Detection of Malicious Nodes Using Collaborative Neighbour Monitoring in DSA Networks

Augustine Takyi[1,2(✉)], Natasha Zlobinsky[1], Odametey Akuye-Shika[2], David Johnson[1], and Melissa Densmore[1]

[1] Department of Computer Science, University of Cape Town, Rondebosch 7701, South Africa
{atakyi,mdensmore}@cs.uct.ac.za
[2] Department of Computer Science and Informatics, University of Energy and Natural Resources, Sunyani, Ghana

Abstract. This work addresses position falsification attacks of malicious nodes against spectrum users and devises a strategy to detect such nodes. We conducted over 6 months of measurements to confirm the practicability of using RSSI under varying weather conditions, which confirms that RSSI fluctuates along the mean. Also, the simulation results obtained show that collaborative neighbour monitoring in hybrid (centralized and distributed) networks work well in detecting position falsification attacks in dynamic spectrum access networks, provided that the distance between the actual malicious node position and the falsified position is at least 0.3 km.

Keywords: Spectrum sensing · Collaborative neighbour monitoring · Malicious node detection · DSA networks · Position falsification attack

1 Introduction

This paper advocates the idea of getting rid of malicious nodes that attempt to falsify their position to abuse the sharing principles of the dynamic spectrum access (DSA) networks, which may reduce throughput and increase latency. This subsequently affects the spectrum utilization. In view of this, the paper identifies some possible attack scenarios within a threat model and subsequently develops a detection algorithm to detect malicious nodes that may exploit the identified attack scenarios. Malicious nodes may falsify location information to mount attacks in the spectrum, causing harm to a primary transmitter or a neighbour secondary node. By falsifying its position the malicious node can easily adjust its parameters such as transmit power and antenna height to unduly cause unwarranted interference to prevent original nodes from transmitting. We study the above malicious node position falsification attacks in a network setup

H. Jin et al. (Eds.): CROWNCOM 2021/WiCON 2021, LNICST 427, pp. 215–230, 2022.
https://doi.org/10.1007/978-3-030-98002-3_16

of dynamic spectrum access-using network devices. Firstly, this is a challenging problem because of the coexistence of both the licensed and the unlicensed transmitters within the same space. Abusing spectrum etiquette of transmitting above approved power levels and antenna heights could have a serious effect on the genuine nodes. Secondly, the problem is challenging because of the shadowing and multipath fading effects in wireless transmissions. In mitigating shadowing and multipath fading effects we employ collaborative spectrum sensing, which improves the probability of detection in the highly shadowed environment [22].

The problem of position falsification in dynamic spectrum access networks has not yet been addressed in the literature. However, several works [1,6–8,12,21–23] have been proposed for detecting other forms of malicious attacks in DSA networks. Closest to our work is [22], which considers *malicious false reporting attacks* in a large cognitive radio network. Their study employed an approach of crowdsourcing of collaborative sensing to detect malicious users. However, the crowdsourcing of collaborative sensing approach cannot detect position falsification attacks, as the authors assume that there is no position falsification by the malicious node [22]. Hence, we develop an algorithm to resolve position falsification attacks, which is critical to consider is DSA-based networks.

In this work we develop an algorithm based on received signal strength indicator (RSSI) and fingerprinting of the node to detect any malicious node (a node that abuses the network rules) within the network. The algorithm is designed to operate in a back-haul of the network design architecture. The contribution of this paper is fourfold. First, we design a new system and threat model that fits in the DSA-based network. Second, we develop a threat model for the DSA-based network. Thirdly, we develop a detection strategy algorithm and also develop a naive detection algorithm based on common knowledge of statistics, using averages and dispersion of averages from similar data sets that operate at the layer one of the TCP/IP network layering architecture. The naive algorithm only depends on averages and standard deviation values. The results obtained from the naive algorithm as compared to the proposed algorithm are all false positives. We also show that computing weighted decision factors on the RSSI values of a neighbour node helps in making accurate decisions. The weighted decision factor introduces a new hypothesis: whether the node is malicious or not. Hence, the RSSI values obtained by using any of the free space models or the data propagation model or by measurement cannot be reliably depended on to make decisions in the proposed algorithm, unless the weighted decision factor of the RSSI values are obtained and computed and its hypothesis deduced to obtain the true status of the node as being malicious or not. Again, from the naive approach, averages and deviation values alone cannot be relied on to prove whether a node is malicious or not. Our algorithm depends solely on averages and dispersion of averages without the weighted decision factor to make decisions as to whether a node is malicious or not. Finally, we conduct simulations to investigate the effects of antenna height and distance on the propagation signal

in the spectrum and also validate the proposed detection algorithm through simulation. Simulation results show that the algorithm is able to detect all falsified nodes with the minimum distance between the falsified position and the genuine position of at least 350 m.

2 System Model

In our model, we position fixed secondary (or unlicensed) nodes and malicious nodes, connected by a Central Decision Center (CDC), which is the decision-making platform implemented in the master node that controls the network, as also used by Basavaraj, Mancuso, and Probasco [5]. The CDC shall be the decision centre of the algorithm. The positions of the secondary nodes and the malicious users are independently distributed in an $(L \times L)\text{km}^2$. We assume that all secondary and malicious nodes are embedded with spectrum analysers to capture the transmission signals from the neighbours within their transmission range. The obtained RSSI values and the node identification information are sent to the CDC. The i^{th} device has position coordinates $P_i = (x_i, y_i)$ where, $i = 1, 2, 3, ..., n$. All our secondary user nodes are transceiver nodes. Each of the secondary users has a transmission range of R within the area. Each secondary node transmits at a power of P_s and the malicious nodes at a power of P_m. The secondary and malicious users are located at a minimum distance of L km from the primary user (licensed user within the spectrum), to prevent interference. Any RSS value received by the CDC below a threshold of λ is not used by the CDC in the estimation of channel statistic parameters. Secondary and malicious nodes are sensed using energy detection [17].

There are N secondary nodes and M malicious nodes in the system. Each secondary node communicates to the CDC over a secure end-to-end connection, such as a TLS tunnel, between each participating secondary node and the CDC [17]. Since we are interested in using our secondary nodes as back-haul nodes for our network, we assume that the secondary nodes are static and do not change position.

We again assume that malicious nodes may not have prior knowledge of all the nodes within its transmission range. This enables anonymous reporting about malicious nodes to the CDC to avoid compromising secondary nodes. Again, all nodes transmitting at an energy level greater than the approved energy level are considered to be malicious. We assume that all nodes can hear and decode any modulation scheme, which will prevent nodes from hiding behind modulation schemes to cheat on the network. Finally, we assume that each node on the network has an in-built system that is able to decode its neighbours' received signals to obtain their identities.

3 Threat Model

In our model, we assume that the links between the CDC and the secondary nodes are wireless and provide IP connectivity. We also assume that an attacker

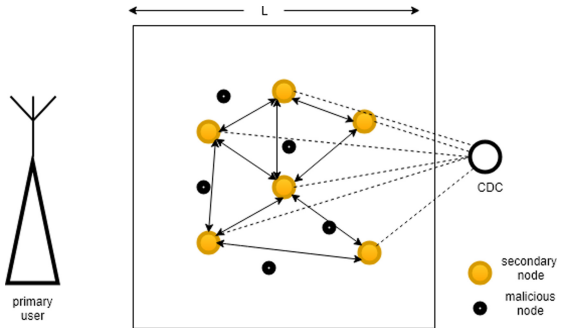

Fig. 1. Overall system model with six secondary nodes ($N = 6$) and five malicious nodes ($M = 5$).

has full access to the network medium between the CDC and secondary nodes and also between secondary neighbour nodes. We also assume that there is no mechanism to ensure confidentiality of the communication between the nodes. A malicious node on the network can cause an attack we refer to as a **position falsification attack (PFA)**. In a PFA the malicious node falsifies its location, resulting in physical and/or logical attacks. In a physical attack the PFA causes interference to neighbouring nodes on the network and in a logical attack the malicious user unduly takes channels that should be allocated to other nodes. An attacker exploiting PFA may pretend to be in the range of the network by adjusting its location information to conform to the propagation area of the network and request for a channel from the CDC just to deny genuine nodes from getting access to channels. Under such an attack the malicious node may increase its transmission power or antenna height above the agreed level in order to obtain a competitive advantage over the other secondary nodes. Any of the above can be exploited by the malicious node, thus negatively impacting on the performance of the network. Additionally, whenever any secondary node requests a channel from the CDC all the nodes within its transmission range hear the request. Again exploiting position falsification by a malicious node, the node can also create a Sybil attack [29] by creating several virtual nodes located in different locations as if those virtual nodes were part of the network.

All the attack scenarios considered in this threat model can highly affect the successful implementation of dynamic spectrum access based networks, especially opportunistic networks such as a TV White Space network deployment on a large scale. While the PFA as described in this work can occur in both fixed spectrum access (FSA) and dynamic spectrum access (DSA), it is a much more significant problem in DSA networks because of the scarcity of resources [14,15]. To detect these attacks, we propose to use collaborative neighbour monitoring.

4 Neighbour Monitoring in Cooperative Sensing

In neighbour monitoring, all nodes within transmission range of any transmitting secondary node in the network will hear it and measure its received signal strength (RSS). We do not rely on the individual nodes to report their RSSI values or distance from the CDC because malicious nodes can easily fake their RSSI values and their estimated range. Our proposed detection hypothesis is:

$$\begin{aligned} H_0 &: \text{ malicious node absent} \\ H_1 &: \text{ malicious node present} \end{aligned}$$

We consider the main detection strategy proposed in the algorithm to detect malicious nodes if present.

4.1 Detection Strategy and Weighted Decision Factor at the CDC

In identifying a malicious node, we use a mean (average) received power indicator for all the individual neighbour nodes within the transmission range of the transmitter node. The CDC shall keep all the initially computed means of the received power values in dBm in its database and subsequently compare all the RSSI means calculated to check for deviations from the initially computed means. In the CDC, each node shall have separate means of the received power values measured for each neighbour node. Let the mean of the RSSI measurements from the i^{th} neighbour of a given potential malicious node be represented by μ_i.

$$\mu_i = \frac{1}{S}\sum_{j=1}^{S} P_{ij} \quad \forall\ i, j \in \mathbb{N};\ i, j > 0 \tag{1}$$

where P_{ij} is the j^{th} power sample obtained from the i^{th} neighbour. Let σ_i represent the standard deviation of the power samples obtained from the i^{th} neighbour node; that is

$$\sigma_i = \frac{1}{S}\sum_{j=1}^{S}(P_{ij} - \mu_i)^2 \quad \forall\ i, j \in \mathbb{N};\ i, j > 0 \tag{2}$$

The hypothesis decisions shall be the following:

$$\begin{cases} \text{if } |\mu_i - \mu_{ic}| \leqslant k\sigma_i & H_0 : \text{ no suspected malicious node} \\ \text{if } |\mu_i - \mu_{ic}| > k\sigma_i & H_1 : \text{ suspected malicious node} \end{cases} \tag{3}$$

where μ_i is the initial mean of the received signal strength indicators and μ_c is the current mean of the received signal strength indicators and $k \in \mathbb{R}; k \leq 1$ is the threshold factor to account for interference and terrain conditions. To further compensate for the RSSI fluctuation we use weighted factors based on whether the node is potentially malicious and the initial advertised distance from the reporting neighbour node. In calculating the weighted factor, the estimated

distance is compared with the advertised distance. We assume that any node whose estimated average received power is greater than or equal to twice the average advertised power of the node, is a potential malicious node as shown in Eq. (4). We therefore define the weighted factor in Eq. (5) based on the criteria defined in Eq.(4). If the null hypothesis is rejected by the Eq. (4), a weighted factor of 1 is assigned to the neighbour node; else the weight is assigned based on Eq. (5).

$$criteria = \begin{cases} -2\mu_i \leq \mu_i \leq 2\mu_i & \text{where either } H_0 \text{ or } H_1 \text{ is accepted} \\ \mu_{ic} > 2\mu_i & \text{where } H_0 \text{ is rejected} \end{cases} \tag{4}$$

where μ_i is the initial mean of RSSI and μ_{ic} is the current mean of the RSSI.

$$w_i = |\frac{\hat{d}_i}{D_i} \ - \ 1|, \ \forall i = 1, 2, 3, ..., N \tag{5}$$

where w_i is the estimated weight obtained from the estimated distance and the advertised distance, $\hat{d}$ is the estimated distance from the neighbour node, D is the initial advertised distance of the node and τ (which appears in Eq. (8)) is the tolerance factor to compensate for the variations in the RSSI values. The τ is set based on the initial advertised distance received at the CDC.

Therefore, for each node, the CDC computes the collaborative weight, W, on a node based on the neighbours within the sensed region using Eq. (6)

$$W = \frac{1}{N} \sum_{i=1}^{N} w_i \tag{6}$$

where N is the total number of the applicable neighbour nodes. We consider a weighted decision factor threshold at the CDC to be 10% of the total weights of the individual nodes calculated by the CDC of the individual nodes. Let I be the indicator variable for the weighted factor hypothesis.

$$I = \begin{cases} 0 & \text{where } H_0 \text{ is accepted} \\ 1 & \text{where } H_0 \text{ is rejected} \end{cases} \tag{7}$$

Therefore the hypothesis will be

$$\begin{cases} |\frac{\hat{d}}{D} \ - \ 1| \geq \tau & H_1: \ \text{malicious node present} \\ |\frac{\hat{d}}{D} \ - \ 1| \ < \tau & H_0: \ \text{malicious node absent} \end{cases} \tag{8}$$

This means that the collaborative weight W calculated by Eq. (6) is always less than 0.90 when H_0 is to be rejected. Based on this strategy we propose the detection algorithm that is as depicted in Algorithm 2.

4.2 Malicious Node Localization

The malicious node can then be localized using trilateration [35]. However, implementation of this component of the algorithm is out of the scope of this work. Let the location error be represented by lr and the location error threshold be represented as $lr_{threshold}$. Then the localization decision is given by the following:

$$\begin{cases} lr \leqslant lr_{threshold} : & \text{position not falsified} \\ lr > lr_{threshold} : & \text{position falsified} \end{cases} \tag{9}$$

5 Naive Detection Approach

We compare the naive detection algorithm with our cooperative weighted decision detection algorithm that goes further to compute weighted values and considers environmental factors of the terrain conditions. As shown in Tables 1 and 2 using our cooperative weighted decision detection algorithm shows more effective as compared to the naive approach. The naive algorithm is obtained from the idea of statistics which indicates that same datasets obtained should have the same deviation. According to common knowledge in statistics, when a node does not change its position, it shall produce similar signal strength at any time interval, which is expected to be the same dataset. However, according to this work, a node may falsify its position or change some of its parameters such as the power and antenna height to achieve its goal, by providing different datasets of RSSI values to cheat the system. So ideally, if a node in a DSA network does not change its position or parameters, then there will not be significant changes or deviations from the mean values obtained at any given data point such as n (for all n greater than zero and less than infinity).

5.1 Naive Detection Hypothesis

$$\text{naive hypothesis} = \begin{cases} H_0 : |\mu_i - \mu_c| > \sigma_i : & \text{the node is malicious} \\ H_1 : |\mu_i - \mu_c| \leq \sigma_i : & \text{the node is not malicious} \end{cases} \tag{10}$$

where μ_i is the initial mean of the initial dataset;
μ_c is current mean of the current dataset;
σ_i standard deviation of the initial dataset;
Each dataset is obtained from at least 20 simulation runs.

$$\begin{aligned} If\ lr \leqslant lr_{threshold}\ \ then,\ position\ not\ falsified \\ If\ \ lr > lr_{threshold}\ \ then,\ position\ falsified \end{aligned} \tag{11}$$

5.2 Naive Detection Algorithm and Test Results

Table 1. Detection of malicious node M using naive algorithm by neighbour monitoring nodes

Node	μ_i	μ_c	μ_i-μ_c	σ_i	Hypothesis
A	–75.2889	inf		inf	accept H_0
B	–70.7047	–84.6650	–13.9603	7.2180	reject H_0
C	–52.7557	–73.3967	–20.6410	6.8531	reject H_0
D	–64.3251	–82.4262	–18.1011	7.1369	reject H_0

The simulation results as shown in the Tables 1 and 2 indicate that all the neighbouring nodes of node M shows that M is not a malicious node and accepted H_0 (null hypothesis), which confirms that node M as indicated in Fig. 2 is not a malicious node.

Algorithm 1. Naive Detection algorithm based averages

1: Set i, j := 0; Set $\{P_{ij}\}$:=$\emptyset$;
2: Set N; Set S;
3:
  for (i, j) **do**
    Set d_{ij}:= 0;
  end for
4:
  for i; i $\leq$ N; i++ **do**
    for j; j $\leq$ S; j++ **do**
      Read received power values p_{ij}
      if $p_{ij} < \lambda$ **then**
        discard value
      end if
    end for
    Send P_i to fusion center
    Compute μ_i
    Compute σ_i
  end for
5: verify the detection using (3)
  if $|\mu_i - \mu_{ic}| \leqslant k\sigma_i$ **then**
    No suspicious malicious node
  else if $|\mu_i - \mu_{ic}| > k\sigma_i$ **then**
    Malicious node suspected
  end if
7: Compute the location errors using (11)
  if $lr \leqslant lr_{threshold}$ **then**
    malicious node position not falsified
  else if $lr > lr_{threshold}$ **then**
    malicious node position falsified
  end if

Algorithm 2. Cooperative Weighted Decision Detection Algorithm (CWDDA)

1: Set i, j := 0; Set $\{P_{ij}\}$:=$\emptyset$;
2: Set N; Set S;
3:
for (i, j) **do**
Set d_{ij}:= 0;
end for
4:
for i; i $\leq$ N; i++ **do**
for j; j $\leq$ S; j++ **do**
Read received power values p_{ij}
if $p_{ij} < \lambda$ **then**
discard value
end if
end for
Send P_i to CDC
Compute μ_i
Compute σ_i
end for
5: verify the detection using (3)
if $|\mu_i - \mu_{ic}| \leqslant k\sigma_i$ **then**
No suspicious malicious node
else if $|\mu_i - \mu_{ic}| > k\sigma_i$ **then**
Malicious node suspected
end if
6: Compute weights according to (5)
if $|\frac{\hat{d}_i}{D_i} - 1| \geq \tau$ **then**
Malicious node present;
else if $|\frac{\hat{d}_i}{D_i} - 1| < \tau$ **then**
Malicious node absent;
end if
7: Compute the location errors using (11)
if $lr \leqslant lr_{threshold}$ **then**
malicious node position not falsified
else if $lr > lr_{threshold}$ **then**
malicious node position falsified
end if

Table 2. Detection of malicious node M using CWDDA by varying distances as indicated in Fig. 2

Node	μ_i	μ_c	μ_i-μ_c	σ_i	Hypothesis
A	0	–75.2889	0	6.9234	accept H_0
B	–84.6650	–70.7047	13.9603	6.7720	reject H_0
C	–73.3967	–52.7557	20.6410	6.1937	reject H_0
D	–82.4262	–64.3251	18.1011	6.5585	reject H_0

5.3 Comparison of Naive Algorithm to Cooperative Weighted Decision Detection Algorithm

In reference to Algorithm 1, the naive algorithm which is based on common statistical knowledge, i.e., it depends on the mean and standard deviation of similar datasets obtained from multiple simulation runs of RSSI values of neighbour nodes and determine how the current means deviate from the initial means obtained from similar datasets by comparing the means to its standard deviation and determine the hypothesis (the null (H_0) and alternative (H_1)). However, the cooperative weighted decision detection algorithm takes into consideration the expected differences in the RSSI values due to the environmental factors such as weather conditions and the intention of each node to cheat the system by introducing weighted factors and the threshold factors in the algorithm. The results of the two algorithms show that the naive approach in most times show that there is malicious node even when there is no malicious node and the vice versa. It can therefore be concluded that naive approach cannot be depended on in detecting malicious node, which may give false location information if computed. The cooperative weighted decision detection algorithm has three levels of hypothesis testing, whereas the naive approach has one hypothesis test, which is based on mean and standard deviation only. This indicates that the naive approach is not verified after the first hypothesis test, hence the result is not confirmed. Its output cannot be compared to the cooperative weighted decision detection algorithm, which verifies the first hypothesis twice before the algorithm completes.

6 Real World Measurements

As part of our work, we undertake real-world measurements on the University of Cape Town campus to verify the possibility of using received signal strength values to detect malicious nodes. In the measurement setup, we use two routers with 2.4 GHz WiFi, 5 GHz WiFi, and TVWS (television white space) network cards in each router as well as directional antennas for both the WiFi and the TVWS transmissions. We collected our data using a laptop on the 2.4 GHz WiFi band with the support of a measurement script we wrote. In the measurements, we considered the following variable parameters apply: channel number, channel width, transmission power and the distance between the two secondary nodes. The weather and terrain conditions were considered. The measurement results are shown in Table 3.

Table 3. Measurement of signal strength taken at a distance of about 200 m with one tree between the secondary nodes obstructing the signals

Ch no.	Ch width	TxPower	Min (RSSI)	Max (RSSI)	Mean (RSSI)	Std (RSSI)
1	20	20	–63	–54	–55.8	4.0249
1	20	15	–82	–58	–67	6.9585
1	10	20	–42	–28	–34.86	7.14
1	10	15	–28	–23	–25.83	1.309

Table 4. Experimental parameters

Parameter	Value
Secondary power	4 W to 10 W
Secondary height	10 m to 30 m
Frequency	470–694
Transmission range	1 km to 10 km
Antenna gains	5 dbi to 20 dbi

7 Experimental Set Up

We test this algorithm with by doing a simulation in Matlab. We adopt the Hata propagation model [4], which supports different terrain propagation. The values of the numerical parameters we consider for our simulation test are listed in Table 4. We consider Fig. 2 in the experimental setup when testing our detection algorithm above through simulation. In both Fig. 2 we positioned five nodes, of which node M was a malicious node that falsified its location. We run the simulation with different position coordinates and measure the effectiveness of our proposed algorithm.

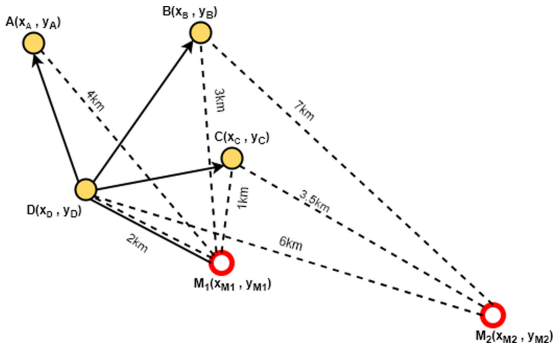

Fig. 2. Attacker may be positioned within the victim's network as M_1 but falsify its position as M_2 or the attacker may be positioned outside the victim's network as M_2 and falsify position as M_1 for verification by the CDC.

8 Results and Discussion

8.1 Simulation

In all the simulations, I fixed the k value at the threshold of 1. This is because I assumed there are no varying environmental effects that affected the propagation. The results obtained were much more interesting. In Table 3, I observed that when node A could not detect node M, it recorded the current mean as

Inf (infinity) and subsequently recorded node M as not malicious. Nodes B, C and D detected node M because the collaborative weights assigned to the three nodes were significant, node M was labelled by the CDC as a malicious node.

8.2 Models

This chapter designed a system model and a threat model which best fit in the scenario considered by this thesis. In the system model, the number of secondary and malicious nodes were independently distributed within a range in order not to create MAC layer issues. CDC was also considered as the part of the nodes that accepts and computes RSSI values and runs that detection algorithm. In the system model, it is assumed that all secondary and malicious nodes are embedded with spectrum analyzers to capture the transmission signals from the neighbour nodes and forward same to the CDC. In the system model, it is further assumed that the nodes are static and do not change positions. Again the model assumed that malicious nodes may not have prior knowledge of all the nodes within the transmission range. This enables anonymous reporting about malicious nodes to the CDC to avoid compromising secondary nodes. All nodes are embedded with equal moderation and de-moderation scheme which may prevent nodes from hiding behind different moderation scheme to cheat the system. The system model considered is a unique model applicable for DSA networks where channel availability is rare. The chapter further considers a threat model that assess the loopholes in the proposed system model for an attacker or malicious node may take advantage to cheat on the system. In the threat model the main attack that is considered to be easily exploited by a malicious node is Position Falsification Attack (PFA). We noted that there are several ways in which an attacker can pretend its position parameters such as varying it antenna height and changing its approve power transmission level, which are detailed explained in chapter 3 of the thesis. To prevent this attack from happening the chapter proceeded to develop an algorithm that seeks to detect malicious nodes that try to falsify their position.

8.3 Algorithm - CWDDA

The algorithm (CWDDA) is developed to check nodes either malicious or genuine secondary nodes that tries to alter its transmission power or antenna height to increase or decrease its transmission signal strength to cheat the system or faulty nodes that may transmit unevenly in the network. The algorithm computes averages of signal strength and employs other detection strategies such as weighted decision factor that computes weight on every RSSI value received by the CDC. In computing the weighted factor, every node have an advertised position so when RSSI value is received by the CDC, the CDC decoded to know the node that forwarded the RSSI value and by using an appropriate signal propagation model the distance is estimated from the RSSI value received. Reference Eq. (5) for computation of weighted decision factor. Our algorithm uses mean values but its different from naive approach that we considered above.

9 Naive Detection Approach

In order to better assess CWDDA, we have also simulated a naive detection approach for comparison.

The naive approach is based on common statistical knowledge, i.e., it depends on the mean and standard deviation of similar datasets obtained from multiple simulation runs of RSSI values of neighbour node and determines how the current means deviate from the initial mean obtained from similar dataset by comparing the means to its standard deviation and measure hypothesis (the null (H_0) and alternative(H_1)). However, the cooperative weighted decision detection algorithm takes into consideration the expected differences in the RSSI values due to the environmental factors such as weather conditions and the intention of each node to cheat the system. By introducing weighted decision and the threshold factors in the algorithm. The results of CWDDA compared to naive approach show that the naive approach in most times indicates that there is malicious node present (false positive) even when there is no malicious node and the vice versa. It can therefore be concluded that naive approach cannot be depended on in detecting malicious nodes, which may give false location information if computed. The cooperative weighted decision detection algorithm has three levels of hypothesis testing whereas the naive approach has one hypothesis test which is based on mean and standard deviation only which indicates that, the naive approach is not verified after the first hypothesis test hence the result is not confirmed. Its output cannot be compared to the cooperative weighted decision detection algorithm which verify the first hypothesis twice before the algorithm completes.

9.1 Limitation of the Algorithm

It is difficult to know the exact number of malicious nodes present at a time hence in distributing the number of secondary and malicious nodes it could be uniformly distributed. It is difficult to work on a simulation platform that do not support wireless sensing. According to the cooperative weighted decision detection algorithm in this chapter, each secondary node within the network area is expected to forward neighbour nodes RSSI to the CDC for computation of the threshold and decision of either malicious or not is determined by the CDC but not the individual nodes. The channel availability is scarce, therefore nodes within the network area cannot communicate at all times. The cooperative weighted decision detection algorithm is to detect the presence of malicious nodes in the DSA network; however, the algorithm is limited by the conditions under which it works. Conditions under which the algorithm works are

1. The presence of 3 nodes and above
2. When the environmental factors threshold is below 1.0
3. Availability of free white spaces

Conditions under which the algorithm may not work

1. When nodes are less than 3
2. When the environmental factors threshold is above 1.0
3. Unavailability of free white spaces

10 Conclusion

In conclusion, we have demonstrated that in spite of fluctuating RSSI values, it is still possible to use them to detect malicious nodes in our cooperative weighted decision detection algorithm. In our simulation, we observed that the algorithm was effective in detecting malicious nodes that falsified their positions. However, at the minimum distance of 300m the results received were mostly false positives. Also, we showed through simulation that between distances of 0.3–7 km, it is possible to reliably detect malicious nodes. The selection of k value greatly affects the performance of the algorithm, as large values resulted in false negatives. Nevertheless, more work needs to be done by optimizing the threshold and tolerance factors for highest accuracy. The simulation results demonstrated that, CWDDA works better than the Naive Detection Algorithm.

References

1. Matthee, K.W., et al.: Bringing Internet connectivity to rural Zambia using a collaborative approach. In: International Conference on Information and Communication Technologies and Development, 2007, ICTD 2007. IEEE (2007)
2. Chen, E.T.: The Internet of Things: opportunities, issues, and challenges. In: The Internet of Things in the Modern Business Environment, pp. 167–187. IGI Global, Hershey (2017)
3. Takyi, A., Densmore, M., Johnson, D.: Collaborative neighbour monitoring in TV white space network. In: Proceedings Southern Africa Telecommunication Networks and Applications Conference (SATNAC 2016), George, South Africa (2016)
4. Yuvraj, S.: Comparison of Okumura, Hata and COST-231 models on the basis of path loss and signal strength. Int. J. Comput. Appl. **59**(11), 37–41 (2012)
5. Patil, B., Anthony M., Scott P.: Protocol to Access White-Space (PAWS) Databases: Use Cases and Requirements (2013)
6. Anand, S., Jin, Z., Subbalakshmi. K.P.: An analytical model for primary user emulation attacks in cognitive radio networks. In: 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2008, DySPAN 2008. IEEE (2008)
7. Kamat, P., et al.: Enhancing source-location privacy in sensor network routing. In: Proceedings 25th IEEE International Conference on Distributed Computing Systems, 2005, ICDCS 2005. IEEE (2005)
8. Tapiador, J.E., Clark, J.A.: Masquerade mimicry attack detection: a randomised approach. Comput. Secur. 30(5), 297–310 (2011)
9. Richard Yu, F.: Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. In: MILCOM 2009 - 2009 IEEE Military Communications Conference, p. 2009. IEEE (2009)
10. van den Heuvel, M.P., et al.: High-cost, high-capacity backbone for global brain communication. Proc. Natl. Acad. Sci. **109**(28), 11372–11377 (2012):

11. Subramanian, L., et al.: Rethinking wireless for the developing world. In: IRVINE IS BURNING, p. 43 (2006)
12. Jonathan, P., et al.: Successful deployment and key applications of Television White Space Networks (TVWS) Malawi (2014)
13. Albert, A.L., Moshe, T.M., David, L.J.: The television white space opportunity in Southern Africa: from field measurements to quantifying white spaces, In: White Space Communication, pp. 75–116. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-08747-4
14. Kaligineedi, P., Majid, K., Vijay, K.B.: Secure cooperative sensing techniques for cognitive radio systems. In: IEEE International Conference on Communications, ICC 2008. IEEE (2008)
15. Zargar, S.T., et al.: Security in dynamic spectrum access systems: a survey. (2009)
16. Bhattacharjee, S., Shamik, S., Mainak, C.: Vulnerabilities in cognitive radio networks: a survey. Comput. Commun. **36**(13), 1387–1398 (2013)
17. Fatemieh, O., Ranveer C., Carl , A.G.: Secure collaborative sensing for crowd sourcing spectrum data in white space networks. In: 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum. IEEE (2010)
18. Zarrin, S., Teng J.L: Belief propagation on factor graphs for cooperative spectrum sensing in cognitive radio. In: 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2008, DySPAN 2008. IEEE (2008)
19. Jayaprakasam, A., Vinod S.: Sequential detection based cooperative spectrum sensing algorithms in cognitive radio. In: 2009 First UK-India International Workshop on Cognitive Wireless Systems (UKIWCWS). IEEE (2009)
20. Zhang, W., Ranjan K.M., Khaled B.L.: Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks. IEEE Trans. Wirel. Commun. **8**(12), 5761–5766 (2009)
21. Saad, W., et al.: Coalitional games for distributed collaborative spectrum sensing in cognitive radio networks. In: IEEE INFOCOM 2009. IEEE (2009)
22. Visotsky, E., Kuffner, S., Peterson, R.: On collaborative detection of TV transmissions in support of dynamic spectrum sharing. In: 2005 First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks 2005, DySPAN 2005. IEEE (2005)
23. Meng, J.J., et al.: Collaborative spectrum sensing from sparse observations in cognitive radio networks. IEEE J. Select. Areas Commun. **29**(2), 327–337 (2011)
24. Wang, W., et al.: Attack-proof collaborative spectrum sensing in cognitive radio networks. In: 43rd Annual Conference on Information Sciences and Systems 2009, CISS 2009. IEEE (2009)
25. Angelosante, D., Ezio, B., Marco, L.: Neighbor discovery in wireless networks: a multiuser-detection approach. Phy. Commun. **3**(1), 28–36 (2010)
26. Pejovic, V., et al.: VillageLink: a channel allocation technique for wide-area white space networks. In: White Space Communication, pp. 249–280. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-08747-4
27. Jin, Z., Anand, S., Subbalakshmi, K.P.: Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. ACM SIGMOBILE Mobile Comput. Commun. Rev. **13**(2), 74–85 (2009)
28. Augustine, T., et al.: Performance analysis of a collaborative DSA-based network with malicious nodes (2017)
29. Bouassida, M.S., et al.: Sybil nodes detection based on received signal strength variations within VANET. IJ Netw. Secur. **9**(1), 22–33 (2009)

30. Al-Khalid, O., Adams, A.E., Charalampos C.T.: Node discovery protocol and localization for distributed underwater acoustic networks. In: Advanced International Conference on Telecommunications, 2006/International Conference on Internet and Web Applications and Services, AICT-ICIW 2006. IEEE (2006)
31. Karthikeyan, V., Vinod, A., Jeyakumar, P.: An energy efficient neighbour node discovery method for wireless sensor networks. arXiv preprint arXiv:1402.3655 (2014)
32. Althunibat, S., et al.: On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio. IEEE Commun. Lett. **17**(8), 1564–1567 (2013)
33. Alahmadi, A., et al.: Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Trans. Inf. Forensics Secur. **9**(5), 772–781 (2014)
34. Kaemarungsi, K., Prashant, K.: Properties of indoor received signal strength for WLAN location fingerprinting. In: The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004, MOBIQUITOUS 2004. IEEE (2004)
35. Rida, M.E., et al.: Indoor location position based on bluetooth signal strength. In: 2015 2nd International Conference on Information Science and Control Engineering (ICISCE). IEEE (2015)