An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks

Murat Demirbas, Youngwhan Song
Department of Computer Science and Engineering Department
State University of New York at Buffalo
Buffalo, NY 14260-2000
Email: {demirbas, ywsong}@cse.buffalo.edu

***Abstract*— A sybil node impersonates other nodes by broadcasting messages with multiple node identifiers (ID). In contrast to existing solutions that are based on sharing encryption keys, we present a robust and lightweight solution for sybil attack problem based on received signal strength indicator (RSSI) readings of messages. Our solution is robust since it detects all sybil attack cases with 100% completeness and less than a few percent false positives. Our solution is lightweight in the sense that alongside the receiver we need the collaboration of one other node (i.e., only one message communication) for our protocol. We show through experiments that even though RSSI is time-varying and unreliable in general and radio transmission is non-isotropic, using ratio of RSSIs from multiple receivers it is feasible to overcome these problems. In this paper we report on experimental evaluation of our implementation.**

I. Introduction

The term *sybil attack* is introduced in [2] to denote an attack where the attacker (sybil node) tries to forge multiple identification in a certain region. Sybil attack is particularly easy to perform in wireless sensor networks (WSN) where the communication medium is broadcast, and same frequency is shared among all nodes. By broadcasting messages with multiple identifications, a sybil node can rig the vote on group-based decisions and also disrupt network middleware services severely.

Existing solutions for sybil attack prevention are too costly for the resource-poor sensor platforms, such as the popular Berkeley mote platform [6]. Motes have very limited computational resources (e.g., 8K RAM, 4Mhz CPU) and are energy constrained; thus, algorithms that impose an excessive communication burden on nodes are not acceptable since they drain the battery power quickly. Solutions [4], [10] that adopt key exchange to vouch identification severely effect the energy consumption due to distribution and piggybacking of randomly generated keys in messages. Moreover, they consume precious memory space as every node is required to store pairwise keys with neighbors.

A received signal strength indicator (RSSI) based solution for sybil attack is desirable as it does not burden the WSN with shared keys or require piggy backing of keys to messages. Ideally, upon receiving a message, the receiver will associate the RSSI of the message with the sender-id included in the message, and later when another message with same RSSI but with different sender-id is received, the receiver would complain of a sybil attack. However, due to the unreliable, time-varying nature of RSSI [8], [15], this scheme fails. Moreover, since it is very easy to change the transmission power [3] in WSN, a sybil node can send messages with different IDs using varying transmission power to trick the receiver. Since RSSI is a function of transmission power, different transmission powers will lead to different RSSI readings.

Contributions of this paper

In this paper, we report on our implementation of a robust and lightweight solution for detecting sybil attack in WSN using RSSI. Our solution is robust since it detects all sybil attack cases with 100% completeness and very good accuracy (less than a few percent false positives.) Our solution is lightweight in the sense that alongside the receiver we need the collaboration of one other node (i.e., only one message communication) for our protocol. To the best of our knowledge, this is the first implemented solution for sybil attack detection on the WSN platform.

We show through experiments that even though RSSI is unreliable and time-varying in general and radio transmission is non-isotropic [15], using ratio of RSSIs from multiple receivers it is possible to overcome these problems easily. Use of ratio of RSSIs from multiple receivers was introduced in [14], however, this is the first time that this technique is implemented in practice. We show through experiments that using one receiver there is a lot of variation on RSSI values, however using multiple receivers and ratio of RSSIs the time-variance of RSSI is overcome and the standard deviation is very small. We give confidence intervals for this variance from our experiments at varying distances.

To achieve a lightweight solution, we first point out that we do not need calculation of sender's position. So we relax the computation requirements of [14] by avoiding calculation of fading through distance. Moreover, we show through experiments that even for a 3-D coordinate system, for sybil node detection, two nodes is enough rather than four receiver nodes that is required in the theory [14]. We show that using two receivers 100% completeness and less than a few percent false positive rate is possible in practice.

Our software for the sybil attack detection program and experiments are available at `http://www.cse.buffalo.edu/~ywsong/data/yw_Sybil_SourceCode.zip`

Outline : After the preliminaries section, in Section III we present our protocol and investigate the variance in RSSI values and ratio of RSSI values from multiple receivers. In Section IV we discuss the experiments with our implemented solution with varying number of detector nodes. Finally, we conclude in Section V.

II. Preliminaries

In this section, we first define the sybil attack problem, and discuss our implementation platform. We then provide a brief summary of the RSSI-based localization protocol in [14] which we base our work.

A. Problem Statements

We assume a static network, where all nodes are immobile after initial deployment. We assume an initial set of nodes that are trustworthy (non-sybil). Later, as part of re-populating the network, new nodes are introduced some of which can be sybil. New nodes may be arriving to the network also due to topology-control and sleep-wake up protocols: Previously sleeping nodes might become active later as part of load balancing [5]. Note that sybil nodes can vary their transmission power between transmissions to trick other nodes.

- **Completeness:** If there is a sybil attack in the network, the protocol can detect sybil attack with probability, greater than.
- **Accuracy:** The protocol should not identify non-sybil nodes as sybil (as this can ultimately render the WSN useless.). In other words, we require the false-positive rate to be less than 10%.

B. Platform

Hardware: The hardware we use is the Mica2 mote [6], [7] with CC1000 chip [1] using 433 MHz radio frequency and FSK. Mica2 has Atmega128 chip for the processor which is running at 4MHz clock frequency. Mica2 has 128KB of flash memory, 4KB SRAM and 4KB EEPROM. All of our RSSI experiments are done in a large in-door environment.

Software: We implement our protocol on TinyOS version 1.1. [3]. We use the default MAC layer, B-MAC [11].

C. RSSI is non-isotropic

In contrast to simplistic representations of radio signal as isotropic, and communication range as uniform, [8] and [15] show that broadcast is non-isotropic in WSN (Figure 1). Therefore, using RSSI value directly for sybil attack detection is unreliable. In fact, later in Section III-B, our experiment shows that it is impossible to detect sybil attack robustly (completely and accurately) by using RSSI values directly. However, as we show next by using ratio of RSSIs from multiple receivers, it is possible to overcome to this problem.

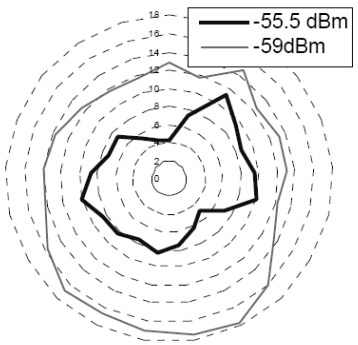


Fig. 1. Non-isotropic connectivity in WSN. (Reprinted from [15])

D. Localization with power

An RSSI-based localization scheme is introduced in [14]. Theorem 5 in [14] argues that if at least four sensors monitor radio signals, then no user can hide its location. Suppose node i receives radio signal from node 0, then the RSSI is

$$R_i = \frac{P_0 \cdot K}{d_i^\alpha} \tag{1}$$

where P_0 represents transmitter power, R_i is RSSI, K is constant, d_i is Euclidean distance, and α is distance-power gradient. Suppose node j receives radio wave from node 0 at the same time, then the P_j is similar to equation (1).

The RSSI ratio of node i to j is

$$\begin{aligned} R_i/R_j &= (\tfrac{P_0 \cdot K}{d_i^\alpha})/(\tfrac{P_0 \cdot K}{d_j^\alpha}) \\ &= (\frac{d_i}{d_j})^\alpha \end{aligned} \tag{2}$$

and the user's location (x, y) can be computed by solving following equation through four receivers, i, j, k, and l:

$$\begin{aligned} (x-x_i)^2 + (y-y_i)^2 &= (\tfrac{R_i}{R_j})^{\frac{1}{\alpha}}((x-x_j)^2 + (y-y_j)^2) \\ &= (\tfrac{R_i}{R_k})^{\frac{1}{\alpha}}((x-x_k)^2 + (y-y_k)^2) \\ &= (\tfrac{R_i}{R_l})^{\frac{1}{\alpha}}((x-x_l)^2 + (y-y_l)^2) \end{aligned} \tag{3}$$

, where x_i and y_i is the location of node i, and other notation is similar.

III. RSSI-based sybil node detection

Here we first present our RSSI-based sybil attack detection protocol in section III-A, and in section III-B, we show that in contrast to nonuniform nature of individual RSSI values, ratio of RSSI values recorded of multiple receivers exhibit a Gaussian PDF, and, hence, are suitable for detection of sybil nodes.

A. Basic Algorithm

It is possible to use the localization algorithm in [14] to detect a sybil attack as follows. Upon receiving a message, the four detector nodes compute the location of sender using equation 3 and associate this location with the sender-ID included in the message. Later when another message with

different sender-ID is received and the location of the sender is computed to be the same as the previous one, the nodes detect a sybil attack.

However, it is very cumbersome to calculate the location in formation using equation 3 for every node. Indeed, we do not need this calculation for sybil node detection. Since all of x, y, and x_i, y_i location stays the same, it is possible to detect sybil attack by just recording and comparing the ratio of RSSI for the received messages.

Here, we describe our protocol in terms of a scenario. Let four monitoring nodes have ID as $D1$, $D2$, $D3$, and $D4$ respectively and a sybil node forge its ID as $S1$, $S2$, and so on with time. Here is an example topology in Figure 2.

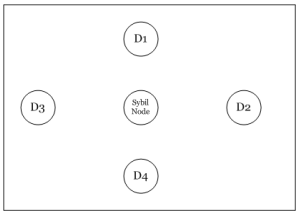


Fig. 2. Example topology

At time t_1, a sybil node broadcasts messages and its forged ID as $S1$. Monitoring four neighboring nodes receive the radio power and the forged ID. Each nodes transmits messages with its own ID and the received RSSI from sybil node to representative node, $D1$. Note R_i^k denotes the RSSI value when sender k receives i. Then, sensor node $D1$ computes each ratio

$$\frac{R_{D1}^{S1}}{R_{D2}^{S1}}, \frac{R_{D1}^{S1}}{R_{D3}^{S1}}, \text{ and } \frac{R_{D1}^{S1}}{R_{D4}^{S1}} \tag{4}$$

and store them in locally.

Similarly, at time t_2, the sybil node broadcasts messages again but different ID as $S2$. Four neighbor nodes monitor each power from the sybil node and report to node $D1$. Node $D1$ computes each ratio

$$\frac{R_{D1}^{S2}}{R_{D2}^{S2}}, \frac{R_{D1}^{S2}}{R_{D3}^{S2}}, \text{ and } \frac{R_{D1}^{S2}}{R_{D4}^{S2}} \tag{5}$$

At this time, node $D1$ can detect sybil node by comparing the ratio at time t_1 and t_2. Node $D1$ concludes if the difference between two information is very close to zero, the sybil attacking is happened in the region since received power ratio is same which means the location is same, but the node broadcasts messages with multiple ID. Otherwise, node $D1$ can tell there is no sybil node. That is, if

$$(\frac{R_{D1}^{S1}}{R_{D2}^{S1}} = \frac{R_{D1}^{S2}}{R_{D2}^{S2}}), (\frac{R_{D1}^{S1}}{R_{D3}^{S1}} = \frac{R_{D1}^{S2}}{R_{D3}^{S2}}), (\frac{R_{D1}^{S1}}{R_{D4}^{S1}} = \frac{R_{D1}^{S2}}{R_{D4}^{S2}}) \tag{6}$$

are true, we can detect sybil attack.

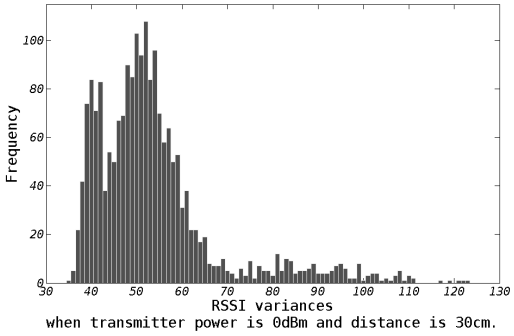
Later, in section IV-A, we show through experiments that even for a 3-D coordinate system, for sybil node detection, two nodes is enough rather than four receiver nodes that is required in the theory [14].

B. Variance of RSSI

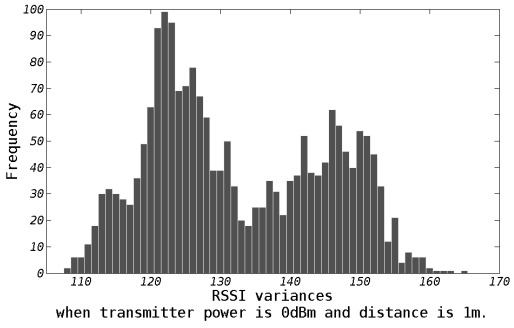
Ideally, RSSI should stay the same if the locations of the two transceivers are fixed, but even in this case RSSI fluctuates a lot in practice. Here we quantify over this fluctuation by experiments, and we investigate the variance of RSSI and how we can overcome it.

Setup1: We deploy a node to transmit "Hello" messages with constant power (0 dBm). Another node acts as a receiver, captures RSSIs[1], and transmits them to the PC through RSC-232 serial interface[2]. The transmitter sends messages over 2000 times. We set the distance between the transmitter and receiver as 30cm. We repeat the experiment by changing distance to 1m.

Result1: Two of the histogram in Figure 3 demonstrates the nonuniform nature of RSSI. The poor correlation of RSSI values makes it unsuitable for detection of sybil attacks. Later as part of our control experiment in Section IV-C, we show that using one receiver sybil attack cannot be robustly detected.



(a) ρ =51.00, μ =53.84, and σ =14.04 with distance of 30cm



(b) ρ =129.00, μ =132.50, and σ =12.56 with distance of 1m

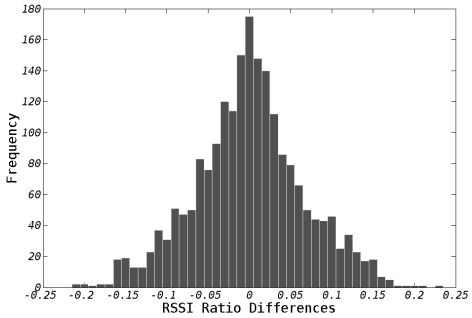
Fig. 3. Variance of RSSI (ρ stands for median value, μ for mean, and σ for standard deviation)

Setup2: Here, we use two receivers (instead of one) and compare ratio of RSSIs at the two receivers (instead of absolute value of RSSIs) to cope with time varying nature

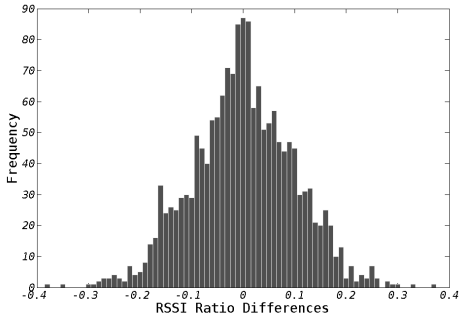
[1]TinyOS provides RSSI reading for each received message automatically via TOS_Msg− >strength

[2]We use a programming board as MIB510 which is connected to PC through RSC-232 serial interface running at 115200 bps

of RSSI. Note that using ratios of RSSIs also takes care of varied transmission power at a sender. In this setup the sender broadcasts messages 2000 times using different (random) transmission power each time. The two receivers record RSSI values and transmit them to the base station which is connected to PC. We repeat experiment twice keeping the same distance of 1m.



(a) $\rho = 0.000$, $\mu = 0.000$, and $\sigma = 0.066$



(b) $\rho = 0.000$, $\mu = 0.000$, and $\sigma = 0.100$

Fig. 4. Variance of difference of RSSI ratio

For the analysis, the basestation computes the ratio of two RSSI values it received from the two receivers at time $t1$, and later does the same for RSSIs received at time $t2$. Then it calculates the difference of two ratios and logs this value. The calculation is repeated throughout the experiment. Histogram in Figure 4 shows the results.

Result2: The histograms show uniform distribution of values. The difference of RSSI ratio of 0 dominates the other values. The values -0.2 and 0.2 occurred only once out of 2000 times (0.05 %) in Figure 4(a), and similarly those of -0.35 and 0.425 in Figure 4(b). Note that the histograms follow Gaussian Probability Distribution Function (PDF) with standard deviation of 0.066 and 0.106 respectively.

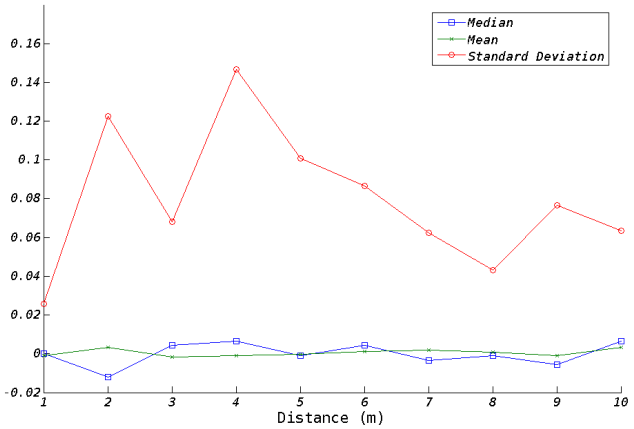
Therefore, if we set the threshold used in judgement of a sybil node to $k * \sigma$, where $k > 3$, and apply the algorithm described in III-A, we can detect sybil attacks robustly using the following equation. If $S1$ and $S2$ are different but their location is same, we can infer the sybil attack by noticing that the difference of RSSI ratios for both cases are within the threshold.

$$(\frac{R_{D1}^{S1}}{R_{D2}^{S1}} - \frac{R_{D1}^{S2}}{R_{D2}^{S2}}) < \sigma, (\frac{R_{D1}^{S1}}{R_{D3}^{S1}} - \frac{R_{D1}^{S2}}{R_{D3}^{S2}}) < \sigma \text{ , and } (\frac{R_{D1}^{S1}}{R_{D4}^{S1}} - \frac{R_{D1}^{S2}}{R_{D4}^{S2}}) < \sigma \quad (7)$$

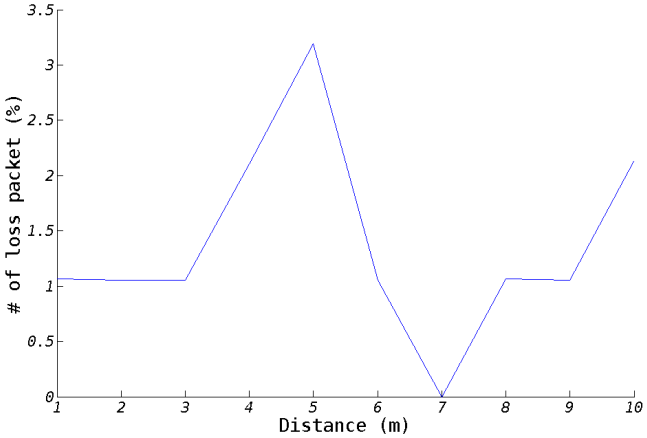
The standard deviation in Gaussian PDF covers around 70% of values, hence setting the threshold to σ means that sybil node is detected with 70% probability. To cover more than 99.999999%, we set the threshold to be 5σ, more specifically 0.5 in our sybil attack detection experiments.

Setup3: In order to evaluate the effect of distance on σ, here we repeat the experiment in Setup2 with respect to increasing distances between the transmitter and the receivers. We performed 100 transmissions at each distance, and vary the distance between 1m to 10m.

Result3: The result is shown in Figure 5(a). We see that σ does not stray away from 0.1. Therefore, we conclude it is safe to set σ as 0.1 and threshold to 0.5 for detection of sybil node attacks.



(a) Various Median, Mean and Standard deviation by distance



(b) Number of lost messages

Fig. 5. Observation according to distance

Note that this experiment is performed in an in-door environment. According to [13], usually gray area (non-deterministic communication range) starts from 20 meter in in-door environment. All of our experiments and readings fall within the in-band communication range and are not subject to the gray area problems.

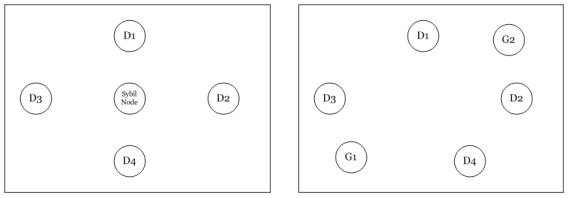
IV. Experiments

Here we test our RSSI based sybil attack detection protocol under different setups. First, in Section IV-A we use four receivers for detection. In Section IV-B, we use only two receivers and show that the protocol achieves the similar performance to the four receiver case. Finally, as a control experiment, we use the single receiver setup (restricting the sybil nodes from varying their transmission power) to evaluate completeness and accuracy in this case.

A. Sybil experiments with four detectors

We perform two experiments, the first for evaluating completeness, second for accuracy. The first experiment uses the topology in Figure 6(a), and the second in Figure 6(b).

Setup4: Figure 6(a) shows a sybil node and four receiver nodes in the network. When a sybil node sends a message, each of the four detectors records the RSSI value and ID associated with the message, and the remaining three nodes transmit their readings to node D1. When the sybil performs another broadcast with different ID and different transmission power, each of the four detectors records the readings for this message, and the information is again accumulated at node D1. Next D1 detects whether there is a sybil attack in the network using Equation 7. We set the threshold to be $5 * \sigma$, which is 0.5 according to section III-B. To avoid message collisions during the experiment, we regulate the message transmission times using timers at each node. In our experiment, the sybil node broadcasts every 30 seconds, and each receiver transmit to D1 with 3 second intervals after the sybil node's detection.



(a) Topology in case of four monitoring nodes and one sybil node

(b) Topology in case of four monitoring nodes and no sybil node. Gx represents good nodes, Dx, detectors

Fig. 6. Sybil attack experiment with four detectors

Result4: We repeated the above experiment 100 times, before each instance we changed the deployment location of receiving nodes and the sybil node. Using 30 second intervals for sybil node transmission meant that we changed the topology once every minute. We saw that node D1 always detected the sybil attack in all instances.

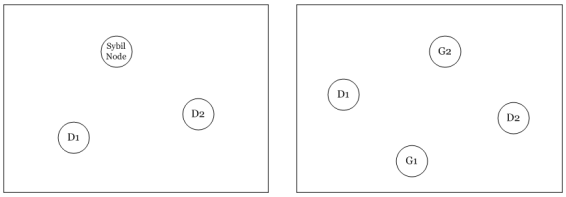
Setup5: To test for accuracy (absence of false-positives), we changed the setup to the topology in Figure 6(b). Here, we eliminated the sybil node in the network, and deployed two good nodes which broadcasts only their own IDs. The good nodes used varying transmission powers [9], as due to energy-efficiency purposes some protocols require nodes to transmit with varying transmission power, also as the battery power decreases and environmental factors change transmission power inevitably changes. Note that, since the receivers use ratio of RSSI values, the varying transmission powers have no effect in correct evaluation of good nodes versus sybil nodes. We changed the location of good nodes for each run to force a false-positive at the detectors.

Result5: In none of our 100 tries node D1 complained about a sybil attack. Even when the two good nodes are located within centimeters of each other, D1 was able to tell that there was no sybil node in the network. Therefore, we conclude that RSSI-based scheme for sybil attack detection using four detectors satisfies our accuracy requirements.

B. Sybil experiments with two detectors

We again perform two experiments, the first for evaluating completeness, and second for accuracy. The first experiment uses the topology in Figure 7(a), and the second in Figure 7(b).

Setup6: Here we have two receivers and a sybil node. Otherwise, the experiment is performed as in Setup 4. We repeated the experiment 100 times changing the deployment location of nodes in between iterations. Since there are only two receivers, we used only one comparison in Equation (7).



(a) Topology in case of two monitoring nodes and a sybil node

(b) Topology in case of two monitoring nodes and no sybil node. Gx represents good nodes, Dx, detectors

Fig. 7. Sybil attack experiment with two detectors

Result6: Similar to Result4, node D1 always detected a sybil attack.

Setup7: In order to see that the detectors can distinguish whether there is sybil or good case, we setup like in Figure 7(b). In the setup, there is two monitors and two good nodes. Each good nodes has distinct ID and uses different transmission power. Two detectors work as in Section IV-A except for comparing just one time. The experiment was repeated 100 times changing location of good nodes to force a false-positive at the detectors.

Result7: 3 cases out of 100 times, node D1 detected a sybil attack inaccurately. That is, when using only two receivers, upto 5% false-positives may be possible.

Remark: These false-positive experiments are best effort in that they do not provide an absolute scale for false-positives for

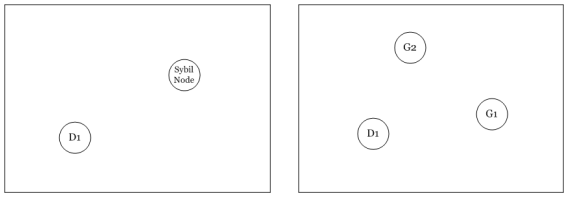
any environment or distance. Rather, they help us compare the false-positive rates when using varying number of detectors, as we try to perform the false-positive experiments similarly for each case. *(End of remark)*

Note that in the two receiver case, only one transmission is enough for sybil node detection, that of node D2 to D1. Hence, the overhead is very low in this case, but the tradeoff is increased false-positive rate. However, for sybil attack problem completeness is more critical than the accuracy: Not detecting a sybil node has severe implications for security, whereas falsely detecting upto 5% of nodes as sybil has only implications in reducing the system performance. Based on this observation, we suggest that RSSI-based scheme for sybil attack detection using two detectors is more suitable than the four node version for practical deployments.

C. Control experiments with one detector

Here we perform experiments with only one detector for comparison. Since with one detector it is impossible to use the equation 7 and differentiate between multiple transmission powers, we restrict the transmitters to always use the same transmission power.

Setup8: The topology is as in Figure 8(a). Since the sybil node is limited to use the same transmission power, we use the difference of RSSI values directly and use the standard deviation "15" as per the experiment in III-B. We performed two experiments, one with threshold $\sigma = 15$ and the other with threshold $5\sigma = 75$. Each experiment was executed around 4000 times.



(a) Topology in case of one monitoring node and a sybil node

(b) Topology in case of one monitoring node and no sybil node

Fig. 8. Sybil Node experiment with one detectors

Result8: Since sybil node always uses constant transmission power and its location is not changed also, receiver detects sybil attack if received node ID is different and RSSI variance is within threshold. In this test, the receiver warned of a sybil attack in 99% of the cases with σ threshold and all cases with 5σ threshold.

Setup9: Here we test for accuracy of sybil attack detection with one receiver. The topology is as in Figure 8(b). We used the two thresholds as before and performed the two experiments around 100 times changing the location of good nodes between each run.

Result9: We observed that the receiver detects a false-positive about 25% of the time with threshold set to σ (Figure 9). Moreover, when the threshold is set to 5σ, the false-positive rate becomes 80%. That is, due to the very high ratio of false-positives, single detector is unsuitable for sybil node detection.

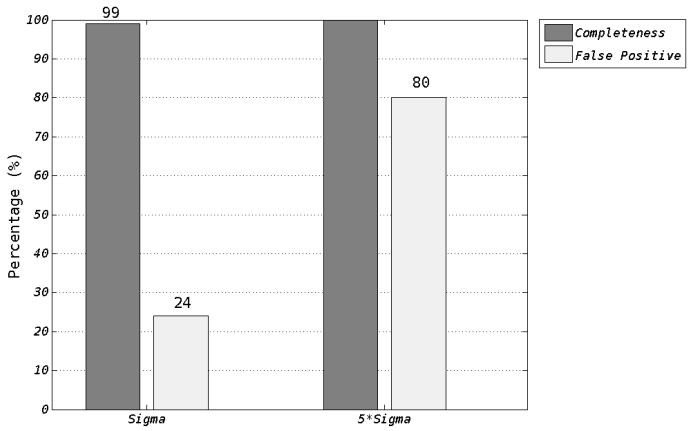


Fig. 9. Accuracy and completeness using one receiver

V. Concluding remarks

We presented an RSSI-based solution for the sybil attack problem in WSN. We showed that even though RSSI is time-varying and unreliable in general and radio transmission is non-isotropic, using ratio of RSSIs from multiple receivers it is feasible to overcome these problems. Our protocol is lightweight—alongside the receiver we need the collaboration of one other node— and robust—we achieve detection with 100% completeness and less than a few percent false positives.

In future work we will try to answer how we can extend our protocol to tolerate existing sybil nodes in the network. We will test our protocol in a large-scale WSN testbed, Kansei [12], in preparation for using our solution in real deployments.

References

[1] Chipcon. Cc1000 radio datasheet. `www.chipcon.com/files/CC1000_Data_Sheet_2_3.pdf`, 2003.

[2] J. R. Douceur. The sybil attack. In *IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pages 251–260, 2002.

[3] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler. The nesc language: A holistic approach to networked embedded systems. In *PLDI '03: Proceedings of the ACM SIGPLAN 2003 conference on Programming language design and implementation*, pages 1–11, 2003.

[4] Philippe Golle, Dan Greene, and Jessica Staddon. Detecting and correcting malicious data in vanets. In *VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pages 29–37, New York, NY, USA, 2004. ACM Press.

[5] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. In *HICSS '00: Proceedings of the 33rd Hawaii International Conference on System Sciences-Volume 8*, page 8020, 2000.

[6] J. Hill and D. Culler. Mica: A wireless platform for deeply embedded networks. volume 22(6), pages 12–24, Nov/Dec 2002.

[7] J. Hill, R. Szewcyk, A. Woo, D. Culler, S. Hollar, and K. Pister. System architecture directions for networked sensors. November 2000.

[8] D. Kotz, C. Newport, R. S. Gray, J. Liu, Y. Yuan, and C. Elliott. Experimental evaluation of wireless simulation assumptions. In *MSWiM '04: Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 78–82, 2004.

[9] Li Li, Joseph Y. Halpern, Paramvir Bahl, Yi-Min Wang, and Roger Wattenhofer. A cone-based distributed topology-control algorithm for wireless multi-hop networks. *IEEE/ACM Trans. Netw.*, 13(1):147–159, 2005.

[10] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *IPSN'04: Proceedings of the third international symposium on Information processing in sensor networks*, pages 259–268, 2004.

[11] J. Polastre, J. Hill, and D. Culler. Versatile low power media access for wireless sensor networks. In *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 95–107, 2004.

[12] OSU NEST ExScal Team. Kansei: Sensor testbed for at-scale experiments. `http://www.cse.ohio-state.edu/kansei`.

[13] J. Zhao and R. Govindan. Understanding packet delivery performance in dense wireless sensor networks. In *SenSys '03: Proceedings of the 1st international conference on Embedded networked sensor systems*, pages 1–13, 2003.

[14] S. Zhong, L. Li, Y. G. Liu, and Y. R. Yang. Privacy-preserving location-based services for mobile users in wireless networks. Technical Report YALEU/DCS/TR-1297, Yale Computer Science, July 2004.

[15] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic. Impact of radio irregularity on wireless sensor networks. In *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 125–138, 2004.