at the rest of this section we prove the efficiency of the proposed algorithm in detecting spoofing attacks through mathematical analysis.

Step 1: As the first detection step, assuming the distribution function of $N(\mu_g,\sigma_g)$ for the genuine node, for each window the number of frames differing from the mean value, μ_g, more than σ_g is counted as nout. Then parameter $R = n_{out}/n$ is compared with a threshold $\tau(0 < \tau < 1)$. The value of R under normal condition is proportional to the area denoted by dots in Fig. 2b. Presence of an attacker, increases the value of R, since in this case nout will be related to the summation of dotted and crossed areas. Smaller value of τ results in a higher DR, yet it increases the FPR. We formulate the FPR as (6), which is the probability of R exceeding the threshold, when there is no attacker.

$$FPR = \Pr(R > \tau|normal) = \Pr(n_{out} > \tau n|normal) \tag{6}$$

$$\Pr_{normal}(RSS) = N(\mu_g,\sigma_g) \tag{7}$$

The probability that from n frames n_{out} are out of a boundary, follows a binomial distribution.

$$\Pr(n_{out}|normal) = \binom{n}{n_{out}} P_{out}^{n_{out}}(1-P_{out})^{(n-n_{out})} \tag{8}$$

$$P_{out} = \Pr_{normal}(|RSS-\mu_g| > \sigma_g) = 2\Phi(\mu_g - \sigma_g;\mu_g,\sigma_g) \tag{9}$$

where P_{out} is the probability of a frame having an out-of-bound RSS under normal condition. In (8), $\Phi(\cdot)$ is the cumulative distribution function (CDF) of the Gaussian distribution. Considering (6) and (8) the FPR is:

$$FPR = \sum_{n_{out}=\tau n}^{n} \Pr(n_{out}|normal) = 1 - F(\tau n; n, P_{out}) \tag{10}$$

where $F(.)$ is the CDF of the binomial distribution.

As the above formula suggests, FPR is inversely related to τ. On the other hand DR is formulated as below:

$$DR = \Pr(R > \tau|attack) = \Pr(n_{out} > \tau n|attack) \tag{11}$$

Considering a Gaussian distribution for the attacker, $N(\mu_a,\sigma_a)$, PDF of the RSS values under attack is:

$$\Pr_{attack}(RSS) = (1-\eta)N(\mu_g,\sigma_g) + \eta N(\mu_a,\sigma_a) \tag{12}$$

where η is the ratio of the spoofed frames. Similar to the explanation for FPR, n_{out} has a binomial PDF.

$$\Pr(n_{out}|attack) = \binom{n}{n_{out}} (P'_{out})^{n_{out}}(1-P'_{out})^{(n-n_{out})} \tag{13}$$

where p'_{out} is the probability of a frame having an out-of-bound RSS under attack condition, considering (12):

$$P'_{out} = 2(1-\eta)\phi(\mu_g - \sigma_g;\mu_g,\sigma_g) + \eta Q(\mu_g + \sigma_g;\mu_a,\sigma_a) \tag{14}$$

In (14), Q is the Q-function (the complement of the CDF) of the Gaussian distribution. Finally, DR can be summarized as:

$$DR = 1 - F(\tau n; n, P'_{out}) \tag{15}$$

From the above equations and considering Fig. 2b, one can conclude that DR is a function of τ, η, $|\mu_g - \mu_a|$, σ_g and σ_a. The influence of η and $|\mu_g - \mu_a|$ on detection performance, in terms of receiver operating characteristic (ROC), is depicted in Fig. 3a and b. τ defines the tradeoff between FPR and DR. From Fig. 3a it can be seen that as the ratio

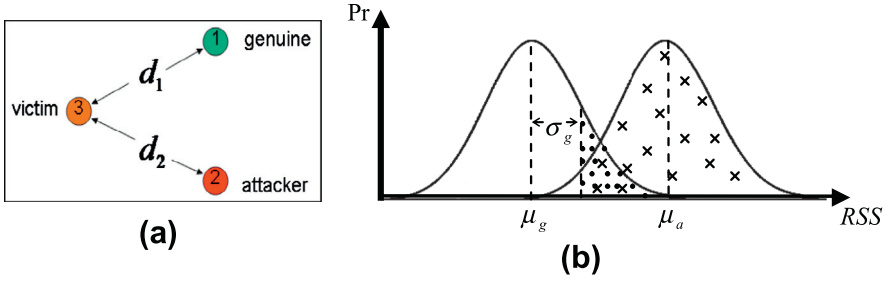

Fig. 2. (a) Attack scenario. (b) CDF of the RSS values of the attacker and the genuine node.

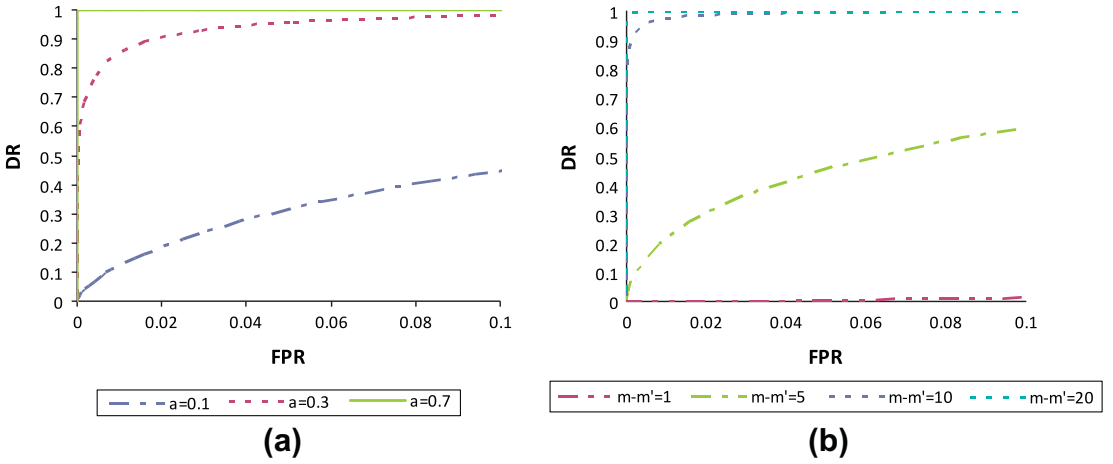

Fig. 3. Effect of (a) malicious traffic ratio (a), and (b) difference between mean values of RSS distribution on detection performance using *R*.

of malicious frames increases the detection performance improves.

As it was expected, Fig. 3b shows that detection performance improves when the distance between mean values increases. On the other hand enlargement of variance degrades the detection performance. In summary, the more separable are the distribution functions of attacker and the genuine node, the better is the detection performance.

In step two of the algorithm, by applying DHWT on the RSS stream, we achieve a parameter with more separable distribution for a given RSS stream.

Step 2: In this step, for each window, the DHWT is utilized to provide a measure of oscillations in RSS values. While fast Fourier transform (FFT) have been widely used to extract frequency components of time series, discrete wavelet transform (DWT) is proved to be a superior alternative in many applications. The DHWT has the desirable features of wavelet transform. Not only it contains the frequency content of the input, but also shows the temporal order. Another advantage of DHWT is the low number of required operations, which makes it time and resource effective. Computing DHWT of N points takes O(N) arithmetic operations, which is much less than O(N∗logN) required for FFT. Resource and time efficiency are the major reasons why we employed DHWT in our detection algorithm.

Fig. 4 shows the decomposition process in a wavelet transform. In the figure, $g[n]$ and $h[n]$ are low pass and high pass filters which must be quadratic mirror. At each level, the input stream is decomposed into low and high frequencies. The outputs of low-pass and high-pass filters are called approximation coefficients and detail coefficients respectively. In summary, DHWT pairs up the input values, stores the differences, and passes the sums to the next level. The process is repeated until finally $2^n - 1$ differences and a mean value remain [14].

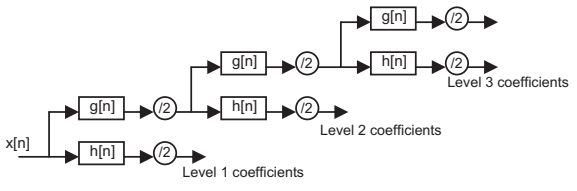

Fig. 4. Discrete wavelet transform decomposition algorithm.

Assume that m AMs are monitoring the RSS values of the frames with identity of a legitimate node. ΔRSS, which is the total RSS deviation from the mean values in m landmark is calculated as:

$$\Delta RSS^2 = \sum_{i=1}^{m} (RSS_i - \mu_{gi})^2 \tag{16}$$

where RSS_i is the value of RSS in landmark i, and μ_{gi} is the mean RSS of genuine node in landmark i. As it was shown in [9], when the two nodes are co-located (there is no attack), the random variable $X = \Delta RSS^2$ has a central Chi-square distribution $\chi^2(m)$, where m is the degree of freedom which is equal to the number of AMs. On the other hand, when wireless nodes are at different locations, X follows a non-central Chi-square distribution $\chi^2(m, \lambda)$, where m is the degree of freedom and λ is the non-centrality parameter, which in this case is:

$$\lambda = \sum_{i=1}^{m} \left(\frac{\mu_{gi} - \mu_{ai}}{\sigma} \right)^2 \tag{17}$$

In (17), μ_{gi} and μ_{ai} are the mean values of RSS stream of the genuine and attacker nodes in ith AM. The variance is assumed to be the same for both nodes, σ. Therefore, the DR and FPR are calculated using the following equations.

$$DR = P(x > \tau | attack) = 1 - F_{\chi^2\left(m, \frac{\lambda}{2\sigma^2}\right)}\left(\frac{\tau}{2\sigma^2}\right) \tag{18}$$

$$FPR = P(x > \tau | normal) = 1 - F_{\chi^2(m)}\left(\frac{\tau}{2\sigma^2}\right) \tag{19}$$

where $F_\chi(\cdot)$ is the CDF of χ, and τ is a threshold. When τ is exceeded, a spoofing attack is detected.

While τ explains the trade-off between DR and FPR, DR is affected by m, σ, and λ. To achieve a higher DR, previous works increased the number of AMs (m). To further improve the detection performance, we suggest application of frequency components; instead of $X = \Delta RSS^2$, we define the random variable X as $X = \Delta SDC^2$ where,

$$\Delta SDC^2 = \sum_{i=1}^{m} (SDC_i - \mu_{SDCgi})^2 \tag{20}$$

where μ_{SDCgi} is the mean of SDC of the genuine node in the ith AM and,

$$SDC_i = \sum_{j=1}^{n-1} dc_i[j] \tag{21}$$

In (21), n is the window size and $dc_i[j]$ is the jth detail coefficient, starting from the high frequencies, for ith AM.

Assume that the legitimate node sends a frame stream with RSS values $S_g = \{s_{g1}, s_{g2}, \ldots, s_{gn/2}\}$, where $S_g \sim N(\mu_g, \sigma_g)$. At the same time attacker sends the stream with RSS values of $S_a = \{s_{a1}, s_{a2}, \ldots, s_{an/2}\}$, $S_a \sim N(\mu_a, \sigma_a)$. For simplicity of analysis we consider an ideal case when the ratio of malicious traffic is 0.5, and each pair of legitimate frames is interleaved by one malicious frame. Then the RSS stream in an AM is: $S = \{s_{g1}, s_{a1}, vs_{g2}, s_{a2}, \ldots, s_{gn/2}, s_{an/2}\}$. By applying DHWT on S, level 1 detail coefficients are: $\{\frac{s_{g1}-s_{a1}}{2}, \frac{s_{g2}-s_{a2}}{2}, \ldots, \frac{s_{gn/2}-s_{an/2}}{2}\}$. For simplicity we ignore higher level detail coefficients (Including higher level coefficients will have a positive effect on separability of SDC).

The SDC of the first level detail coefficients is $SDC_{S1} = \sum_{i=1}^{n/2} \frac{s_{gi}-s_{ai}}{2}$. Considering the summation property of Gaussian variables $(\sum_i a_i N(\mu_i, \sigma_i) = N(\sum_i a_i \mu_i, \sqrt{\sum_i a_i^2 \sigma_i^2}))$, and assuming the same variance for both attacker and genuine nodes $SDC_{S1} \sim N(\frac{n}{4}(\mu_g - \mu_a), \frac{\sqrt{n}}{2}\sigma)$, while $SDC_{S_g 1} \sim N(0, \frac{\sqrt{n}}{2}\sigma)$. Therefore, $\Delta SDC \sim N\left(\frac{n}{4}(\mu_g - \mu_a), \frac{\sqrt{n}}{2}\sigma\right)$, while $\Delta RSS \sim N(\mu_g - \mu_a, \sigma)$.

Thus, for $n = 64$ as it can be calculated from (17), the λ of ΔSDC is 16 times the λ of ΔRSS.

However, we remind that this is for an ideal case, where benign frames are alternatively interleaved by malicious frames. Also the higher level coefficients are ignored. Therefore, the above computation provides an estimate of improvement of λ rather than a deterministic value.

According to (18) and (19), Fig. 5 compares the effect of increase in the number of AMs and non-centrality on detection performance. It can be seen in the figure that when the non-centrality parameter is scaled by 4, the detection performance of single AM outperforms the performance of a system with 12 AMs which has a fixed non-centrality. Other parameters of Fig. 5 are: $\mu_g - \mu_a = 10$ and $\sigma = 5$.

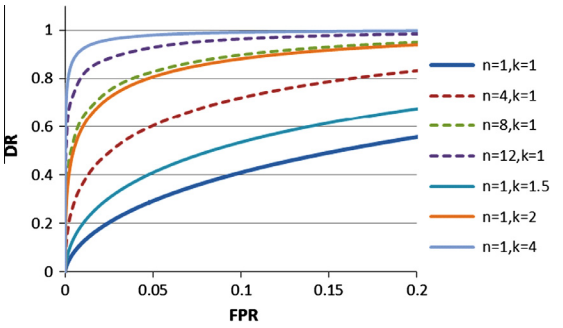

Fig. 5. Effect of increase in the number of AMs and non-centrality parameter (n presents the number of AMs and k is the scale of non-centrality).

6. Experiment

6.1. Testbed

In order to evaluate the performance of our spoofing detection approach, we conducted two experiments in an IEEE 802.15.4 network testbed. The network was established in a real office environment located in communication lab, in Electrical and Computer Department at the University of British Columbia. The office size is 9903 ft^2. The network contained four landmarks (AMs), an attacker and a genuine node. We used six telosB motes as network nodes; four were programmed to act as AMs to monitor the RSS of received frames. The AM motes were connected to four personal computer (PC) systems, and the RSS readings were directly transferred to the PCs .Two other motes which had the role of the attacker and the genuine node, were programmed to send constant bit rate (CBR) traffic with 5 frames per second. The position of the AMs and the genuine node are depicted in Fig. 6 by arrows and a star sign respectively. During the course of experiments the attacker was placed in different locations depicted in Fig. 6 by bold dots.

6.2. Experiment 1

The goal of the first experiment was to study the changes in SDC, under normal and attack conditions. We wanted to confirm that in practice ΔSDC provides a more separable representation of the data, compared to ΔRSS.

In this experiment, first the RSS logs of genuine node frames were collected by AM3 for the duration of four hours. Then, the SDCs of RSS streams were extracted, and the mean value and variance of SDCs were calculated. In computing the SDC, we used the absolute value of DCs to avoid cancelation of DCs with different polarities. The window size was set to 64. In the next step, the attacker node was placed in 50 cm, 1 m, 3 m, 4 m and 5 m distance from the genuine nodes. For each position RSS log of genuine and attacker nodes were captured for 1 h, and the mean value and variance of SDC were calculated. The ratio of malicious and benign traffic was 0.5. The experiment results are presented in Table 1. As it can be seen from the table, ΔSDC provides a larger λ in several orders of magnitude. In addition, when the distance between two nodes expands, λ increases. Table 1 also includes the result of single AM spoofing detection using the proposed algorithm for each dataset. Even when the distance is as low as 50 cm, using SDC, attack detection is to some extent possible, while RSS based approach is completely incompetent due to the similar mean values. As the distance increases

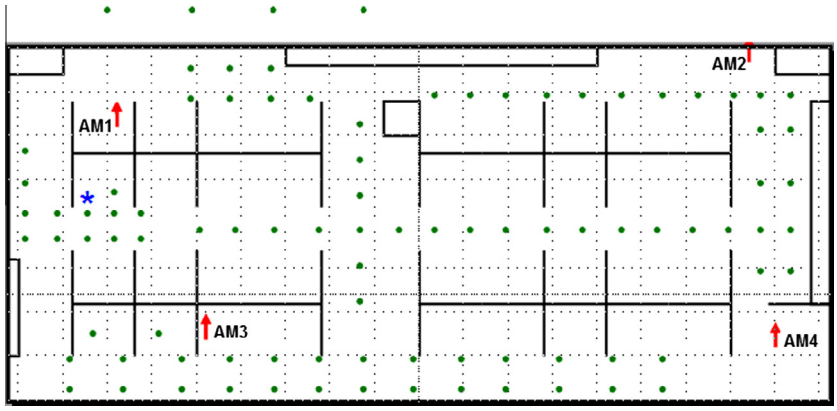

Fig. 6. Testbed setting (the distance between consecutive grid dots is 50 cm).

Table 1
Comparison between λ of RSS and SDC.

Distance	Mean RSS	Var. RSS	Mean SDC	Var. SDC	λ RSS	λ SDC	DR (%) SDC	FPR (%) SDC
0 (leg. node)	−67	4.24	8	13	–	–	–	–
50 cm	−67	2.96	19	16	0	0.14	70.37	23.07
1 m	−62	2.1	70	22	0.62	3.13	84.21	11.11
3 m	−59	2.33	122	26.73	1.46	8.23	98.08	2.56
4 m	−55	3.93	188	35.4	2.16	15.05	99.33	0

to 3 m, the detection performance improves to a satisfactory level. In previous works, on the other hand, even with multiple AMs, the minimum detectable distance was reported to be about 6 m.

6.3. Experiment 2

In the next experiment we evaluated the performance of the proposed spoofing detection mechanism. In the testbed, the attacker node was placed in each position marked by a bold dot in Fig. 6, for 5 min, and transmitted CBR traffic. During the whole experiment the benign node was located at the position depicted by a star in the figure, and sent CBR traffic with the same rate as the attacker. Overall, 90 different placements of attacker and benign nodes were tested. The 4 AMs, monitored the stream of RSS values from both the attacker and the genuine nodes, and stored the values in a log file. At the end of the experiment the log files were collected and the detection algorithm was applied for each AM separately. We used 4 AMs for a single AM detector and analyzed the results separately to study the effect of the position of AM on detection performance. The detection performance of each AM is depicted in Fig. 7. As the figure suggests, AM1 has the best detection performance. The reason is the closer distance of AM1 to the genuine node. We remind that according to (5), attack detection depends on the ratio of distance between attacker and genuine nodes to the AM, rather than the distance between 2 nodes. Therefore, for a fixed distance between the nodes, a closer AM has a better chance of attack detection.

While the experiment was conducted in an office building with usual amount of people movement, to study the effect of moving objects, we deliberately introduced more movements in close proximity of AM3. As Fig. 7 shows, we observed worst but still acceptable performance for this AM.

To further study the effectiveness of the magnitude and frequency features on detection process, Fig. 7 also includes the ROC curve of the detection processes purely based on magnitude (R) and frequency (SDC) features. As it can be seen in Fig. 7, SDC provides a better detection performance. Also we can see that combining both features, significantly improves the performance.

We also studied the effect of the ratio of malicious and benign traffic. The results are shown in Fig. 8. When the rate of malicious and benign traffic is close, the fluctuations in RSS stream is high, therefore, SDC can effectively distinguish the malicious traffic. However, when the ratio of malicious traffic is very high, the RSS stream will have less fluctuations, since the traffic will mostly belong to one node (the attacker in this case). Yet as discussed in Section 5, step 1 of the algorithm will be very effective in this scenario. Therefore, by applying both features the spoofing detection mechanism can successfully detect a vast range of malicious traffic ratio. However, when the traffic rate of the benign node is much higher than that of the malicious node, the algorithm will not be effective. Yet, such scenario can be less hazardous. At least most DoS attacks require high traffic rate. Fig. 8 presents the ROC curve of the spoofing detection in AM4 using R, SDC and both features under various attack ratios.

7. Discussions and comparisons with previous work

A summary of various RSS-based spoofing detection methods is provided in Table 2. The datasets used for performance evaluation in experimental section of the papers

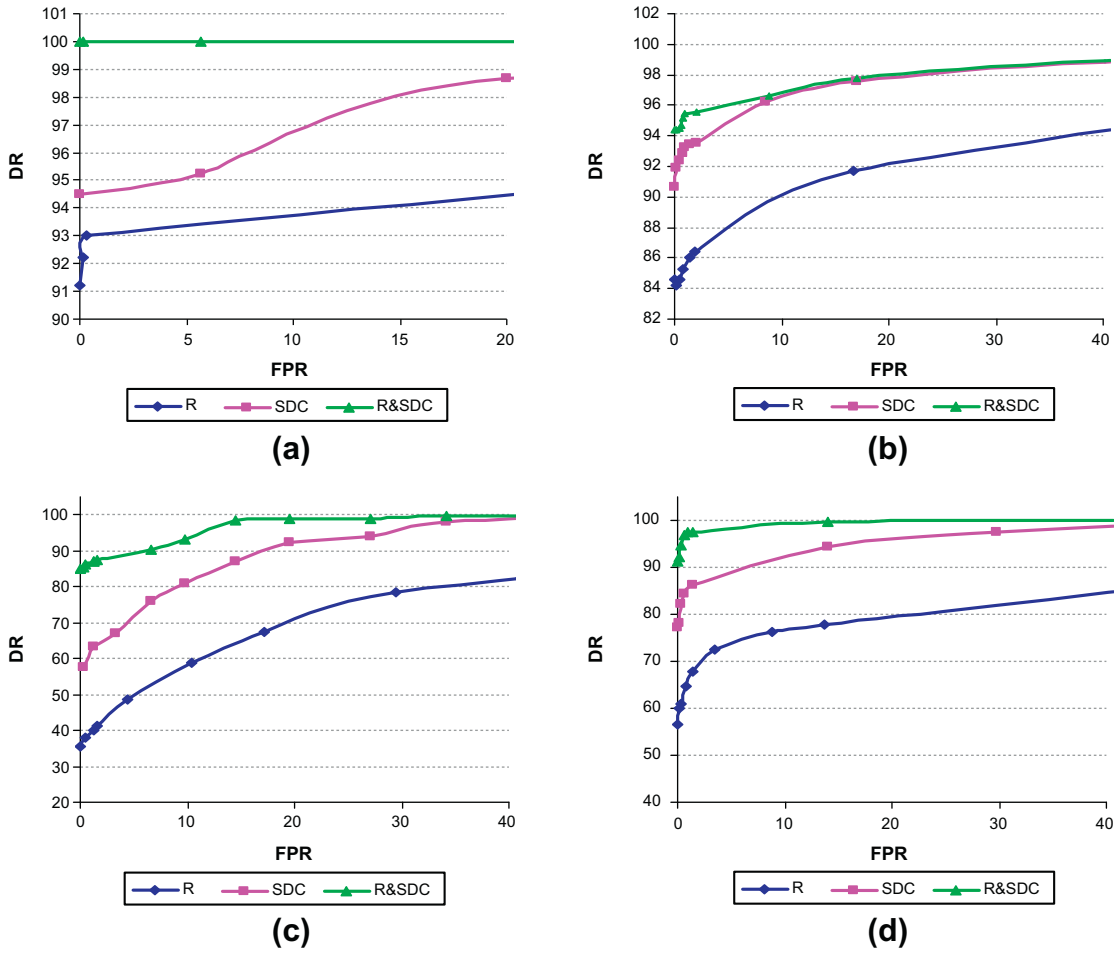

Fig. 7. ROC curve of the spoofing detection algorithms for (a) AM1, (b) AM2, (c) AM3, (d) AM4.

are not the same. Yet, similar approaches have been taken in setting up the testbeds. In some papers both IEEE 802.11 and IEEE 802.15.4 networks were evaluated. In this case we only included the IEEE 802.15.4 results since it is the focus of this work. If the experiments were merely based on WiFi, we included the IEEE 802.11 results. According to [6,9], the detection performance for IEEE 802.11 and IEEE 802.15.4 is close. Though, the minimum distance for detectable attacks in IEEE 802.15.4 is a little higher (about 5 feet) than IEEE 802.11.

As Table 2 shows the test area in our experiment was smaller than other works. However, we argue that smaller area is not in favor of the detection performance; since larger testbed includes more samples with farther distances between attacker and original nodes which as discussed earlier, increases the chance of attack detection.

From Table 2, it can be seen that for both single AM and multi-AMs our method outperforms other approaches. Especially, for single AM other methods have a weak performance. Beside lower cost, space efficiency and increased security, single AM detection, facilitates development of preventive measures. The detector can be implemented on sensitive nodes in a network and whenever a spoofing attack is detected, abnormal frames (in terms of RSS value) would be denied by the receiver. While for multi-AM detection, even when an attack is detected, informing the victim node that which frames are malicious is problematic.

Two step attack detection based on the two RSS stream features, not only improves the number of required AMs, FPR and DR, but also is more time and resource efficient. When RSS values are highly separable (due to the large distance between nodes or high attack rate) attack is detected in step 1 which is very fast and requires little operations. In other methods the same mechanism is employed in all cases; this for instance in [9,10] introduces a high detection delay, even when attacker and genuine nodes are highly distinct (in terms of RSS value). The algorithm delay further depends on the window size. Larger window size poses higher delay, yet improves the detection performance.

Single AM detector might seem inefficient when attacker and benign nodes have the same distance to the AM, although located in different and possibly far locations. Still, dependency of RSS on factors such as path loss and multi path effect increases the chance of attack detection even for this scenario.

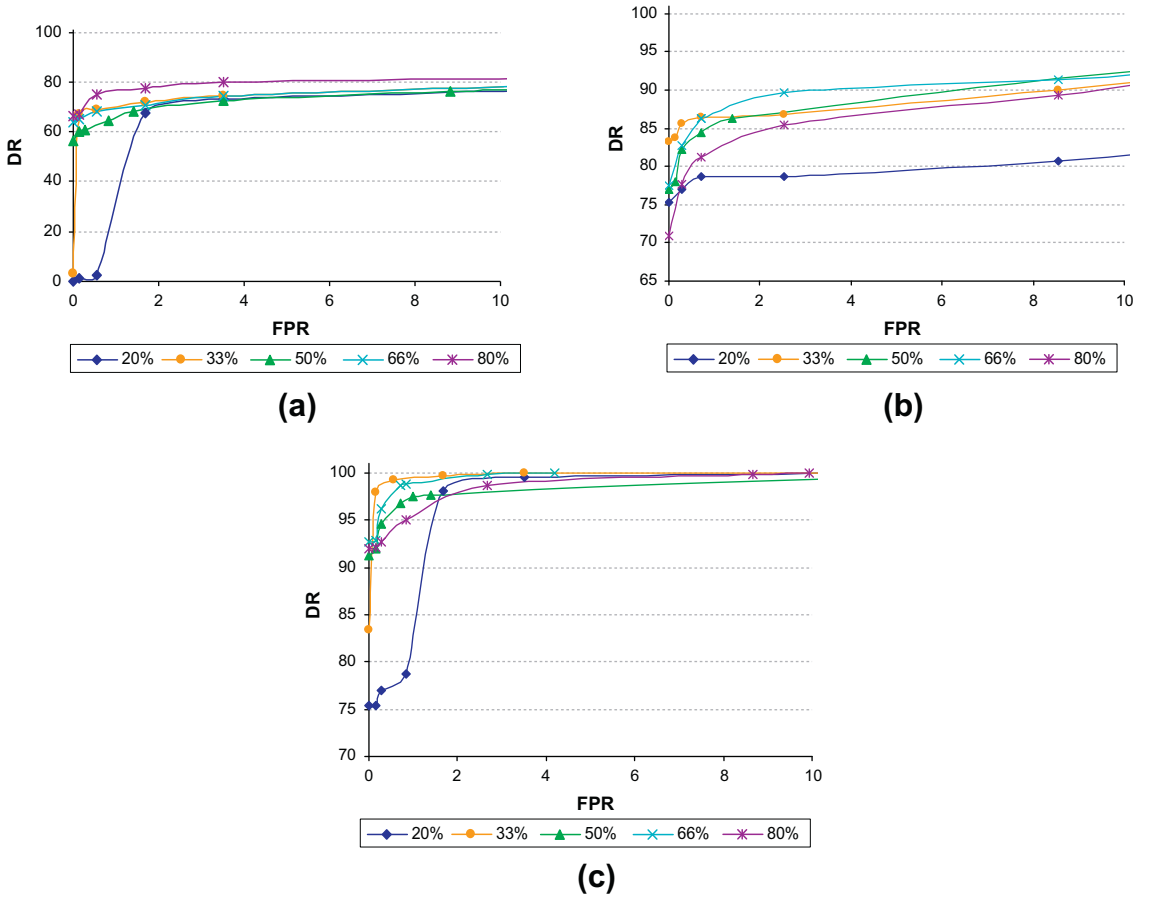

Fig. 8. ROC of spoofing detection in AM4 based on (a) *R*, (b) SDC, (c) proposed algorithm (R&SDC). The vertical axis shows DR percentage while the horizontal axis is the percentage of FPR.

Table 2
Comparison of different RSS-based spoofing detection techniques.

Approach	Test area (ft^2)	Network type	DR 1 AM (%)	FPR 1 AM (%)	# of AMs	DR (%)	FR (%)	Minimum distance (ft)	DR (%)	FR (%)	Resistant to env. changes	Detection of high rate attack
R&SDC	9903	802.15.4	* 92.63 94.75	* 0.00 0.56	4	99	0.0	9.84	98.08	2.56	Yes	Yes
k-Means [6]	16,000	802.15.4	–	–	4	95.7 98	0.0 9.5	20.00	90.0	–	Yes	No
PAM [9]	16,000	802.15.4	–	–	4	96.5 98.5	0.0 10	20.00	90.0	5	Yes	No
Fourier [9]	–	802.11	80.42	0.05	NA	NA	NA	–	–	–	Yes	No
Signalprint [4]	11,625	802.11	NA	NA	6	95.6	–	16.40	72.2	–	No	Yes
Multi-Gaussian [5]	16,000	802.11	64.4	1.00	20	94.4 97.8	1.0 3.0	9.84	84.3	1	No	Yes

(NA: not applicable, –: was not provided in the paper, *: average of the results of 4 AMs).

8. Conclusion

In this work we have studied the existing RSS-based spoofing detection methods for static IEEE 802.15.4 networks and explained the limitations of the existing approaches. In addition to long detection delay, ineffectiveness in mitigating high rate attacks and lack of robustness against environmental changes, most existing approaches rely on multiple AMs which discourage implementation of intrusion prevention techniques. Further, we have presented a novel spoofing detection technique which employs both magnitude and frequency features

of RSS streams to provide a high detection performance even with a single AM. Evaluations of the proposed method through theoretical and experimental analysis have proved its high performance both for single and multi-AMs. Therefore, in addition to introducing an efficient approach for spoofing detection, for the first time we have provided an effective and low-cost method that facilitates deployment of automatic RSS-based spoofing prevention techniques in static IEEE 802.15.4 networks.

Acknowledgment

This work is supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada through grant STPGP 396838.

References

[1] A. Bittau, M. Handley, J. Lackey, The final nail in WEP's coffin, in: IEEE Symposium on Security and Privacy, 2006.
[2] O. Li, W. Trappe, Relationship-based detection of spoofing related anomalous traffic in ad hoc networks, in: IEEE SECON, 2006.
[3] F. Guo, T. Chiueh, Sequence number-based mac address spoof detection, in: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection, Springer, Berlin/Heidelberg, 2006, pp. 309–329.
[4] D. Faria, D. Cheriton, Detecting identity-based attacks in wireless networks using signalprints, in: ACM Workshop on Wireless Security (WiSe), 2006.
[5] Y. Sheng, K. Tan, G. Chen, D. Kotz, A. Campbell, Detecting 802.11 MAC layer spoofing using received signal strength, in: IEEE INFOCOM, 2008.
[6] Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in: IEEE SECON, 2007.
[7] Smart grid interoperability panel, Cyber security working group, Smart grid cyber security strategy and requirements, 2010.
[8] P. Jokar, N. Arianpoo, V.C.M. Leung, A survey on security issues in smart grids, J. Security Commun. Networks (2012), http://dx.doi.org/10.1002/sec.559.
[9] Jie Yang, Yingying Chen, Wade Trappe, Jerry Cheng, Detection and localization of multiple spoofing attackers in wireless networks, J. IEEE Trans. Parall. Distrib. Syst. 99 (2012).
[10] D.C. Madory, New methods of spoof detection in 802.11b wireless networks, Hanover, NH: M. Eng. Thesis, Dartmouth College, 2006.
[11] R. Sokullu, O. Dagdeviren, I. Korkmaz, On the IEEE 802.15.4 MAC layer attacks: GTS attack, in: Second International Conference on Sensor Technologies and Applications, 2008.
[12] S. Radosavac, A.A. Crdenas, J.S. Baras, G.V. Moustakides, Detecting IEEE 802.11 MAC layer misbehavior in Ad Hoc networks: robust strategies against individual and colluding attackers, J. Comput. Security 15 (2007) 103–128 (Special Issue on Security of Ad Hoc and Sensor Networks).
[13] Y. Xiao, S. Sethi, H.-H. Chen, B. Sun, Security services and enhancements in the IEEE 802.15.4 wireless sensor networks, in: IEEE GLOBECOM'05, 2005.
[14] P.J. Van Fleet, Discrete Wavelet Transformations: An Elementary Approach with Applications, first ed., Wiley, New Jersey, 2008.

Paria Jokar received her B.Sc. and M.Sc. degree with distinction in electrical engineering from the Iran University of Science and Technology. She is currently working toward Ph.D. in the Department of Electrical and Computer Engineering, University of British Columbia, Canada. Her Research interests include computer networks, wireless networks and network security.

Nasim Arianpoo received her B.Sc. in Electrical and Computer Engineering form University of Tehran, Iran, and her M.Sc. in Electrical and Computer Engineering from University of British Columbia, Canada, with focus on wireless communications. She is currently working toward Ph.D. in the Department of Electrical and Computer Engineering, University of British Columbia, Canada. Her Research interests include computer networks, wireless networks and network coding.

Victor C.M. Leung (S'75–M'89–SM'97–F'03) received the B.A.Sc. (Hons.) degree in electrical engineering from the University of British Columbia (U.B.C.) in 1977, and was awarded the APEBC Gold Medal as the head of the graduating class in the Faculty of Applied Science. He attended graduate school at U.B.C. on a Natural Sciences and Engineering Research Council Postgraduate Scholarship and completed the Ph.D. degree in electrical engineering in 1981.