Faisal et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:128
https://doi.org/10.1186/s13638-018-1143-0

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Identity attack detection system for 802.11-based ad hoc networks

Mohammad Faisal[1*], Sohail Abbas[2] and Haseeb Ur Rahman[1]

Abstract

Due to the lack of centralized identity management and the broadcast nature of wireless ad hoc networks, identity attacks are always tempting. The attackers can create multiple illegitimate (arbitrary or spoofed) identities on their physical devices for various malicious reasons, such as to launch Denial of Service attacks and to evade detection and accountability. In one scenario, the attacker creates more than one identity on a single physical device, which is called a Sybil attack. In the other one, the attacker creates cloned/replicated nodes. We refer collectively to these attacks as identity attacks. Using these malicious techniques, the attacker would perform activities in the network for which the attacker may not be authorized. In the existing literature, these attacks are often counteracted separately. However, in this paper, we propose a solution to counteract both attacks jointly. Our proposed scheme uses the received signal strength for the detection without using extra hardware (such as GPS, antennae or air monitors) and centralized entities (such as trusted third party or certification authority). Upon the detection of malicious identities, they will be quarantined and will be blacklisted for future data communication by the mobile nodes. Our proposed attack detector detects the presence of Sybil attacks and replication attacks locally by analysing the received signal strength captured by each node. Moreover, we propose a technique that will identify these attacks in the overall network. In both local and global cases, we evaluate our solutions theoretically and via simulation in NS-2. The obtained results demonstrate that it is possible to detect identity attacks with considerable accuracy without causing extra overhead in the form of extra hardware, periodic beacons or expensive localization operations in the wireless ad hoc networks.

Keywords: Impersonation, Sybil attack, Replication attack, Intrusion detection, Mobile ad hoc networks

1 Introduction

The IEEE 802.11-based wireless ad hoc architecture represents networks that consist of mobile nodes that randomly construct ad hoc topologies in a self-organized manner. The mobile nodes may be laptops, tablets, or smartphones irrespective of the operating systems that they use, such as Windows, Linux/Unix, Apple, Android, Blackberry, Symbian and iOS. These networks facilitate users in infrastructure-less environments where intentional or unintentional catastrophic violent situations may occur, such as earthquakes, floods, battlegrounds and search and rescue operations. In such situations, infrastructure-based networks are difficult to be installed because of their ad hoc or ephemeral nature [1–3].

Traditionally, the networks were formed using homogenous nodes (computers). However, due to the emergence of 5G and the Internet of Things (IoT) paradigms, heterogeneous networks comprising heterogeneous nodes such as sensors, phones, computers and satellites form, thereby providing various ubiquitous services. These wireless ad hoc networks are fully applicable in the field of the IoT. In the IoT, virtual objects, services, processes and devices are considered as nodes that are interconnected through the Internet. Soon, the IoT will amalgamate different technologies wirelessly in which ad hoc networks will play an integral part. Examples of such systems are smart cities, the Internet of connected vehicles (intelligent transportation system), etc. [4, 5].

Similar to all other networks, communications in 802.11-based ad hoc networks are commonly conducted based on a unique identifier that represents a network entity called a node. These identifiers are used for inter-nodal

* Correspondence: mfaisal@uom.edu.pk; mfaisal_1981@yahoo.com
[1]Department of Computer Science and IT, University of Malakand, Chakdara, KPK, Pakistan
Full list of author information is available at the end of the article

communications. This forms a one-to-one relationship between an entity (i.e. a node) and an identity used by a single user. This implication is commonly followed by many protocols directly or indirectly [6]. The ad hoc networks require each node to have a unique and distinct identifier to ensure the correct operations of the networked system and secure transactions. However, this one-to-one relationship may not be followed, thus resulting in serious security threats. There are two major types of identity attacks that violate this one-to-one entity-identity philosophy, the Sybil attack and the replication attack, which are discussed below.

Sybil attack: In this attack, one-to-one becomes one-to-many, which means that the attacker creates and manages more than one identity on a single physical device [7]. These newly forged identities will all be used simultaneously or in sequential order. That is, they may be used one-after-the-other, but only one identity will be up and running at a time. In the former case, the attacker uses the identity group to launch different types of attacks where the number of identities plays an important role, in some ways, to counteract a working system, such as Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks or altering the outcome of voting-based protocol(s). In the latter case, the identities may be used to escape accountability and/or traceability, such as evading a detection system where after the detection of one identity another forged identity emerges [8], thereby whitewashing all the malicious actions committed. The Sybil attacker may either adopt arbitrary identifiers for his Sybil, virtual identities or spoof the already existing nodes' identities. In the latter case, the attacker can gather the identity information of network nodes by snooping or sniffing in which an attacker sniffs the identity of privileged nodes and adopts them for malicious activities. Sybil attacks are detrimental to the correct network functioning and can disrupt the entire functionality of such systems in multiple ways. For example, a Sybil attacker can disrupt the routing of packets by giving a false impression of being distinct nodes on different locations or disjointed nodal paths. In trust or reputation-based schemes, a Sybil node can deteriorate the system by increasing or decreasing the reputation or trust by exploiting its virtual identities. In wireless sensor networks and smart grids, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based protocols, a Sybil attacker can manipulate the resulting outcome by rigging the polling process using Sybil identities. In vehicular ad hoc networks (VANETs), Sybil attackers can forge virtual non-existent vehicles and communicate false information in the network for malicious intents, such as to give false impressions of traffic congestion to divert traffic. Similarly, in a distributed system environment, a Sybil attacker can access and gain more resources using its forged identities [9–12].

Replication: In this attack, a many-to-one (entity-to-identity, i.e. multiple nodes have the same identity) strategy is used. In it, an attacker captures a node (most probably a sensor node in a wireless sensor network) and creates multiple clones of that physical node. Then, the malicious node or authority deploys these cloned or replicated nodes at various important locations in the network for malicious purposes, such as data analysis or launching a DoS or DDoS attack in the network. Moreover, these replicated nodes at various locations may hardly be detected by an intrusion detection system in place. The distinction between cloned identities and original ones is considered a challenging task [2, 13–17]. It is worth mentioning here that the Sybil attack with spoofed identities and replication attacks are logically identical because in both cases multiple nodes exist with the same identifier.

There are mainly three techniques used in the literature for Sybil and replication attack detection and/or protection, which are described below.

Trusted certification: The traditional approaches to detect or prevent these attacks use cryptographic-based authentication or trusted certification [16]. However, these approaches do not suit the infrastructure-less domain of the IoT since these schemes are costly in terms of their initial setup and the overhead incurred for maintaining and distributing cryptographic keys [8, 18, 19]. Moreover, they are also not scalable.

Resource testing: Some of the schemes have been proposed to counteract Sybil attacks based on the physical resource testing, such as radio, storage and computational resource testing [8, 17]. The goal of these schemes is to check (by employing some tests) whether an identity possesses resources greater than the resources normally possessed by a single node. These schemes are not effective due to the unrealistic bounds imposed on the attackers.

Position verification: Some authors, such as [10, 18], proposed position verification-based techniques to counteract Sybil attackers. These schemes work based on the assumption that each identity is bound by a single distinct location at any particular time. These approaches use the received signal strength indicator (RSSI) for position verification and hence are more promising than the others because of their lightweight and distributed nature [11, 20, 21]. However, since

RSSI varies with time, they rely mostly on extra hardware, such as directional antennae or GPS (Global Positioning System) or periodic beacon messages [11, 20, 21].

In this paper, we propose a received signal strength (RSS)-based scheme for identity-based attacks' counteraction. Since the RSS is a rough indicator of distance, we use the distance parameter to detect identity attacks in two ways: in a single radio range and, locally and globally, in the network. Each node will use the proposed algorithm in a distributed manner using the distance parameter to detect malicious identities in its own radio range. In addition to that, each node will also cooperate and collaborate with its neighbours to detect these attacks using our proposed global map algorithm. As soon as a malevolent identity is detected, it will be quarantined and will be blacklisted for future communication that are either detected in same radio range or different radio ranges within the network. It is worth mentioning that our scheme neither takes the services of any other third party nor does it use any sort of extra hardware, such as directional antennae or GPS. Furthermore, our proposed scheme is lightweight since it does not create any extra overhead on the overall architecture of the network.

We articulate our model through statistical and analytical analyses. Through these analyses, we are able to prove our detection rationale. Our detection works in two phases. First, attackers are detected locally (i.e. in a single radio range) and then globally (i.e. in the network). In the local detection, we use statistical analysis to generalize our scheme, create empirical cumulative distributive functions of three different radio ranges and compare the RSSI fluctuation in each range by employing a greater than 90% confidence interval for improved accuracy. In the global detection, we analytically analyse a criterion by which replicated nodes can be detected. Finally, to evaluate our proposed scheme, we use the NS-2 simulator where we plug in the thresholds that were analysed empirically into the simulated scenarios. The obtained results indicate a greater than 90% detection accuracy with less than 10% false positives.

The remainder of the paper is organized as follows. In Section 2, we discuss the literature review in our proposed classification manner. In Section 3, we discuss the feasibility of the identity attacks and the detection of such attacks in two scenarios, which are the detection in a single radio range and the detection across the network. We also develop a theoretical threshold for the detection using statistical significance testing. Section 4 is about the simulation-based evaluation of our proposed scheme using the NS-2 simulator and the result analysis. In Section 5, we discuss the main pros and cons of our proposed work. The paper is concluded in Section 6 in which we also highlight future work.

2 Literature review

We classify and briefly discuss the traditional countermeasures proposed in the literature for the detection or prevention of identity attacks in the following subsections.

2.1 Trusted third party or certification authority

In these schemes, a centralized or semi-centralized trusted third party (TTP) is used to create, maintain and revoke the identity certificate for each node. However, the certification authority (CA) suffering from an expensive initial installation setup is deficient in its scalability and is vulnerable to single point intentional (attack) and unintentional (failure) shutdowns [1, 22, 23].

In securing the wireless ad hoc networks, Hoeper and Gong [24] listed the various schemes based on the TTP or CA. In all these schemes, the centralized architecture is responsible for countering identity attacks in 802.11-based ad hoc networks. In practical security for disconnected nodes, Hoeper and Gong [24] proposed a concrete cryptosystem for ad hoc networks by focusing on hierarchical identity-based cryptography (HIBC). The authors introduced the concept of anonymity in the HIBC because of its roaming capability in different regions since the scheme is distributed in different hierarchies and can cover multiple regions.

Xing and Cheng [14] proposed two node replication schemes based on the time reference and space tradeoff called the Time Domain Detection (TDD) and the Space Domain Detection (SDD), respectively. The schemes generate a cryptographic one-way hash function with high accuracy and resilience to collusion, which is stored with a TTP for validation. However, the schemes did not tackle the problem of the overhead incurred, which affects the resource constraint nodes of mobile ad hoc networks (MANETs). In addition, the authors focused on node replication only.

Hoeper and Gong [24] proposed bootstrapping security in MANETs using identity-based schemes with key revocation. The authors combined the identity-based authentication and the key exchange (IDAKE) mechanism in one scheme, thereby using the symmetric key cryptography for reduced computational overhead. The TTP initialized all the nodes of MANETs with unique identities for communications. The proposed scheme relied heavily on the TTP.

Chen et al. [25] proposed a cluster-based certificate revocation with proof capability for MANETs. In this scheme, the authors focus on the revocation to isolate the problem of reuse by the intruders, which increases the accuracy threshold that is imposed on the mobile nodes for certificate activation. However, the scheme

assumed that all nodes already have certificates before joining the network and the nodes must be uniformly distributed among the radio range of the ad hoc network, which is not practicable.

In preventing impersonation attacks in MANETs with multi-factor authentication, Glynos et al. [26] proposed a framework via a cryptographic association to secure the physical device with the logical address. The framework achieved this target by using the certification of keys and nodes with the use of additional hardware and firmware installed on each node of the ad hoc network.

2.2 Software-based approaches

These schemes work as standalone solutions that use cryptographic-based authentication that imposes greater computation and communication overhead, which is usually caused by key distribution, maintenance and revocation operations. Hence, these issues make these approaches unsuitable for infrastructure-less environments, such as 802.11-based ad hoc networks, due to the resource constraint devices and distributed nature of the network [22, 25, 26].

Bouassida and Shawky [27] proposed anonymous multipath routing protocol based on secret sharing in mobile ad hoc networks. The protocol delivered the location, identity, data and traffic anonymity using cryptography. The protocol was also capable of countering interceptions and tampering attacks. However, the protocol assumed that every legal node in the ad hoc network must possess the same session and symmetric key, which could be easily impersonated by the intruders.

Hall et al. [28] proposed a novel secure identity-based cryptographic-based scheme for the hybrid wireless mesh protocol for IEEE 802.11s. The authors, in their proposed scheme, used a software-based approach to counter identity attacks. The scheme focused on securing the route discovery mechanism in which the route request and route reply control messages are communicated during the routing. The authors concentrated on securing the data exchange in both the route request and route reply mechanisms. However, the scheme increased the overhead, which does not suit IEEE 802.11-based ad hoc networks.

Bouassida and Shawky [27] proposed a fuzzy logic system that predicted the behaviours of nodes, such as how much a node in question can be trusted, while considering the partial history of the nodes' actions. The logic delivered the shortest possible route to ensure security against identity attacks and to identify the intruders. However, the scheme assumed that the nodes can predict the neighbouring node behaviours and broadcasting packets are reached to all nodes appropriately, which is a challenge in MANETs due to the presence of intruders.

2.3 Transceiver fingerprinting

In this category of schemes, the main logic of attack detection assumes that each radio transceiver generates a distinct radio frequency signal that reflects some physical characteristics that make it distinguishable from other transceivers, which is called its frequency fingerprint. These frequency fingerprints are used to counter identity attacks. However, the schemes may not be able to detect the attack if multiple devices are installed close to each other, thus creating the same fingerprints. Hence, DoS attacks can be launched easily. Moreover, this transceiver requires higher costs in terms of fingerprinting measurements and extra hardware implementation with enough precision, which restricts its use [27, 28]. Some of the schemes that use frequency fingerprinting are given below.

He and Wang [29] proposed a robust biometrics-based authentication scheme for the multi-server environment using transceiver fingerprinting. In the traditional system, for user authentication, authorization passwords were used. However, passwords may be stolen, shared or lost, and thus, here, the authors introduced the fingerprinting concept using elliptic curve cryptography in a multi-server environment. It is difficult to lose or forget copies or share, distribute, forge, guess or break a biometric generated key. However, in addition to the costs incurred for equipping each node with a biometric device, the computational costs of the scheme were also non-affordable for the 802.11-based ad hoc networks.

Faria and Cheriton [2] proposed the signal print-based solution to detect identity-based attacks in wireless networks. The author identified the transmitting devices by their distinct signal prints, which were also correlated with their physical location. By keeping the signal print information of all participating nodes, the network can identify the signal print of each node, which can help categorize the packets used for identity attacks. The authors assumed that the intruder would use an omnidirectional antenna equipped with standardized transmitters. However, the scheme may not be able to detect the intruders' signal prints if the devices were installed close to each other with below standard specifications, thus generating odd single prints.

Debdutta and Rituparna [30] proposed a three-pronged method based upon the transceiver fingerprinting. The scheme measured (normalization phase), attuned (database for patterns) and approximated (via data mining techniques) the RSSI values irrespective of the hardware devices to counter the effects of doors and walls on RSSI. The scheme used artificial neural networks to make clusters of the mobile nodes. Since the scheme used artificial neural networks, it is expensive for the low energy networks of MANETs.

Debdutta and Rituparna [30] proposed a scheme for detecting masquerading attacks in 802.11-based wireless networks. The authors identified the intruders by assigning unique fingerprints to each host of the wireless ad hoc network. The fingerprints were calculated by the Bayesian classifier from the networking activities of the wireless host. The scheme was precise and accurate in detection and was the pioneer in the category of transceiver fingerprinting. The scheme did not require any specialized extra hardware or any change in the existing hardware architecture; it may even be able to be implemented in the firmware of the already installed hardware. However, the scheme did not propose the solution of the new architecture hardware's fingerprints and address the limitations and computational overhead of the Bayesian classifier.

2.4 Received signal strength

The received signal strength (RSS) is used to localize nodes and hence is used to detect identity attacks since these schemes assume that each location must be bound by a unique and distinct identity. Messages emanating from the same location bearing two or more than two identities will be detected as Sybil attacks. Similarly, messages received from different locations with the same identities will be classed as replication attacks. The RSS is also hard to be forged. Existing RSS-based countermeasures use diverse antennas and Global Positioning System (GPS) technology. Some authors [31, 32] use air monitors (AM) as an additional hardware device that sniffs the traffic passively to detect spoofing attacks on the MAC layer. However, this approach creates additional hardware overhead for the infrastructure-less 802.11 [27]-based ad hoc networks [31–33].

Bouassida and Shawky [27] proposed an intrusion detection technique based on the degree of distinguishability analysis. In this technique, the nodes can verify each other's location and can authenticate the incoming nodes to the network based on the physical characteristics of the signals. However, the scheme was designed for static scenarios only. That is, the authors assumed that the verifier node's location and distance were fixed.

Yang et al. [22] proposed a detection mechanism for spoofing attacks in mobile environments. It used RSSI values when the attacker node was in motion. In this scheme, the authors developed a DEMOTE (DEtecting MObile spoofing aTtacks in wireless Environments) system. The scheme can predict the best RSS alignment over the radio range spread in the 802.11-based ad hoc networks without any supervision.

Dhamodharan and Vayanaperumal [34] proposed a Sybil attack detection technique in wireless sensor networks by using the message authentication and passing method. The message is passed to the new nodes joined to the sensor network to check its trustworthiness. If the message is verified and is not found to be a duplicate communication, the base station will allow it to start communications. Otherwise, it will be declared as a Sybil identity. The proposed work differs from ours in that it relies on the centralized entity, which is the base station in sensor networks without using mobility.

Zdonik et al. [35] proposed a scheme to detect Sybil attacks using the spatial variance of the physical layer in the WSN. The scheme focused on accurate detection without creating any extra overhead. The scheme used the iterative least squares (ILS) channel estimation method to determine the channel identification (CI). The detection idea is very interesting. However, the proposed scheme differs from ours in that the scheme strongly relied on a "powerful" base station in the WSNs, which may not work in 802.11-based ad hoc networks.

Qabulio et al. [36] proposed a scheme to counter the clone node attack in the WSN, irrespective of the node's location. The scheme does not use extra processing time and memory to calculate the distances between the nodes similar to its predecessor schemes, which is why it is a lightweight solution. Again, this paper implements its solution in wireless sensor networks while we implement our work in 802.11-based ad hoc networks that were mentioned in the topic of the paper. Qabulio et al. [37] also surveyed and analysed approximately 25 schemes that detect replication attacks in WSNs.

3 The proposed detection methodology

In wireless networks, the RSS is considered as a rough estimator of the distance between any two nodes. RSS-based schemes are usually based on a simple radio model where the received power approximately decays with the mth power of the distance. That is,

$$P_{\mathrm{r}} \propto \frac{P_{\mathrm{t}}}{d^m}$$

where P_{r} is the received power at the receiver, P_{t} is the transmission power at the transmitter node (which is considered constant at each transmitter) and d is the distance between the transmitter and the receiver. The value of m is called the path loss exponent, and its value depends on the environment being used. For outdoor line-of-sight (LoS) conditions, its value is 2, and for indoor environments, its value is 4. For a known transmitted power, the receiver node can compute the distance between itself and the transmitter, and by using simple geometric triangulation, the receiver can locate the transmitter.

In this section, we will use the RSS to detect Sybil attacks and replication attacks. Due to the lack of centralized identity management and administration in ad hoc networks where nodes have no information about

their remote neighbours at the *n*th hop, in the following subsection, we will devise local and non-local detection strategies. In the former, each node will detect the attackers in its local radio range, whereas in the latter, nodes will construct partial global maps of neighbours for the detection by collecting topological information.

3.1 Local detection

In identity attacks, multiple nodes can illegitimately acquire the same identity. In 802.11-based ad hoc networks, mobile nodes frequently find new neighbours by periodically broadcasting beacon packets in which these nodes ascertain their identities. Due to the non-predictable nature of these ad hoc networks, a malevolent node can claim the same identities without being detected. Our goal is to detect the identity attacks by ensuring that each physical node is bound with only one legal identity.

In the local detection approach, each node must store the RSS that is captured along with its capture time in a table from all the neighbouring nodes. Furthermore, each node monitors and records the RSS that is received from every 1-hop neighbour, as shown in Fig. 1. For any two successive RSS messages that originated from the same identity, the receiver will need to determine whether the messages that are received are from the same legitimate node or from two distinct nodes with the same identity. However, there are some intricacies involved here, which make the task of detection slightly more complicated. For example, in Fig. 1, node *A* receives messages *f1* and *f2* at times *t1* and *t2*, respectively, from same identity *m*. Now, node *A* needs to determine whether the messages received are from the same node moved from location *l1* to *l2* with the induced change in distance from *d1* to *d2* or from two distinct nodes. In this case, one is legitimate and the other would be the attacker node.

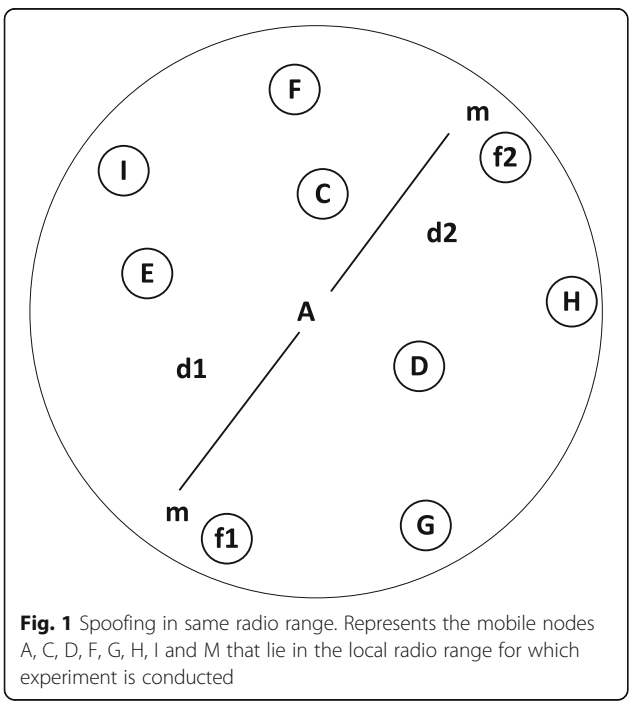

Fig. 1 Spoofing in same radio range. Represents the mobile nodes A, C, D, F, G, H, I and M that lie in the local radio range for which experiment is conducted

Before we answer the above question, it is important to build some terminology. Let $R_i^j(t_k)$ be the RSS value of node i received at node j at time t_k. Similarly, the change in RSS from successive messages from the same sender at the receiver will be

$$\Delta R = R_i^j(t_k) - R_i^j(t_{k-1})$$

We put an upper bound on the speed V that nodes can have by assuming that the maximum speed a node can have in the network is $V_{\max}$ ms^{-1}. In addition, $R_{\max}$ is the change induced in the RSS when a node's covering distance is $d_{\max}$, which is the distance covered by a node moving from any arbitrary location *l1* to any *l2* with $V_{\max}$ in Δt time. Hence, a node can never induce more change in the RSS than that of the R_{max} at the receiver since no node can cover more than $d_{\max}$ distance in Δt time.

In the above example, for the detection of spoofing attacks and replication attacks where attackers take on duplicate identities, node A will test the following condition.

$$\Delta R = R_A^m(t_k) - R_A^m(t_{k-1})$$

$$\text{Detection} = \begin{cases} \frac{\Delta R}{\Delta t} > R_{\max} & \text{Attack} \\ \frac{\Delta R}{\Delta t} \leq R_{\max} & \text{Normal} \end{cases}$$

3.1.1 Attack formulation

Due to its reusability feature, the RSS is an attractive choice for us to adopt it for attack detection. In addition, it is almost appropriate to meet the accuracy constraints of many applications. For that reason, we develop an attack detector using the RSS properties for identity-based attack detections [38, 39].

Here, we formulate the detection of an identity attack as a statistical significance testing problem in which the null hypothesis is

H_0 normal (no attack).

In this kind of testing, we will consider a test statistic T and will keep it under observation to establish whether the data under consideration belong to the hypothesis or not.

For a specific significance level α (defined as the probability of rejecting the hypothesis if it is true), there is a

corresponding *acceptance region* Ω such that we declare the null hypothesis to be valid if an observed value of the test statistic $T_{obs} \in \Omega$ and reject the null hypothesis if T_{obs} Ω. In other words, we declare that an attack is present if $T_{obs} \in \Omega_c$, where Ω_c is the *critical region* of the test.

Here, in our identity attack detection problem, we use the distance in the signal space and make the decision in comparison with the calculated threshold. Then, the acceptance region Ω and the detection rate are based on the specified *T*. If the attack is present, then our proposed null hypothesis will be rejected.

3.1.2 Statistical analysis of the RSS

Given that the RSS is usually affected by noise, environmental factors and multipath fading, we measure the RSS with a reference node and determine the distance to that reference node. Here, we consider three different scenarios: scenario I, scenario II and scenario III. In scenario I, the reference node is separated from the receiving node by 1, 6 and 11 ft. In scenario II, the reference node is separated from the receiving node by 20, 25 and 30 ft. In scenario III, the reference node is separated from the receiving node by 50, 55 and 60 ft. Thus, the RSS readings show a strong statistical correlation. We will assume that the reference node has the same transmission power.

According to the propagation model, the RSS at a receiving node from the reference node is given by [18].

$$P(d_i)[\text{dBm}] = \text{P}_\text{i}(d_0)[\text{dBm}] - 10\gamma \log\left(\frac{d_i}{d_i}\right) \quad (1)$$

where *i* is the *i*th receiving wireless node, $P_i(d_0)$ represents the transmission power of the reference node *i* at the reference distance d_0, d_i is the distance between the receiving wireless node and the reference node and γ is the path loss exponent whose value for free space communications is 2 and is greater than 4 for indoor communications [25, 40, 41].

Hence, the RSS distance between two nodes (reference node and receiving node) in signal space is given by

$$\Delta P = 10\gamma \ \log\left(\frac{d_i}{d_0}\right) \quad (2)$$

Here, we show the empirical cumulative distribution function (CDF) of the RSS distance between the reference and the receiving nodes in the signal spaces of scenario I, scenario II and scenario III, which are shown by Figs. 2, 3 and 4 respectively.

In all the abovementioned three scenarios, we find that the observed changes in variance and standard deviation increase with the increase in the distance. A minimum change in the skewness (a measure of the asymmetry of the probability distribution of a real-valued random variable about its mean) is also observed when the nodes are near each other.

It is important to analyse how well we can derive a threshold under which the distance in the signal space can effectively be exploited to perform attack detection. We refer to Eq. (2), where the two wireless nodes are at two different positions, such as the reference and the receiving node, with their respective means (μ_0 and μ_i) and standard deviations (δ_0 and δ_i).

The probability density functions (*pdf*s) of the distance under these two different conditions can be represented as follows

$$f_{\Delta P}\ (p \mid \text{Reference point}) = \frac{1}{\sqrt{\pi\delta}} e^{\frac{-(x-\mu_0)^2}{\delta^2}} \quad (3)$$

$$f_{\Delta P}\ (p \mid \text{consideration point}) = \frac{1}{\sqrt{\pi\delta}} e^{\frac{-(x-\mu_i)^2}{\delta^2}} \quad (4)$$

$$\text{DR} = \text{Prob}\ (\Delta P > t \mid \text{Reference point}) = 1 - \phi\ (t - \mu_0)/\delta_0 \quad (5)$$

$$\text{FPR} = \text{Prob}\ (\Delta P > t \mid \text{consideration point}) = 1 - \phi\ (t - \mu_i)/\delta_0, \quad (6)$$

where *t* is the detection threshold.

If we calculate the detection rate taken from the real test bed data, calculate it based on the detection rate by using Eq. (5) and then plot the result with the normal expected data without any attack; the following graph can be constructed.

We take the detection threshold $t = d_{\max}$, which is the maximum distance that can be covered by the mobile node, where *t* can be given as

$$t = \frac{\mu_0 + \mu_1}{2}$$

$$t = \frac{0 + 10\alpha \log\left(\frac{d_i}{d_0}\right)}{2}$$

$$t = 5\alpha \log\left(\frac{d_i}{d_0}\right)$$

To tune our detection accuracy by increasing true positives and reducing false positives using a 95% confidence interval, we add two standard deviations to our calculated threshold *t*, which can be seen in Figs. 5 and 6.

3.1.3 Threshold tuning

To theoretically obtain approximate estimates for the nodes moving with the certain speeds of 1, 2, 3 and 4 m/s in the signal space, we obtain the following:

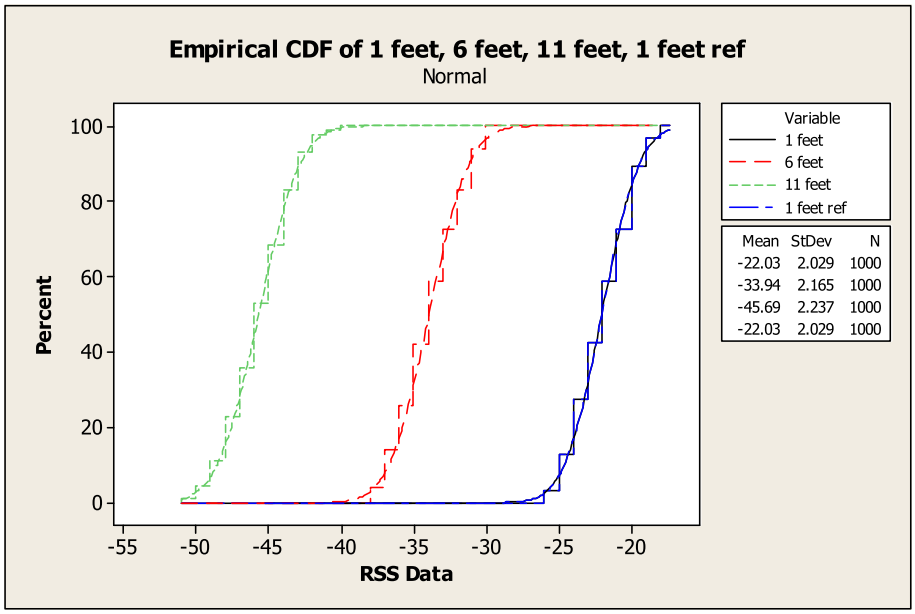

Fig. 2 Empirical CDF of scenario I. Calculates the empirical cumulative distribution functions for 1, 5 and 11 ft. The *x*-axis represents the RSS data while the *y*-axis represents the percentage value of each graph. It also shows the mean and standard deviation values of the three instances taken in scenario I

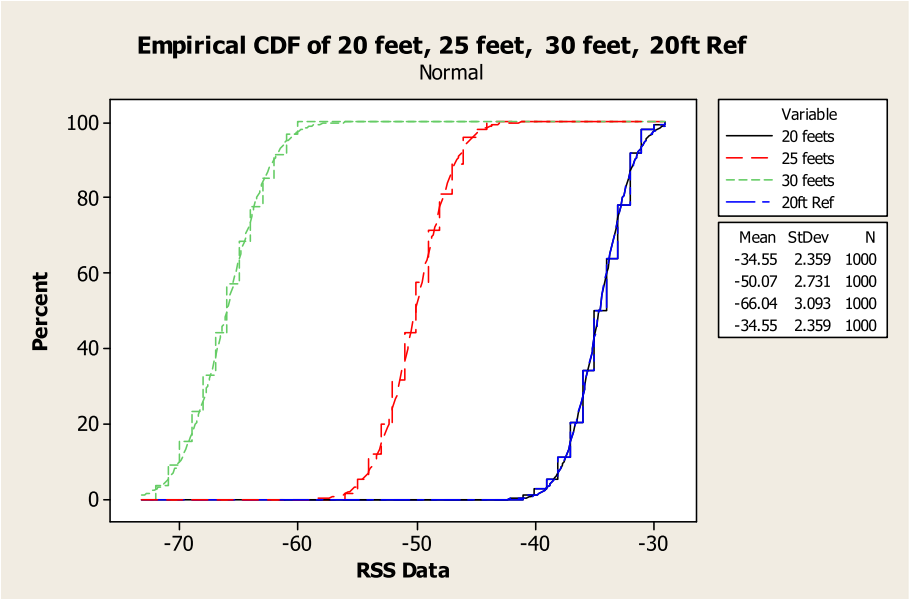

Fig. 3 Empirical CDF of scenario II. Calculates the empirical cumulative distribution function for 20, 25, and 30 ft. The *x*-axis represents the RSS data, while the *y*-axis represents the percentage value of each graph. It also shows the mean and standard deviation values of the three instances taken in the scenario II

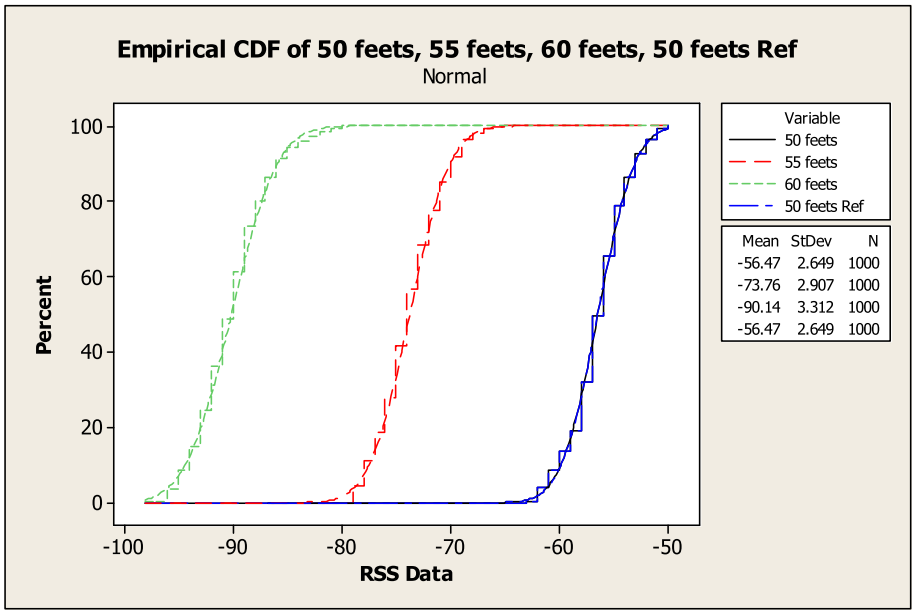

Fig. 4 Empirical CDF of scenario III. Calculates the empirical cumulative distribution function for 50, 55 and 60 ft. The *x*-axis represents the RSS data, while the *y*-axis represents the percentage value of each graph. It also shows the mean and standard deviation values of the three instances taken in the scenario III

For 1 m/s

$$\Delta P = \mid P0 - P1m \mid$$
$$= \mid -18 - (-31) \mid = 13\ dbm$$

For 2 m/s

$$\Delta P = \mid P0 - P2m \mid$$
$$= \mid -18 - (-38.6) \mid = 20\ dbm$$

For 3 m/s

$$\Delta P = \mid P0 - P3m \mid$$
$$= \mid -18 - (-43) \mid = 25\ dbm$$

For 4 m/s

$$\Delta P = \mid P0 - P3m \mid$$
$$= \mid -18 - (-46) \mid = 28\ dbm$$

Hence, it can be deduced that each RSS must not induce a change greater than 13 dbm for 1 m/s, 20 dbm for 2 m/s, 25 dbm for 3 m/s and 28 dbm for 4 m/s. This is also depicted in Fig. 7.

3.2 Non-local detection

Here, in this scenario, we consider multiple radio ranges named as radio range I, II, III, IV and V. In each region, a reference node is considered and shown as an underlined alphabet, as shown in Fig. 8. Please note that these reference nodes are not different than the other nodes and they are just for the explanation. We assume that each node constructs its 1-hop neighbours using the captured RSS directly or via overhearing. This 1-hop list will be shared periodically in order to enable the nodes to construct partial or complete network topology maps, as shown in Table 1. Table 1 shows the maps of the reference nodes only. We will use these maps to detect the replicated identities in the network.

In this section, we will try to solve a problem: how do we distinguish a replicated node from a legitimate node? The replicated identity may either be a distinct malicious node or it may be a spoofed identity created and adopted by a Sybil attacker. For example, in Fig. 8, node *m* shows its presence in three reference nodes' lists of *A*, *D* and *J*, as shown in Table 1. Our aim here is to detect the replicated nodes or identities in the network.

Please note that if the Sybil attacker spawned an identity that does not previously exist in the network, it can be detected by our local detection scheme discussed in Section 3.

3.2.1 System model

To develop the criteria for the replicated identity detection, we will introduce some terminology first, which may be given as follows.

Let N nodes be uniformly distributed in an area A. Let $n(p)$ be the immediate or 1-hop neighbours of node p, which are in p's radio range and share a bidirectional link with p. Two nodes, p and q, can communicate directly with each other if they are 1-hop neighbours of

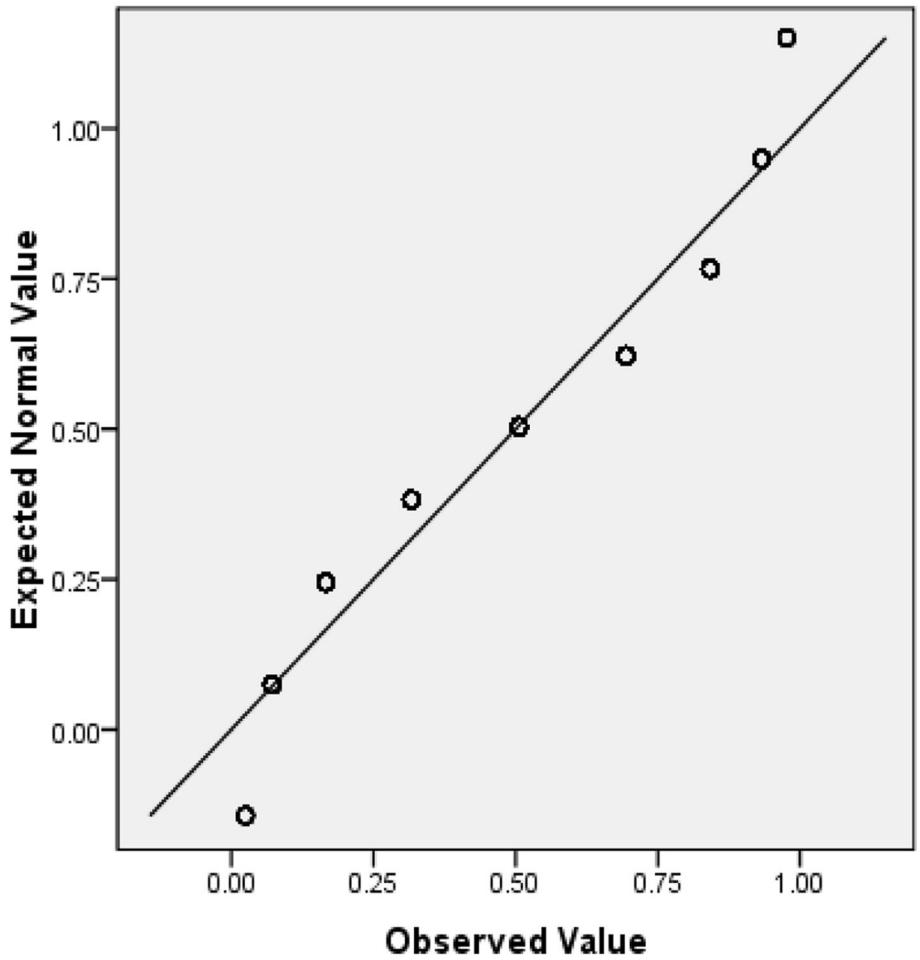

Fig. 5 Accuracy plot. Represents the accuracy plot that compares the expected data with the observed data

each other. That is, if $p \in n(q)$, then $q \in n(p)$. Let $n_2(p)$ denote the 2-hop neighbours of p that are the set of nodes that are neighbours of at least one node of $n(p)$. However, they do not belong to $n(p)$, and $n_2(p) = \{t | \exists z \in n(p) | t \in n(z) \backslash \{p\} \cup \{n(p)\}\}$. For a node $q \in n(p)$, let $\Delta_{\mathrm{p}}^{+}(\mathrm{q})$ be the number of nodes belonging to $n_2(p)$ that also belong to $n(q)$ such that $\Delta_{\mathrm{p}}^{+}(\mathrm{q}) = \mid n_2(p) \cap n(\mathrm{q}) \mid$. In other words, these are the number of nodes in $n_2(p)$ that node p can reach via node q. Similarly, for a node $q \in n_2(p)$, let $\Delta_{\mathrm{p}}^{-}(\mathrm{q})$ represent the $n(p)$ nodes that also belong to $n(q)$ such that $\Delta_{\mathrm{p}}^{-}(\mathrm{q}) = \mid n(p) \cap n(\mathrm{q}) \mid$. In other words, this quantity denotes the number of overlapping nodes in $n(p)$ that acts as bridge nodes and connects p and q in 2-hops.

PROPOSITION: *Let $\mathcal{G}(V, E)$ be an undirected graph with $V = \{v_1, v_2, v_3, \ldots\ldots v_n\}$ vertices connected together using $E = \{e_1, e_2, e_3, \ldots\ldots e_m\}$ edges. Let $\mathcal{G}$ be k-connected, where $k \geq 2$.Let node m be a node under observation. Let $m \in n(p)$ and $m \in n(q)$. Then, for a normal situation, there must exist a bridge node b that connects p to q. Otherwise, m will be deemed as a spoofed identity.*

PROOF: $\mathcal{G}$ is k-connected, and node m happens to be $m \in n(p)$ and $m \in n(q)$. Since $k \geq 2$, then there must be at least one other node x (other than m) such that $x \in \Delta_{\mathrm{p}}^{-}(\mathrm{q})$, which also implies that $q \in \Delta_{\mathrm{p}}^{+}(x)$. However, if $k = 1$, then m will be the only node that will belong to the set $\Delta_{\mathrm{p}}^{-}(\mathrm{q})$.

The average number of 1-hop, 2-hop, Δ^{-} and Δ^{+} nodes of a perspective arbitrary node in the network remain to be shown. We use the unit disk graph in order to model the network, such as that modeled by [42]. Since we are interested in the above mean values only, it is sufficient for us to capture the

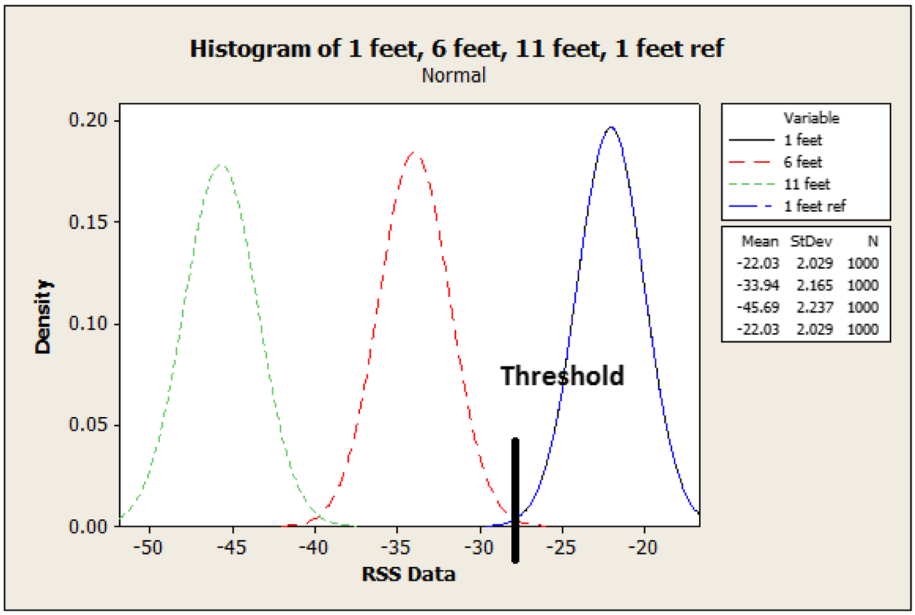

Fig. 6 Threshold with confidence interval graph. Represents the histogram values of 1, 6 and 11 ft. The *x*-axis shows the density value of the data, while the *y*-axis shows the RSS data. The figure also displays the mean and standard deviation of the three separate instances taken into consideration. The confidence interval with the threshold value has also been calculated statistically

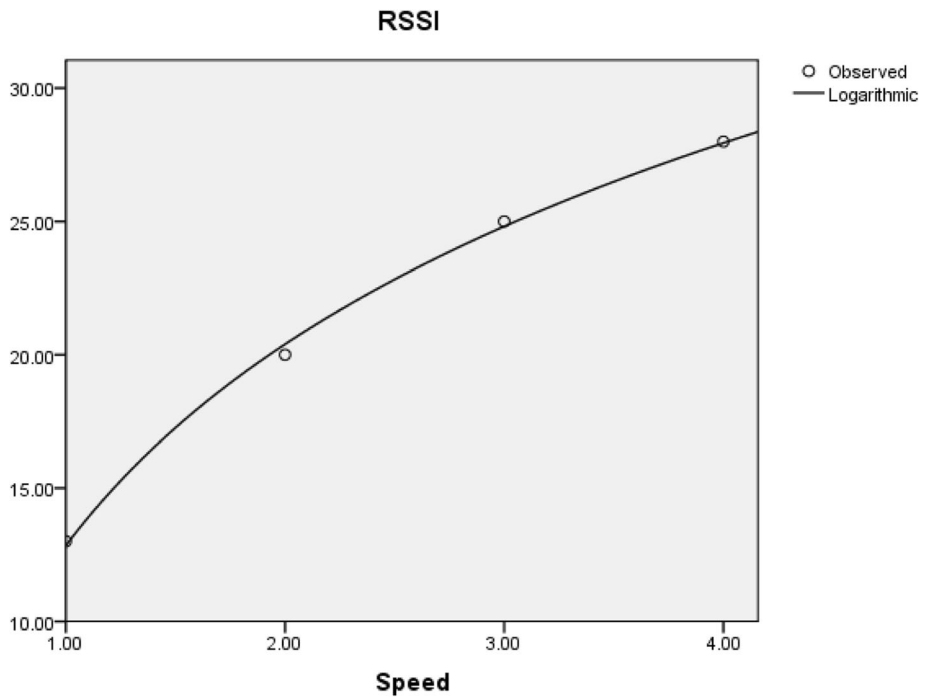

Fig. 7 Change induced in speed versus RSSI comparison. Shows the change induced in the RSS with the increase/decrease in the speed of the mobile nodes. The *x*-axis represents the speed of the mobile nodes in metres per second, while the *y*-axis represents the density of the RSS data

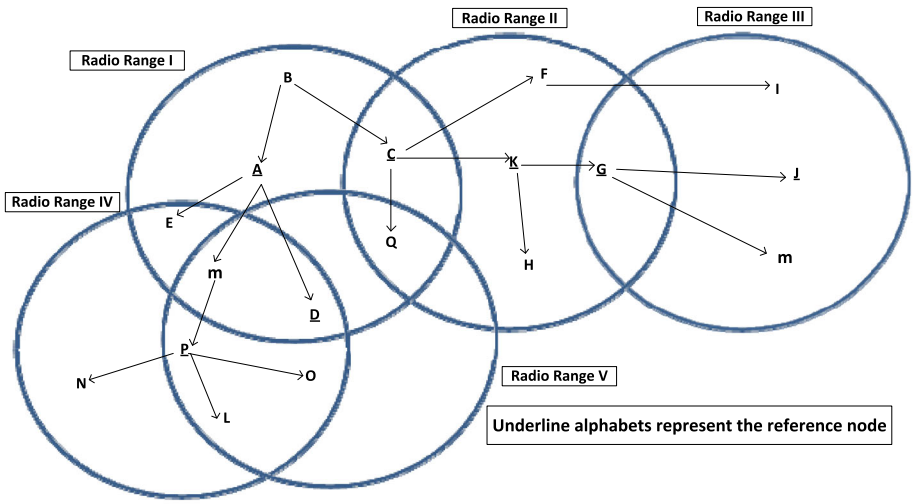

Fig. 8 Connected graph of spoofing in different radio ranges. Shows the radio ranges of the global detection. The participating mobile nodes are A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P and Q, which are divided in the five different radio ranges of I, II, III, IV and V. The underlined letters represent the reference nodes

portion of the network rather than modelling the complete network.

Let $\mathcal{D}(p,R)$ represent a disk with radius R to imitate the radio range R of node p. Let p lie at the origin of the disk. Then, by using the Poisson Point Process, the average number of points (nodes) of the process by the surface unit on $\mathcal{D}(0,R)$ is λ, which is called the intensity of the process, where $\lambda > 0$. The same is true for 2-hop nodes where $\mathcal{D}(0,2R)$. It is worth mentioning that the points are uniformly and independently distributed in each disk. In other words, the points in $\mathcal{D}(0,R)$ are independent of the points distributed in $\mathcal{D}(0,2R)$. As discussed above, we assume bidirectional links between each pair of nodes. These links would exist if and only if $d(p,q) \le R$,where $d(p,q)$ is called the Euclidean distance between the pair p and q. As shown in Fig 9a, $A(r)$ is the area of the intersection of two disks with radii of R that have r as the distance between their centres, which can be computed as follows:

$$A(r) = 2R^2 \arccos\left(\frac{r}{2R}\right) - r\sqrt{\left(R^2 - r^2/4\right)} \tag{7}$$

Table 1 The 1-hop list

A	K	J	P	D
B	C	G	E	Q
C	F	I	D	M
D	G	M	M	P
E	H		N	L
M	Q		L	O
Q			O	

Let p be a point that is uniformly distributed in $\mathcal{D}(0,R)$. Then, the average number of points in $\mathcal{D}(0,R)$ is given as

$$\mathbb{E}[n(p)] = \lambda \pi R^2 \tag{8}$$

To calculate the average number of process points belonging to n_2 (2-hop neighbours) that are accessible to p nodes via q, which is denoted by $\Delta_p^+(q)$, we assume that p and q are the process points uniformly distributed in $\mathcal{D}(0,R)$ and $\mathcal{D}(0,2R)$, respectively (consult Fig. 9a). The quantity $\Delta_p^+(q)$ is basically the q number of nodes that do not belong to $n(p)$ and reside on the $\pi R^2 - A(r)$ surface. By definition of the Poisson Point Process, on average, we have $\lambda \pi R^2$ nodes lying on a surface, and by proportionality, we have $\frac{\lambda}{\pi R^2}\left(\pi R^2 - A(r)\right)$ nodes in $\mathcal{D}(0,2R) \backslash \mathcal{D}(0,R)$. Therefore, by integrating all such points, we obtain the average number of nodes lying in $\mathcal{D}(0,2R) \backslash \mathcal{D}(0,R)$ as

$$\begin{aligned} \mathbb{E}\left[\Delta_p^+(q)\right] &= \frac{\lambda}{\pi R^2} \int_0^{2\pi} \int_0^R \left(\pi R^2 - A(r)\right) r dr d\theta \\ &= \lambda R^2 \frac{3\sqrt{3}}{4} \end{aligned} \tag{9}$$

To compute the average number of Δ^- nodes, assuming Fig. 9b, let p and q be the process points that are uniformly distributed in $\mathcal{D}(0,R)$ and $\mathcal{D}(0,2R)$, respectively. Please note here that some of the q nodes will belong to $\mathcal{D}(0,2R) \backslash \mathcal{D}(0,R)$ without being 2-hop neighbours of p since there must be a node on $\mathcal{D}(0,R)$'s surface to connect p to q. We assume that $A(r)$ is an overlapping area where common neighbours exist for

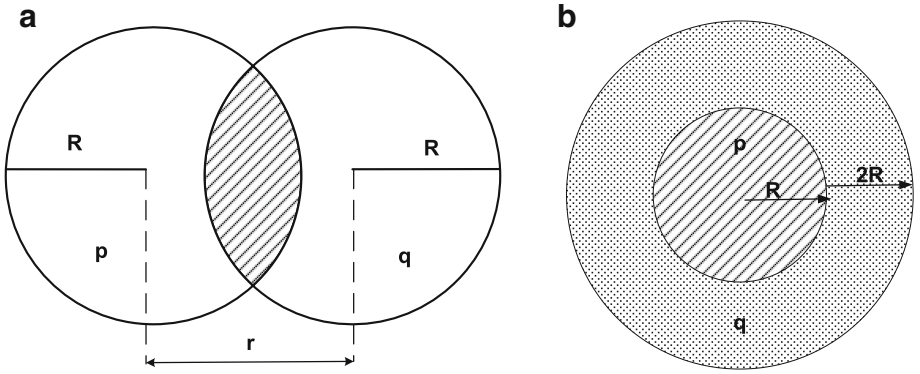

Fig. 9 Analysis of 1-hop and 2-hop neighbours. **a** Intersecting area of overlap between two disks and **b** two disks imitating 1-hop and 2-hop nodes

every r between R and $2R$. There are $\frac{2r}{3R^2}$ nodes at distance r. By integrating these points between R and $2R$, we get

$$\mathbb{E}\left[\Delta_p^-(q)\right] = \lambda \frac{2}{3R^2} \int_R^{2R} A(r) r dr = \lambda R^2 \frac{\sqrt{3}}{4} \tag{10}$$

To calculate the average number of 2-hop neighbours, there must be at least one common neighbour that connects 1-hop to 2-hop nodes, such as

$$\mathbb{E}\left[\Delta_p^-(q) | \, q \in n_2\right] = \frac{\mathbb{E}\left[\Delta_p^-(q)\right]}{\mathrm{P}\left(\Delta_p^-(q) > 0\right)}.$$

The probability that a node in $\mathcal{D}(0, 2R) \backslash \mathcal{D}(0, R)$ has at least one common neighbour in $\mathcal{D}(0, R)$ that makes q a 2-hop neighbour of p is

$$P\left(\Delta_p^-(q) > 0\right) = 1 - \frac{2}{3R^2} \int_R^{2R} \exp\{-\lambda A(r)\} r dr.$$

Therefore, the average number of 2-hop nodes can be written as

$$\mathbb{E}[n_2(p)] = 3\lambda\pi R^2 \times \left(1 - \frac{2}{3R^2} \int_R^{2R} \exp\{-\lambda A(r)\} r dr\right) \tag{11}$$

4 Simulation-based evaluation

4.1 Simulation setup

After evaluating our scheme with the help of statistical testing and analytical modelling, we also evaluate our scheme with the help of the NS2 simulator. We use the simulation parameters listed in Table 2. Here, we conduct our experiment for density versus accuracy in two scenarios, the true positive rate (TPR) versus speed and the false positive rate (FPR) versus speed. In each scenario, we again took three instances with different numbers of nodes.

To evaluate our attack detector, we investigate the effect of the node density on the detection accuracy. In the accuracy, we consider TPR and FPR. Meanwhile, in node density, we take three instances of 20, 30 and 40 nodes in each case of TPR and FPR separately with respect to speed.

4.2 Results

In the first experiment, as shown in Fig. 10, it is observed that the detection accuracy (TPR) of our scheme increases with the increase in node density. In the first instance where the number of nodes is 20, the TPR is almost 93.73%. In the second instance where the number of nodes is 30, the TPR is almost 95.21%. In the last instance where the number of nodes is the maximum of all, the TPR is 99.01%.

In the second experiment, as shown in Fig. 11, again there is no significant effect of the number of nodes on the FPR of our scheme. In the first instance, we take 20 nodes, which produce a low FPR of almost 7.13%. In the second instance, we take 30 nodes, and the resulting FPR is almost 5.51%. In the third instance, we take 40 nodes, and the ensued FPR is almost 0.98%. Hence, we can conclude that high node densities improve our

Table 2 Simulation parameters

Parameter	Value
Used area	1000 m × 1000 m
Maximum speed	10 m/s
Pause time used	60 s
Radio range	250 m
Nodes used	50–60
Connection established	5–15
The MAC	802.11
The application	CBR
Simulation time	900 s
Mobility model	Random wave point model

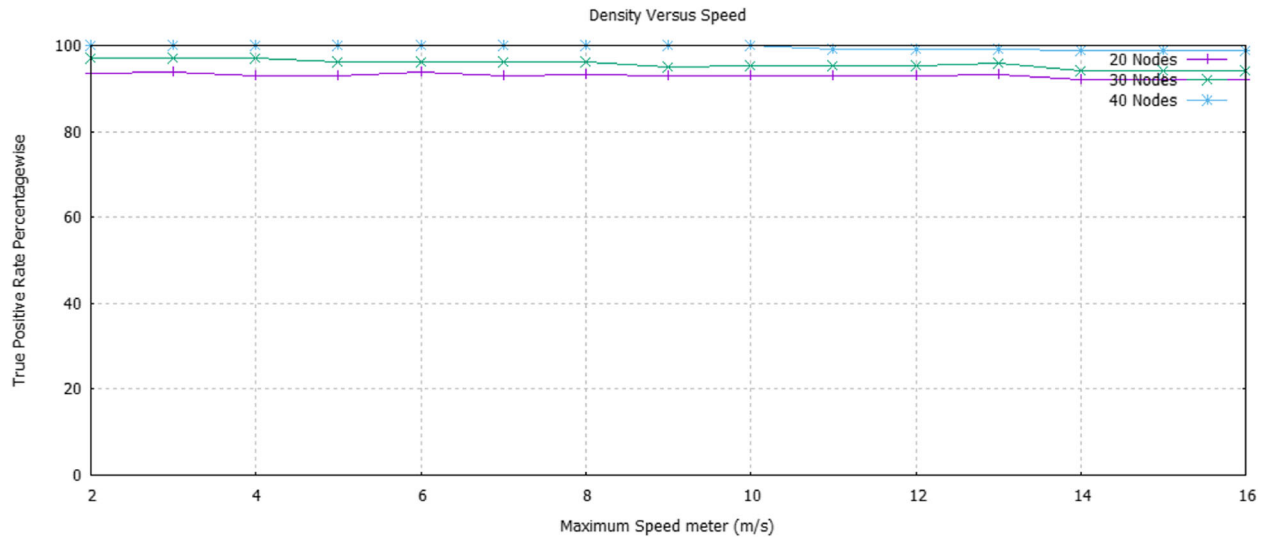

Fig. 10 Density versus speed true positive rate. Shows the simulation results of the density versus speed experiment. The *x*-axis represents the maximum speed per metre second, while the *y*-axis represents the TPR. The experiment was conducted in three different instances of 20, 30 and 40 mobile nodes

scheme's detection accuracy, such as high TPR and low FPR. This is since with high node density, the attackers fall into more radio ranges, which improves the detection accuracy.

5 Discussion

In the above sections, we discussed our proposed detection system and its design rationale. We analysed the RSS using statistical significance testing and theoretically calculated the PDR and FPR. Finally, we evaluated the scheme using the NS-2 simulator in order to analyse the overall detection accuracy of the system in different mobile environments. However, some important points of our proposed work remain to be discussed, which are given below.

First, one of the main issues in our proposed scheme that we discovered during the simulations is that although it performed well in dense environments, the detection accuracy decreased in sparse environments. One of the main reasons for this is that due to the mobility and

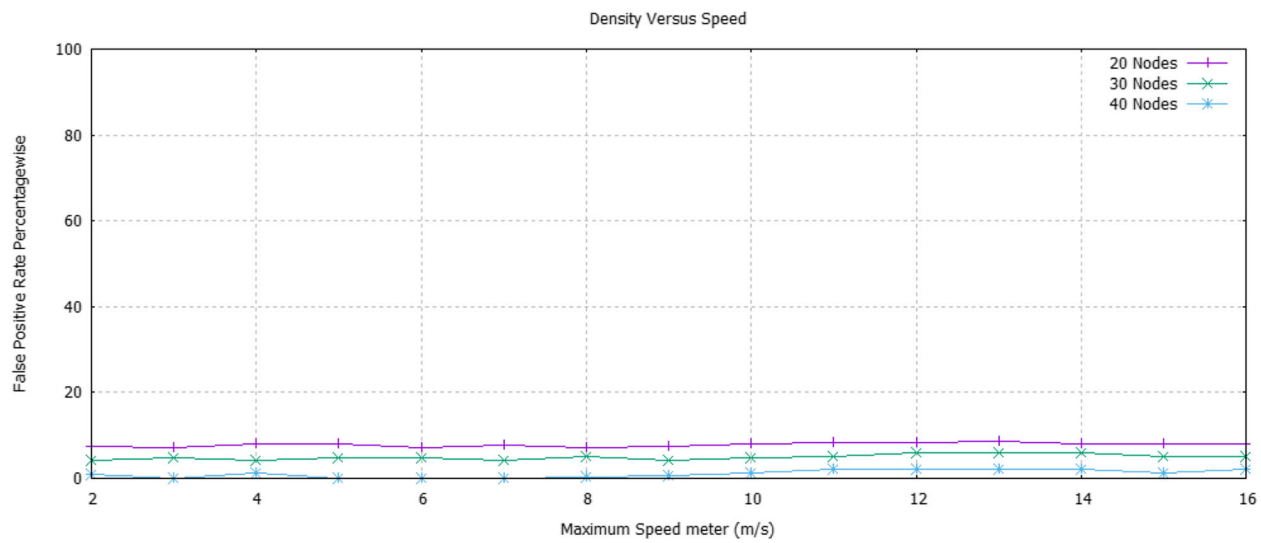

Fig. 11 Density versus speed false positive rate. Shows the simulation results of the density versus speed experiment. The *x*-axis represents the maximum speed per metre second, while the *y*-axis represents the FPR. The experiment was conducted in three different instances of 20, 30 and 40 mobile nodes

fluctuating RSS, some of the neighbouring nodes may not be able to detect the required change in the attackers' RSSs. This induced false negatives in some nodes. However, if the number of nodes was greater in the vicinity, the false negatives decreased.

Second, throughout our detection system, we established nodes to capture and store the RSS during the four-way handshake of the MAC 802.11 protocol. They were the RTS, CTS, DATA and ACK. This sometimes makes the RSS insufficient for the detection. For instance, an attacker node during its lifetime may move to a region in the network where it does not happen to be involved in the active routing path(s) (not forwarding any routing packets). Therefore, no RSS can be collected from this attacker and it will be undetected. This type of false negative can be mitigated by using periodic beacons in which each node broadcasts periodic control frames that are called beacons. Periodic beacons can also improve the topological construction in our non-local detection process. For example, each node will maintain a fresh map of its neighbours. However, periodic beacons are still a problem for a few reasons. First, they cause much overhead in the network. Second, attackers may not be forced to broadcast beacons in the prescribed manner. Third, attackers may broadcast spoofed and fabricated beacons, thus disrupting the overall network operations and deteriorating the detection process.

We assume a maximum speed for the network. By using it, we effectively distinguished between normal nodes and attackers. We believe that this assumption is valid and this will not make our scheme impractical for real environments. For instance, our scheme can still be used in vehicular ad hoc networks (VANETs) where vehicles cannot move faster than a limit. The limit might be the vehicle's maximum speed (from a speed metre) or it might be the permissible speed limit on a particular road or on a highway.

We have observed considerable fluctuations in the RSS, as discussed in Section 3. This fluctuation may produce a few metres of inaccuracy, which normally creates a weak degree of distinguishability of the closely lying nodes. However, our scheme can still be used in various application domains. For example, in VANETs where nodes are vehicles occupying few metres of space, they can easily be distinguished from other nearby vehicles in the signal space. Similarly, in the e-healthcare scenario where each patient's mobile phone can be considered in a single room, it can easily be distinguished from another patient's mobile phone in another room in the hospital.

6 Conclusions

In this paper, we proposed an RSS-based scheme to counter the identity attacks on IEEE 802.11-based ad hoc networks without using any additional hardware or a third-party guarantor. Unlike other schemes, our scheme did not incur any overhead in the form of periodic beacons and expansive localization computations. Similarly, we have validated our scheme theoretically and by using the NS-2 simulator. We have used our empirically collected data in our theoretical analysis. The result obtained from our analysis and the simulation showed that our proposed scheme produced good detection accuracy with negligible false positives.

Throughout our problem formulation, we have assumed homogenous transmission power in all nodes. In our future work, we will aim at improving our work for heterogeneous transmission powers at each node.

Abbreviations

CA: Certification authorityGPSGlobal Positioning System; DDoS: Distributed Denial of Service attack; DoS: Denial of Service attack; FPR: False positive rate; IEEE: Institute of Electrical and Electronics Engineering; IoT: Internet of Things; LoS: Line-of-sight; MANETs: Mobile ad hoc networks; NS-2: Network simulator; RSS: Received signal strength; RSSI: Received signal strength indicator; TPR: True positive rate; TTP: Trusted third party; VANETs: Vehicular ad hoc networks

Acknowledgements

The authors are grateful to Dr. Nathalie Mitton at INRIA labs France for the help with understanding some concepts related to analytical modelling. The authors also thank the anonymous reviewers for their valuable comments to improve this paper.

Authors' contributions

MF is the PhD scholar that performed all the work in this paper. HUR is the main research supervisor of MF who helped him in fine-tuning the proposed scheme. SA is the co-supervisor of MF who helped him in the modelling and simulation of the detection rationale. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Author details

[1]Department of Computer Science and IT, University of Malakand, Chakdara, KPK, Pakistan. [2]Department of Computer Science, College of Science, University of Sharjah, Sharjah, UAE.

Received: 30 June 2017 Accepted: 7 May 2018
Published online: 22 May 2018

References

1. S Abbas et al., Lightweight Sybil attack detection in MANETs. Systems Journal, IEEE **7**(2), 236–248 (2013)
2. DB Faria, DR Cheriton, in *Proceedings of the 5th ACM workshop on wireless security*. Detecting identity-based attacks in wireless networks using signalprints (ACM, 2006)
3. A Cheng, E Friedman, *Sybilproof reputation mechanisms, in Proceedings of the 2005 ACM SIGCOMM workshop on economics of peer-to-peer systems* (ACM, Philadelphia, 2005)
4. M Presser et al., The SENSEI project: integrating the physical world with the digital world of the network of the future. IEEE Commun. Mag. **47**(4), 1–4 (2009)
5. DG Reina et al., *The role of ad hoc networks in the internet of things: a case scenario for smart environments, in Internet of Things and Inter-Cooperative Computational Technologies for Collective Intelligence* (Springer, 2013), pp. 89–113
6. Dorri, A., S.R. Kamel, and E. Kheirkhah, Security challenges in mobile ad hoc networks: a survey. arXiv preprint arXiv:1503.03233, 2015.

7. MA Jan et al., A Sybil attack detection scheme for a forest wildfire monitoring application. Futur. Gener. Comput. Syst. **80**, 613-626 (2016)
8. X Feng et al., A method for defensing against multi-source Sybil attacks in VANET. Peer-to-Peer Netw Appl, 1–10 (2016)
9. SR Jan et al., *An innovative approach to investigate various software testing techniques and strategies*, International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Print ISSN (2016), pp. 2395–1990
10. AK Pal et al., A discriminatory rewarding mechanism for Sybil detection with applications to Tor. Electron. Mark. **208**, 12786 (2010)
11. B Yu, C-Z Xu, B Xiao, Detecting Sybil attacks in VANETs. J Parallel Distrib Comput **73**(6), 746–756 (2013)
12. S Raza, L Wallgren, T Voigt, SVELTE: real-time intrusion detection in the Internet of Things. Ad Hoc Netw. **11**(8), 2661–2674 (2013)
13. L Maccari, RL Cigno, A week in the life of three large wireless community networks. Ad Hoc Netw. **24**, 175–190 (2015)
14. K Xing, X Cheng, *From time domain to space domain: detecting replica attacks in mobile ad hoc networks, INFOCOM, 2010 Proceedings IEEE* (IEEE, 2010)
15. M Conti, S Giordano, Mobile ad hoc networking: milestones, challenges, and new research directions. IEEE Commun. Mag. **52**(1), 85–96 (2014)
16. R Di Pietro et al., Security in wireless ad-hoc networks: a survey. Comput. Commun. **51**, 1–20 (2013)
17. VM Agrawal, H Chauhan, An overview of security issues in mobile ad hoc networks. Int J Comput Eng Sci **1**(1), 9–17 (2015)
18. S Marti, H Garcia-Molina, Taxonomy of trust: categorizing P2P reputation systems. Comput. Netw. **50**(4), 472–484 (2006)
19. MN Mejri, J Ben-Othman, M Hamdi, Survey on VANET security challenges and possible cryptographic solutions. Vehicular Communications **1**(2), 53–66 (2014)
20. G Yan, S Olariu, MC Weigle, Providing VANET security through active position detection. Comput. Commun. **31**(12), 2883–2897 (2008)
21. Jan, M., et al., PAWN: a payload-based mutual authentication scheme for wireless sensor networks. Concurrency and Computation: Practice and Experience, 2016.
22. J Yang, Y Chen, W Trappe, *Detecting spoofing attacks in mobile wireless environments. In Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on* (IEEE, 2009)
23. NB Margolin, BN Levine, *Quantifying resistance to the Sybil attack, in Financial Cryptography and Data Security* (Springer, 2008), pp. 1–15
24. Hoeper, K. and G. Gong, Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation. Centre for Applied Cryptographic Research (CACR) at the University of Waterloo, Canada, Tech. Rep. CACR, 2006. 4: p. 2006.
25. Y Chen et al., Detecting and localizing identity-based attacks in wireless and sensor networks. IEEE Trans. Veh. Technol. **59**(5), 2418–2434 (2010)
26. D Glynos, P Kotzanikolaou, C Douligeris, in *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005. WIOPT 2005. Third International Symposium on*. Preventing impersonation attacks in MANET with multi-factor authentication (IEEE, 2005)
27. MS Bouassida, M Shawky, in *Communications and Information Technologies, 2007. ISCIT'07. International Symposium on*. Localization verification and distinguishability degree in wireless networks using received signal strength variations (IEEE, 2007)
28. J Hall, M Barbeau, E Kranakis, *Using transceiverprints for anomaly based intrusion detection*, Proceedings of 3rd IASTED, CIIT (2004), pp. 22–24
29. D He, D Wang, Robust biometrics-based authentication scheme for multiserver environment. IEEE Syst. J. **9**(3), 816–823 (2014)
30. BR Debdutta, C Rituparna, MADSN: mobile agent based detection of selfish node in MANET. International Journal of Wireless & Mobile Networks (IJWMN) **3**, No. 4 (2011)
31. B Parno, A Perrig, in *Workshop on Hot Topics in Networks (HotNets-IV)*. Challenges in securing vehicular networks (2005)
32. Hoeper, K. and G. Gong, Bootstrapping security in mobile ad hoc networks using identity-based schemes. Security in Distributed and Networking Systems, 2007.
33. Y Sheng et al., in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. Detecting 802.11 MAC layer spoofing using received signal strength (IEEE, 2008)
34. USRK Dhamodharan, R Vayanaperumal, Detecting and preventing Sybil attacks in wireless sensor networks using message authentication and passing method. Sci. World J. **2015**, 841267;7 (2015) https://doi.org/10.1155/2015/841267
35. Zdonik, S., et al., SpringerBriefs in computer science. 2012.
36. M Qabulio, YA Malkani, A Keerio, in *Information Assurance and Cyber Security (CIACS), 2015 Conference on*. Securing mobile wireless sensor networks (WSNs) against clone node attack (IEEE, 2015)
37. M Qabulio, YA Malkani, AA Keerio, On node replication attack in wireless sensor networks. Mehran Univ Res J Eng Technol **34**(4), 413–424 (2015)
38. P Bahl, VN Padmanabhan, in *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings.* RADAR: an in-building RF-based user location and tracking system (IEEE, 2000)
39. MA Youssef, A Agrawala, AU Shankar, in *Pervasive Computing and Communications, 2003.(PerCom 2003). Proceedings of the First IEEE International Conference on*. WLAN location determination via clustering and probability distributions (IEEE, 2003)
40. A Goldsmith, *Wireless communications* (Cambridge university press, 2005)
41. TK Sarkar et al., A survey of various propagation models for mobile communication. IEEE Antennas Propag Mag **45**(3), 51–82 (2003)
42. Busson, A., N. Mitton, and E. Fleury. An analysis of the MPR selection in OLSR and consequences. In Mediterranean Ad Hoc Networking Workshop (MedHocNet'05). 2005.