Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding

Weichao Wang
Department of SIS
Univ. North Carolina Charlotte
Charlotte, NC 28223
weichaowang@uncc.edu

Di Pu and Alex Wyglinski
Department of ECE
Worcester Polytechnic Institute
Worcester, MA 01609
dipu@wpi.edu and alexw@ece.wpi.edu

Abstract

Previous research on the security of network coding focuses on the detection of pollution attacks. The capabilities of network coding to detect malicious attacks have not been fully explored. We propose a new mechanism based on physical layer network coding to detect the Sybil nodes. When two signal sequences collide at the receiver, the starting point of the collision is determined by the distances between the receiver and the senders. When the distance between two receivers is large enough, they can combine their interference sequences to recover the original data packets. On the contrary, the Sybil nodes attached to the same physical device cannot accomplish the data recovery procedure. We have proposed several schemes at both physical and network layers to transform the idea into a practical approach. The investigation shows that the wireless nodes can effectively detect Sybil nodes without the adoption of special hardware or time synchronization.

1 Introduction

Investigators have proposed the concept of physical layer network coding [14, 26] to improve network throughput for multicast traffic, reduce network congestion, and enhance network robustness. The technique is especially valuable in wireless networks when we consider the limited bandwidth and power resources of the nodes. Since network coding may allow data errors and/or corrupted packets to propagate widely and ruin the data recovery procedure at the final destination, previous research into network coding security focused on the protection of data dissemination procedures and the detection of pollution attacks [2, 5].

However, the security capabilities of physical layer network coding to detect malicious attacks have not been fully explored. For instance, it is possible that when signals collide at the receiver, we can extract information about the network structure. This information can then be used to detect attacks on network topology. In this paper, we conduct an initial investigation of this problem. Specifically, we propose a new mechanism to estimate the distance between two wireless nodes and detect Sybil attacks.

Several reasons lead us to choose the detection of Sybil attacks in wireless networks as the primary research topic. First, Sybil attacks impose severe threats to wireless network security. If the same physical device can illegitimately act with multiple identities in the network, it can attack the routing protocols [13] and misbehavior detection mechanisms [18]. Second, a Sybil attack is a representation of stealth attacks on wireless networks, where traditional methods such as encryption and authentication cannot defend against such attacks. Therefore, a detection method based on physical layer network coding will allow us to better understand this problem. Finally, although investigators have proposed the Sybil detection methods based on the signal-level signatures [4], these approaches usually depend on some special hardware [3] or the inaccurate signal propagation models [4]. Our approach does not require time synchronization among wireless nodes or depend on any special hardware.

The basic idea of our proposed approach is as follows: when the long sequences of signals from two senders collide at the receiver, the starting point of collision between the sequences is jointly determined by the sending time and the physical distances between the receiver and the senders. For two receivers, their starting points of collision could be different, and this difference is restricted by the physical distance between them. Therefore, through measuring the interfered parts of the received sequences, we can estimate the physical distance between two receivers. Our analysis will show that when the time difference between the starting points of collision is large enough, the receivers can combine the interfered signals to recover the original data packets. On the contrary, if the two receivers are the Sybil nodes attached to the same physical device, they will receive the same interfered sequences and they cannot accomplish the data recovery operation. In this way, we can distinguish two

978-1-4244-7499-8 /10/$26.00 ©2010 IEEE

separate nodes from the Sybil identities. Since the proposed approach only measures the starting points of collision in the sequences, we do not need time synchronization among the wireless nodes. Our analysis will also show that the approach does not depend on any special hardware. Therefore, the method can be adopted by existing systems without significant difficulty.

Although the basic idea of the proposed approach is clear, we need to design schemes at both physical layer and network layer to make the approach practical. At the physical layer, we need to carefully select data transmission parameters such as modulation and carrier frequency. Consequently, algorithms are designed to recover the received sequences. At the network layer, we need to determine the senders and their data sequences. Mechanisms must be designed to reconstruct the data packets from the interfered signals. The wireless nodes need to verify the authenticity of the recovered sequences. Analysis will be conducted to study the detection capability of the proposed approach and its relationship to the network parameters.

Compared to previous approaches, our investigation has the following contributions:

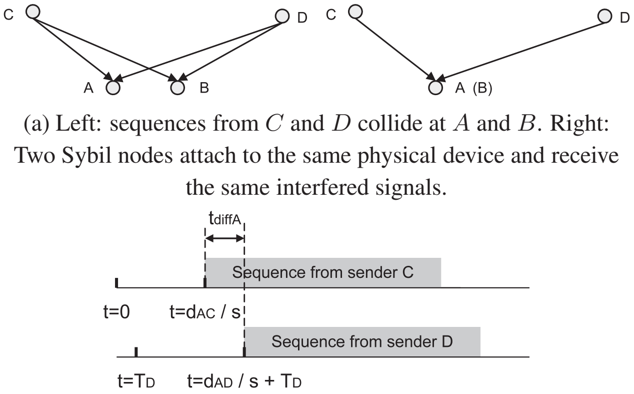
- The research will demonstrate that in addition to improving the bandwidth efficiency and data robustness in wireless networks, physical layer network coding can also be used to detect malicious attacks. This research provides a new incentive for further development of this technique.
- The proposed Sybil detection mechanism does not require any special hardware or time synchronization in the wireless network. Therefore, existing systems can adopt the proposed approach without significant difficulty.
- We carefully design schemes in both network layer and physical layer to make the approach practical. Impacts of different factors on the proposed approach are also studied.

The remainder of the paper is organized as follows: in Section 2, we introduce the basic idea of the detection mechanism. Sections 3 and 4 design mechanisms in the physical layer and the network layer to make the approach secure and practical. In Section 5 we study the security of the proposed approach. Section 6 reviews the related work. Finally, Section 7 concludes the paper.

2 The Basic Idea

In this part, we introduce the basic idea of using physical layer network coding to detect the Sybil attacks. We assume that two wireless nodes are neighbors when the distance between them is shorter than r. However, this assumption does not restrict wireless nodes from transmitting signals at a higher power level in order to reach a longer distance. We consider the direct communication model of the Sybil attacks described in [18]. Under this model, multiple fake identities attached to the same physical device can directly communicate to other legitimate nodes. We assume that every wireless node (including the attackers) is equipped with an omni-directional antenna. Extending our approach to multi-antenna systems will be studied in future work.

We use d_{MN} to represent the Euclidean distance between two nodes M and N. We use T to represent a specific moment and t to represent a time duration. If the radio wave propagates at the speed s, the transmission delay between M and N will be $\frac{d_{MN}}{s}$. In the following analysis, we use the difference between the arriving time of two sequences. We must clarify that we are not using the system clocks in the wireless nodes to directly measure the actual time. On the contrary, we can locate the starting point in the sequence that the collision starts. Then we can translate this information into a time difference using the frequency of the radio signal. This topic is discussed further in Section 5.1.



(a) Left: sequences from C and D collide at A and B. Right: Two Sybil nodes attach to the same physical device and receive the same interfered signals.

(b) t_{diffA}: difference b/w arriving time of two sequences at A.

Figure 1. Two sequences collide at receivers.

Figure 1.(a) illustrates an example of the signals colliding at two receivers. We assume that nodes A and B are two different nodes in the network. The other nodes in the network want to verify that they are not Sybils on the same device. They jointly choose two senders, C and D, in the network that can both hear from. C and D will then send out long pseudo-random sequences that will collide at A and B. Without losing generality, we assume that node C will send out its sequence first. We also assume that C starts sending at $T_C = 0$ and D starts sending at $T_D \geq 0$.

Based on these assumptions, we can derive that A will receive the signals from C at the time $\frac{d_{AC}}{s}$, and the signals from D at $(T_D + \frac{d_{AD}}{s})$. Therefore, the difference between the arriving time of the two sequences is $t_{diffA} = (T_D + \frac{d_{AD} - d_{AC}}{s})$, as illustrated in Figure 1.(b). In other words, A will first receive the sequence from C for t_{diffA} seconds, then the two sequences will collide at the node. If $t_{diffA} < 0$, the sequence from D will arrive first at A. Similarly, we can derive the difference between the arriving time at node B as $t_{diffB} = (T_D + \frac{d_{BD} - d_{BC}}{s})$. Now let us look at the difference between t_{diffA} and t_{diffB}:

$$\begin{aligned} & t_{diffB} - t_{diffA} \\ = & (T_D + \frac{d_{BD} - d_{BC}}{s}) - (T_D + \frac{d_{AD} - d_{AC}}{s}) \\ = & \frac{(d_{BD} - d_{AD}) + (d_{AC} - d_{BC})}{s} \end{aligned} \tag{1}$$

For the three nodes A, B, and D, they either form a triangle or stay on the same line. Either way, we must have $||(d_{BD} - d_{AD})|| \leq ||d_{AB}||$. Similarly, we have $||(d_{AC} - d_{BC})|| \leq ||d_{AB}||$. Therefore, we must have:

$$\begin{aligned} & ||(t_{diffB} - t_{diffA})|| \\ = & \frac{||(d_{BD} - d_{AD}) + (d_{AC} - d_{BC})||}{s} \\ \leq & \frac{||d_{BD} - d_{AD}||}{s} + \frac{||d_{AC} - d_{BC}||}{s} \\ \leq & \frac{||d_{AB}||}{s} + \frac{||d_{AB}||}{s} = \frac{2 \times d_{AB}}{s} \end{aligned} \tag{2}$$

From Equation (2), we can see that the difference between t_{diffA} and t_{diffB} is restricted by the Euclidean distance between nodes A and B. We will derive the distribution of the difference in later section of the paper. In this way, through measuring the time differences from multiple pairs of senders, we can have a good estimation of the distance between A and B.

When two Sybil nodes are attached to the same physical device, they will receive the same interfered signals and t_{diffA} = t_{diffB}. No matter how many different pairs of senders we try, we will always have $t_{diffA} - t_{diffB} = 0$.

While the analysis shows that the difference between t_{diffA} and t_{diffB} can be used to detect the Sybil nodes, we need a mechanism to verify the time difference. We cannot directly use t_{diffA} and t_{diffB} reported by the receivers since the malicious nodes will lie about the values. Fortunately, we have the observation that when $||t_{diffA} - t_{diffB}||$ is large enough, the two receivers can combine their received signals to recover the two sequences. On the contrary, when $t_{diffA} - t_{diffB} = 0$, the receivers cannot accomplish the data recovery operation. Below we use a simplified example to show the idea. The real mechanism to separate the interfered signals depends on the physical layer parameters such as modulation. We will present the mechanism in detail in Sections 3 and 4.

Figure 2 shows the two sequences that are sent out by node C and D. Without losing generality, we assume that the collisions at node A and B happen at the fourth and seventh bits of sequence C respectively. If the interference results can be viewed as the sum of the two signals, Figure 2 also shows the received sequences at A and B. If the interfered signal is '0' or '2', the corresponding bits in both sequences are '0' or '1'. However, if the interfered signal is '1', the receiver cannot tell which sequence contains the bit '1'. The receiver can take a wild guess but it has only 50% chance to guess correctly. Therefore, when the received sequences are long enough, a single receiver cannot recover the two sequences. However, if nodes A and B combine their information, they can accomplish the data recovery task. As illustrated in Figure 2, since B already knows that the fourth bit in sequence C is a '1', it can help A to figure out that the first bit of sequence D is '0'. This will then help B to determine that the seventh bit from C is '1'. This procedure will continue and A and B will recover the two sequences.

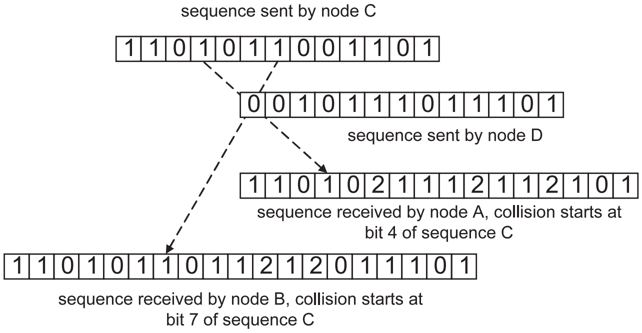


Figure 2. Data recovery of the colliding sequences at the wireless nodes.

From this example, we find that when the difference between t_{diffA} and t_{diffB} is large enough, the two receivers can combine their information to reconstruct the sequences. On the contrary, the two Sybil nodes will receive the same group of signals and they cannot accomplish the task. The reconstructed sequences can be easily verified by other nodes since the original signals propagate in all directions. In this way, we can detect the Sybil nodes.

The proposed approach has several highly desirable properties. First, since the mechanism uses only the starting points of the collisions to detect the Sybil nodes, we do not need the wireless nodes to synchronize their clocks. Second, the proposed mechanism does not require the wireless nodes to be equipped with any special hardware which will result in a lower node cost. Third, the proposed approach works in a distributed manner and does not require a centralized controller. With these desirable properties, the approach can be easily adopted by existing networks.

3 Building a Practical Approach: Physical Layer Issues

To turn the proposed approach into a practical solution, we need to choose the modulation/demodulation methods to map the digital bits to the radio waves. We also need to design the decoding algorithms at the receivers so that they can separate the interfered signals and recover the data bits. Since we do not assume clock synchronization among the nodes, the physical layer needs to locate the starting point of the collision to derive the time difference. In the following subsections, we will describe the selected modulation method and the data separation mechanism.

3.1 Modulation of Signals with MSK

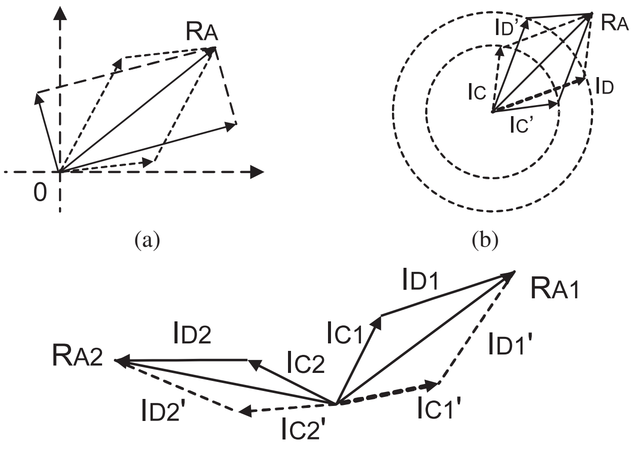
We build our approach upon the successful 'analog network coding' project [14] by the MIT investigators and choose the MSK modulation to map the data bits to the radio waves. MSK represents the data bits by varying the phase difference between consecutive complex signals. Specifically, a phase difference of $\pi/2$ represents bit '1', and a difference of $-\pi/2$ represents bit '0'. In this way, MSK is different from many other modulation methods: the receiver has to capture two consecutive signals to decode one bit.

When the signal traverses the communication channel, its amplitude and phase will change. These changes will not have a large impact on the decoding accuracy of MSK because of the following reasons. First, MSK does not use variations in the amplitude to represent data bits. Second, although the phase shifts will have an impact on the demodulation accuracy, previous research [11] shows that the shifts are relatively stable within a short period of time. In this way, when we compute the angle between two consecutive signals, the phase shift will cancel out. Therefore, we conclude that MSK is very robust against the attenuation and phase shifts caused by the channel. At the same time, the structure of the receiver is much simpler compared to the other modulation schemes, resulting in lower implementation costs of the proposed approach.

3.2 Signal Decoding Procedure

In this part, we describe the operations at a receiver to separate and decode the interfered signals. When the signals from the senders C and D collide at the receiver A, A will get the vector sums of them. If we consider one symbol from C and one symbol from D that collide at A, the received signal at A is $\overrightarrow{R_A} = \overrightarrow{I_C}+\overrightarrow{I_D} = I_C \cdot e^{i\theta_C} + I_D \cdot e^{i\theta_D}$. Here I_C and θ_C jointly describe the symbol from C, and I_D and θ_D jointly describe the symbol from D.

An intuitive illustration of $\overrightarrow{R_A}$ is shown in Figure 3.(a). Here $\overrightarrow{R_A}$ is the vector sum of the two signals from C and D. If A has no prior knowledge about the signals $\overrightarrow{I_C}$ and $\overrightarrow{I_D}$, there are many different combinations of the vectors to construct $\overrightarrow{R_A}$. We show two possible solutions in Figure 3.(a). To solve this problem, the investigators have designed a two-step approach [14]. They first estimate the magnitudes of the two vectors. In the second step, they determine the phases of the signals.



(a)

(b)

(c)

Figure 3. Signal interference and separation.

There are two methods that we can adopt to estimate the magnitudes of the vectors. First, when the two senders C and D are chosen, A can ask the two nodes to send out test signals at the power level that the sequences will be sent out. If we assume that the attenuation functions of the channels are stable, this method can provide a reasonably good estimate.

In the second method, we use the results presented in [9] to estimate the amplitudes of the two signals. We need two equations to solve the two variables I_C and I_D. First, for the long random sequences, we have

$$E[|\overrightarrow{R_A}|^2] = \mu = I_C^2 + I_D^2 \tag{3}$$

With this equation, A can calculate the average energy of a number of samples to estimate $I_C^2 + I_D^2$.

To get the second equation for the problem, A can calculate $\sigma = \frac{2}{N} \sum_{|\overrightarrow{R_A}|^2>\mu} |\overrightarrow{R_A}|^2$. Here it will use only the samples whose squared norm is greater than μ. It has been shown in [9] that $\sigma = I_C^2 + I_D^2 + 4 \cdot I_C \cdot I_D/\pi$. Combining these two equations, A can get the magnitudes of the two vectors.

Now A knows the amplitudes of the two signals and their vector sum. There are only two possible solutions to construct $\overrightarrow{R_A}$ with $\overrightarrow{I_C}$ and $\overrightarrow{I_D}$, as illustrated in Figure 3.(b). Now looking at a single signal $\overrightarrow{R_A}$ will not allow us to determine which solution is correct. The receiver A can then adopt two methods to estimate the phases of the signals.

In the first method, we assume that A has some prior knowledge about one of the colliding sequences. It will then look at two consecutive signals and use its prior knowledge to solve the problem. Figure 3.(c) shows the two consecutive signals $\overrightarrow{R_{A1}}$ and $\overrightarrow{R_{A2}}$ and the four different combinations to construct them when the magnitudes of the individual vectors have been determined. If A already knows the bit in sequence C, it can choose the best fit from the four combinations $(\overrightarrow{I_{C1}}, \overrightarrow{I_{C2}})$, $(\overrightarrow{I'_{C1}}, \overrightarrow{I_{C2}})$, $(\overrightarrow{I_{C1}}, \overrightarrow{I'_{C2}})$, and $(\overrightarrow{I'_{C1}}, \overrightarrow{I'_{C2}})$. As soon as the vectors of sequence C are determined, the vectors of sequence D are also determined. In this way, A accomplishes the decoding procedure.

In the second method, neither A nor B has any prior knowledge about the colliding sequences. However, as the analysis in Section 2 shows, the starting points of collision at the receivers may be different since their distances to the senders are different. In Section 4 we will show that when the difference is large enough, the two nodes can combine their information to recover the sequences.

3.3 Practical Issues

Detection of Collision The receiver needs to distinguish three states of the system: no signal, one incoming sequence, and two colliding sequences. To detect the arrival of the first data sequence, the receiver can monitor the incoming energy level since the received signal demonstrates a much higher energy level than that of the noises.

Since our approach does not require the wireless nodes to maintain synchronized clocks, there is a good chance that the two sequences will arrive at the receiver at different time points. Therefore, the receiver must be able to locate the starting point of the collision. Before this point, the receiver runs standard MSK decoding. After this point, the receiver needs to separate the interfered signals. To distinguish the two states, the receiver can measure the variance in the energy level of the incoming signals. Since MSK encodes the bits in the phase, the energy of a non-interfered signal is almost constant. When two signals collide at the receiver, the variance will become much larger. Therefore, we can set up a threshold. When the variance becomes larger than the value, the sequence separation algorithm will be executed.

4 Building a Practical Approach: Network Layer Issues

4.1 Assumptions and Model of Attackers

We adopt the unit disk graph model in this work and assume that two wireless nodes are neighbors when the distance between them is shorter than r, where r is defined as the communication range for the nominal transmission power. We assume that the links among wireless nodes are bidirectional. The wireless nodes are equipped with omni-directional antennas and they can adjust the transmission power such that the signal range can be increased to, e.g. $2r$. We also assume that the communication channel is half duplex and a node cannot transmit and receive signals at the same time. The wireless nodes will periodically broadcast neighbor discovery beacons such that changes in neighbor lists can be detected.

We assume that the wireless nodes share a secure, lightweight pseudo random bit generator (PRBG) [12, 16]. The senders will use this generator to produce the sequences. By exchanging only the seeds for the PRBG, the other nodes can regenerate the sequences and verify their authenticity. This also prevents a malicious node from using a sequence that is different from what it has sent out to conduct the Sybil detection and frame innocent nodes. We assume that the wireless nodes establish pairwise keys [25] to protect the data traffic amongst them. Note that the generation and maintenance of the keys is beyond the scope of this paper.

For the attackers, we assume that they have the legitimate identities and all knowledge (such as the pairwise keys) bound to these identities. We assume that the attackers use the direct communication model [18] in which multiple fake identities attached to the same physical device can directly communicate to the legitimate nodes. The attackers cannot break the secret keys of the legitimate nodes that are not under their control. Each malicious device is equipped with an omni-directional antenna. Extending our approach to multi-antenna systems will be studied in future work.

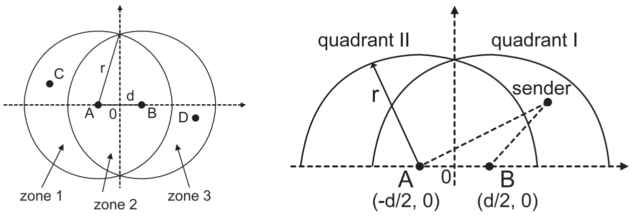
4.2 Operations at the Sender Side

In this subsection we present the operations at the sender side. We focus on the selection of the senders and the generation and verification of the sequences.

1. Selection of Senders

The analysis in Section 2 shows that the distances among the senders and receivers will be removed from equation 2. This implies that there are not many restrictions on the areas from which the senders can be chosen. However, in a real wireless network, several reasons restrict us from choosing a sender that is far away from the receivers. For example, a sender that is far away from the receivers has to transmit the signal at a high power level. This will not only consume the limited battery power of the sender but also cause interference in a large area. Therefore, we propose to choose the senders from the union of the neighbor lists of the receivers.

Figure 4.(a) shows the areas that the senders can be chosen from. Since the Sybils nodes attach to the same physical device and send out the signals through the same antenna, they will share many common neighbors. Therefore, our Sybil detection mechanism will examine the identity pairs that share at least one common neighbor. We can derive that the distance between two nodes that share a neighbor is at most $2r$. In Figure 4.(a), nodes A and B are under Sybil detection and they need to prove that they are not attached to the same physical device. The sender C is a direct neighbor of A and D is a direct neighbor of B. Since A and B are within $2r$, the senders must be within the distance $3r$ to both of the receivers. In this way, the senders can adjust their transmission power to make sure that the signals can be received by both A and B.



(a) (b)

Figure 4. Areas to select the senders and the difference of the distances.

This scheme will greatly increase the pool of senders that we can choose from. As shown in Figure 4.(a), if we require the senders to be direct neighbors of both receivers, we can choose senders only from zone 2. Now we can choose from zones 1 and 3 as well. If the distance between A and B is d where $(d \leq 2r)$, the size of zone 2 is:

$$Area_{zone2} = 2r^2 \arccos(\frac{d}{2r}) - d\sqrt{r^2 - (\frac{d}{2})^2}$$

and the size of zone 1 is $\pi r^2 - Area_{zone2}$. The probability distribution function of the distance between two nodes within $2r$ is given by $F(d) = P(distance < d) = x^2/4r^2$. Therefore, we can calculate the expected size of zone 2, which equals to $0.25\pi r^2$. We find that on average the ratio between the total size of zones 1, 2 and 3 and the size of zone 2 $= \frac{2\pi r^2 - 0.25\pi r^2}{0.25\pi r^2} = 7$. This implies that our approach has a much larger pool of senders to conduct the Sybil detection. More discussions on sender selections and their impacts on the detection accuracy and efficiency will be presented in the later parts.

2. Generation of Sending Sequences

The transmitted sequences should satisfy two requirements. First, the sequences should be kept as secrets from the receivers and they have to separate the interfered signals to reconstruct them. Second, after the seeds for the PRBG are determined, the senders cannot send out other sequences. The first requirement will guarantee that the receivers cannot learn the sequences from some other schemes to compromise the proposed approach. Since the selected senders themselves could be malicious, the second requirement allows all nodes that receive the sequences to verify their authenticity, and prevents the senders from manipulating the data to control the detection results.

To satisfy these requirements, the wireless nodes can use the following procedure to generate the sequences. We assume that every node is equipped with the same pseudo random bit generator (PRBG). First, the neighbors of the nodes under Sybil detection will use a procedure to randomly choose two senders. The sender selection procedure can be accomplished by some trusted nodes or built upon the leader election methods [15]. Each of the senders will then choose a random number as the seed for the PRBG. The senders will apply a one way function to the seeds and broadcast the results as the commitment to the sequences. At this time both requirements are satisfied. Each of the senders can then wait for a random period of time and start its transmission.

4.3 Operations at the Receiver Side

In this subsection, we investigate two problems. First, under what conditions can the two receivers combine their received signals to recover the two sequences? Second, what will be the recovery procedure? Specifically, we will show that only when the difference between t_{diffA} and t_{diffB} is larger than a certain value, the two receivers can accomplish the data recovery task. This result will provide a foundation for the analysis of the detection capabilities of our approach, which will be presented in Section 4.4.

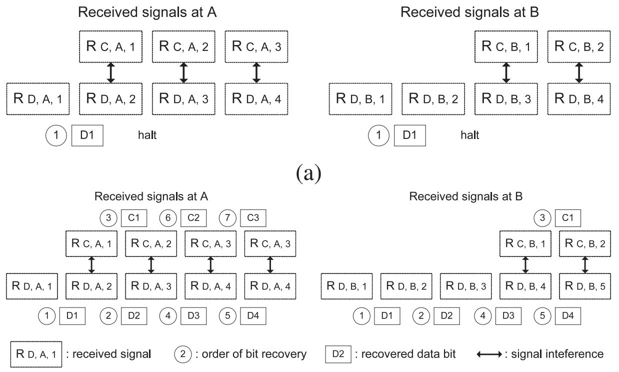
Since in MSK we use the phase shifts between consecutive signals to encode the data bits, in the following analysis we use the number of signals between the starting points of the collisions at A and B to represent $t_{diffB} - t_{diffA}$. We assume that the jth signal sent by node C is represented as $S_{C,j}$. When A receives the jth signal from C, it is represented as $R_{C,A,j}$. If $R_{C,A,3}$ and $R_{D,A,1}$ collide at node A, we define t_{diffA} as $3 - 1 = 2$. Similarly, if B receives the sequence from node D first and $R_{C,B,1}$ and $R_{D,B,4}$ collide, we have $t_{diffB} = 1 - 4 = -3$.

If $||t_{diffB} - t_{diffA}|| = 0$, the nodes A and B receive the same colliding sequences. Based on the analysis in Section 2, we can see that when A and B combine their information, they do not get any new knowledge. Since neither A nor B has any prior knowledge about the sequences, they will not be able to reconstruct the data bits.

If $||t_{diffB} - t_{diffA}|| = 1$, the difference between the starting points of the collisions at the two nodes is one signal. Without losing generality, we assume that $R_{C,A,1}$ and $R_{D,A,2}$ collide, and $R_{C,B,1}$ and $R_{D,B,3}$ collide. The scenario is shown in Figure 5.(a). Since B receives the signals $R_{D,B,1}$ and $R_{D,B,2}$, it will be able to decode the bit between $S_{D,1}$ and $S_{D,2}$. When B shares this information with A, A will be able to determine the vector of the signal $R_{D,A,2}$. This will allow A to determine the vector of the signal $R_{C,A,1}$. However, in MSK the receiver needs two consecutive signals to decode a bit. Note that although $R_{C,B,1}$ and $R_{C,A,1}$ come from the same signal $S_{C,1}$, the communication channels may have different impacts on them. Therefore, even if A sends the vector $R_{C,A,1}$ back to B, B will not be able to separate $R_{C,B,1}$ from $R_{D,B,3}$. The decoding procedure will halt, as illustrated in Figure 5.(a).

If $||t_{diffB} - t_{diffA}|| \geq 2$, the receivers will be able to reconstruct the two sequences. Consider the example in Figure 5.(b). Node B will be able to decode the first and second data bits in sequence D based on the signals $R_{D,B,1}$,

$R_{D,B,2}$, and $R_{D,B,3}$. When B sends the two bits to A, A will be able to separate the signals $R_{C,A,1}$ and $R_{C,A,2}$ from $R_{D,A,2}$ and $R_{D,A,3}$. Now A knows the first data bit in sequence C. When A sends the data bit back to B, B will be able to determine the vectors $R_{D,B,4}$ and $R_{D,B,5}$, and derive the third and fourth bits in sequence D. This procedure will continue until the two sequences are reconstructed.



(a)

(b)

Figure 5. Data bit recovery procedure.

After the two sequences are reconstructed, the nodes A and B can broadcast the decoding results. To prevent the attackers from impersonating A and B, they can calculate the hash values of the sequences and encrypt the hash results with the pair-wise keys with their neighbors. At the same time, node C and D will publish the seeds that they use to generate the two sequences. All nodes that receive the messages can easily verify their authenticity by applying the one way function to the seeds. They can then use the PRBG to regenerate the sequences and compare them to the decoding results of A and B. Previous research [14] has investigated the distribution of the bit error rate (BER) under different conditions. Therefore, we can choose a threshold to determine whether or not A and B successfully recover the data sequences.

4.4 Analysis

In this subsection, we investigate the detection capabilities of the proposed approach. Let us reexamine equation 2. If the nodes A and B are two Sybil identities attached to the same physical device, we must have $d_{BD} - d_{AD} = 0$ and $d_{BC} - d_{AC} = 0$. However, even if A and B are two different physical nodes and they are far apart, there is still a chance that $t_{diffB} - t_{diffA}$ has a very small value. For the two senders C and D, if the difference of their distances to the two nodes A and B is a constant, then C and D are on the same **hyperbola** that is determined by the two foci points A and B. In the following analysis, we will first calculate the expected value of $||d_{AC} - d_{BC}||$. We will then analyze the relationship between the detection accuracy and the number of rounds of the Sybil detections.

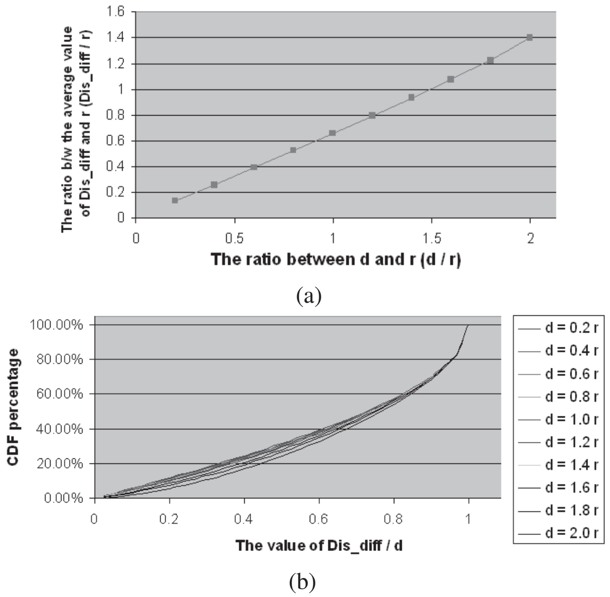
Figure 4.(a) illustrates the positions of A and B. We choose the center point between A and B as the origin and establish a Cartesian coordinate system. If we assume that the distance between A and B is d, their coordinates will be $(-\frac{1}{2}d, 0)$ and $(\frac{1}{2}d, 0)$ respectively. Now we focus on the area in Quadrant I from which the senders can be chosen. If the sender's coordinate is (x, y), we must have $0 \leq x \leq (\frac{1}{2}d + r)$ and $0 \leq y \leq \sqrt{r^2 - (x - \frac{1}{2}d)^2}$. The difference of the distances to the two nodes A and B can be represented as $Dis_{diff} = \sqrt{(x + \frac{1}{2}d)^2 + y^2} - \sqrt{(x - \frac{1}{2}d)^2 + y^2}$. Based on these equations, we can derive that the expected value of Dis_{diff} is:

$$\begin{aligned} & E[Dis_{diff}] \\ = & \frac{\int_{x=0}^{\frac{1}{2}d+r} \int_{y=0}^{\sqrt{r^2-(x-\frac{1}{2}d)^2}} Dis_{diff}\, dx\, dy}{area\ in\ Quadrant\ I} \\ = & \frac{\int_{x=0}^{\frac{1}{2}d+r} \int_{y=0}^{\sqrt{r^2-(x-\frac{1}{2}d)^2}} Dis_{diff}\, dx\, dy}{\frac{1}{4} \cdot (2\pi r^2 - 2r^2 arccos(\frac{d}{2r}) + d\sqrt{r^2 - (\frac{d}{2})^2})} \end{aligned} \tag{4}$$

From Equation 4 we can easily see that the expected value of Dis_{diff} is jointly determined by the values of d and r. We examine different ratios between d and r and run extensive simulations to study their impacts on $E[Dis_{diff}]$. Figure 6 shows the results.

Since we assume that the two nodes A and B share a common neighbor, we have $d \leq 2r$. For different ratios between d and r, we measure the average values of Dis_{diff} when the sender is randomly chosen from Quadrant I in Figure 4.(b). Since the other three quadrants are mirrors of Quadrant I, the average difference will have the same value. Figure 6.(a) shows the average values of Dis_{diff} for different d. We can see that the average difference increases almost linearly with the value of d and their ratio stays nearly constant. Figure 6.(b) shows the cumulative distribution function (CDF) of Dis_{diff} for different d values. We use the ratio between Dis_{diff} and d as the X-axis. We find that the CDF functions of the ten cases are very similar.

The results in Figure 6 provide a lot of useful information to us. First, since the average value of Dis_{diff} and d have a nearly-constant ratio, we can estimate the value of d by measuring the average difference of the distances. Since for different d values the CDF functions of Dis_{diff} are very similar, the estimation accuracy will not be impacted by the value of d. Second, when we look at the CDF functions close to the origin point, we find that Dis_{diff} has a very low probability to have a very small value. The following example will show that this property helps to reduce the false positive alarms.



(a)

(b)

Figure 6. Relationship between the average values of Dis_{diff} and d and r.

An Empirical Example

We assume that the radio communication range is $r = 250\ meters$. When d is uniformly distributed between 0 and $2r$, the probability that for a randomly chosen sender the difference between its distances to the two receivers is smaller than or equal to 3 $meters$ is roughly 1%. The reason that we choose 3 $meters$ as the magic number is as follows. We know that the speed of a radio wave is about 300,000 km/sec. If the sender's carrier frequency is 300MHz, its wavelength is 1 $meter$. If the value of Dis_{diff} is at least 3 $meters$, we will be able to embed at least two complete signals into the distance difference.

Now let us look at Figure 4.(a). We know that for any sender in Quadrant II or III, it is closer to A than B, and for any sender in Quadrant I or IV, it is closer to B than A. So if we choose one sender from each side of the Y-axis, we must have one of the Dis_{diff} to be greater than 0 while the other one smaller than 0. If at least one of the Dis_{diff} has an absolute value greater than or equal to 3 $meters$, the value of $||t_{diffA} - t_{diffB}||$ will be large enough to embed two complete MSK signals. Therefore, the two receivers can combine their information to recover the two sequences.

Based on the analysis, we can see that if we choose one sender from each side of the Y-axis, the probability that both senders have the Dis_{diff} smaller than 3 $meters$ is 1% × 1% = 0.01%. Therefore, if we randomly choose n pairs of senders from different sides of the Y-axis and conduct the Sybil detection, the probability that the distance between the two receivers is greater than 3 $meters$ but they cannot recover any of the sequences of the n tests will be $(0.01\%)^n$. This implies that our approach has a very low false positive rate when multiple rounds of detections are conducted.

To integrate this scheme into our proposed approach, we need to figure out a method to choose the senders from the different sides of the Y-axis. This problem can be solved by two schemes. First, we can choose from the nodes that are the neighbors of only one receiver. In this way, the distance between the selected sender and one receiver is smaller than r, and its distance to the other receiver is larger than r. For the nodes that can hear both of the receivers, we can choose the nodes that have the largest difference in the power level of the received signals.

We need a mechanism to distinguish the Sybil identities on the same physical device from multiple physical devices that are really close to each other. This problem can be solved by two schemes. First, we can increase the carrier frequency of the senders until the receivers can recover the sequences. In this way we can have a more accurate estimation of the distance between the receivers and determine whether or not they are the Sybil nodes. Second, when two nodes fail the Sybil detection, we will not immediately put them into the attacker list. On the contrary, we will put them on the suspicious list. Only when the same pair of identities fail multiple detections, we will claim them to be the Sybil nodes. This threshold-based method will effectively reduce false positive alarms since previous research has shown that even for the group based mobility model of ad hoc networks, the distances among the group members could still change drastically during a period of time.

5 Discussion

5.1 Why Depend on PNC to Measure Time Difference

The proposed approach measures the starting point of interference of two sequences to estimate the distance between the receivers. Here we have to answer one question: why do not we use the system clocks to measure the difference between the arriving time of two sequences? In that way, we can let two senders send out their packets alternatively and still allow the receivers to estimate their distance.

Two reasons make us use physical layer network coding to measure the time difference. First, previous research [21, 22] has shown that wireless nodes have a maximum clock drift rate at microsecond level (10^{-6} sec). At the same time, the deviations of clock drift rates are also at the microsecond level. If we assume the radio range r is 250 $meters$, the difference between the arriving time of a sequence at two receivers is restricted by 500 $m \div$ 300,000 $km/s \approx 1.67 \times 10^{-6} sec$. The measured duration and the clock drift are at the same level. Therefore, directly using the system clocks will introduce a large number of false alarms.

Second, since in Sybil detection the nodes under test could have lied to the senders, we cannot directly use the time differences reported by the receivers. On the contrary, based on whether or not the receivers can recover the colliding sequences, we can get a good estimation of the distance between them. This method prevents the attackers from impacting the detection results by providing false information.

5.2 Security of the Proposed Approach

In this subsection, we investigate the security of the proposed approach. Specifically, we focus on the scenarios when some of the senders are malicious. To compromise the proposed approach, the malicious senders either frame some legitimate nodes as Sybil nodes or help some Sybil nodes avoid the detection.

When only one sender is malicious and both of the receivers are legitimate nodes, it is very difficult for the attacker to frame a good node. The sender has broadcasted the hash result of the seed for its sequence before it is sent out. Since the radio signals will propagate in all directions, the other nodes can easily verify whether or not the transmitted sequence matches to the commitment. If the difference between the regenerated sequence and the received signals is large, we can cancel the detection result and choose another pair of senders. A similar analysis can be applied to the scenarios when both of the senders are malicious and both of the receivers are legitimate.

When one sender is malicious and both of the receivers are the Sybil nodes, the malicious sender will try to help the receivers avoid the detection. We first consider the scenarios when the malicious sender and the receivers are attached to the same physical device. In Section 4.1 we assume that the communication channel is half duplex and a node cannot transmit and receive signals at the same time. Therefore, if the malicious sender is transmitting a sequence, it will not be able to receive the signals from the legitimate sender. In this way, the Sybil nodes cannot recover both of the sequences and will fail the detection.

If the malicious sender and the Sybil receivers are not attached to the same physical device, the sender can provide its sequence to the receivers. In this way, the Sybil receivers will be able to recover the other sequence. To reduce the false negative alarms caused by this scenario, we can follow the analysis in Section 4.4 to conduct multiple rounds of detections with different pairs of senders. A similar analysis can be applied to the scenarios when both senders and both receivers are malicious.

A special case is when the two senders are attached to the same physical device. Since the two sequences are transmitted through the same antenna, all receivers will detect the same interference point. The receivers can then exchange the information and find out this situation. They will detect that the two senders are Sybil identities.

The malicious nodes can send out noises to disturb the Sybil detection procedures. Different from many anti-jamming scenarios, we cannot directly adopt the frequency hopping technique since the senders and the receivers do not have synchronized clocks and they cannot guarantee that the interfered signals always have the same carrier frequency. However, the senders and receivers can determine the carrier frequency of the signals through the secure communication channels among them before the detection. There are such transceivers on the market that allow the wireless nodes to adjust the carrier frequency within the range of 150MHz. For example, if we change the wavelength of the signal from 1 $meter$ to 0.9 $meter$, the carrier frequency will change for about 33.3 MHz. The change at this scale will have a good chance to avoid the jammer signals.

6 Related Work

Sybil Attack Detection

Sybil attack is a very harmful attack on distributed systems and wireless networks [6]. Newsome *et al.* have systematically classified these attacks into several types and analyzed their threats to wireless sensor networks [18].

Based on the detection mechanisms, we divide the previous approaches into three categories: identity based, location based, and signal-print based methods. Identity-based approaches usually mitigate the Sybil attacks by limiting the generation of valid node information, such as the pre-distributed secret keys [18]. A detection approach is proposed for vehicular ad hoc networks through possible explanations for collected data of each node [8].

Location-based approaches utilize the fact that each node can only be at one position at a specific moment. Localization algorithms, such as SeRLoc [17], are proposed to allow sensors to determine their locations under known attacks including Sybil attack. The geometric properties of message transmission delay are also explored to reduce the impacts of Sybil attacks [1]. In [19], every node will sign its ID and position and send this information to several random directions. The different positions signed by multiple replications of the same node have a good chance to be detected.

In the signal-print based detection mechanisms, the investigators try to collect the properties of the radio signals and detect the false claims of the node identities. In [7], multiple access points measure the signal strength from a node to form the signalprint and use it to detect Sybil nodes. The similar idea is adopted in [4]. The approach in [24] integrates a series of position claims and witness reports in VANETs to detect Sybil nodes. In [3], the radio signal transient shape at the start of a packet is used to identify a physical node and detect Sybils.

Physical Layer Network Coding

Physical layer network coding (PNC) uses the additive nature of the electromagnetic waves to serve as the coding procedure. The PNC technique under QPSK modulation is studied in [26]. The researchers investigate the general modulation-demodulation principles and analyze the performance penalty of different factors. In [14], the authors try to decode the interfered signals under MSK modulation. The mechanism can recover the colliding sequences under phase shift and the lack of synchronization. In [23], the authors compare the amplify-and-forward and decode-and-forward techniques. Zhang *et al.* investigate the decoding techniques of PNC over finite and infinite fields in [27]. In [20], the authors propose to dynamically adjust the coefficients to increase the 'distances' among different codes. Investigators also proposed to adopt Tomlinson-Harashima precoding to improve the data recovery accuracy [10].

7 Conclusions

In this paper we propose a Sybil detection mechanism for wireless networks based on physical layer network coding. The analysis shows that the difference between the starting points of interference at two receivers is restricted by the distance between them. Our approach challenges the receivers to separate the colliding sequences to determine whether or not they are attached to the same physical device. To turn this mechanism into a practical approach, we study various problems in the network layer and the physical layer. We also design mechanisms to reduce the false alarm rate and analyze the safety of the proposed approach.

Immediate extensions to our approach consist of the following aspects. First, we will implement the proposed approach in software defined radio and test it in real network environments. Second, we will improve the efficiency of the detection mechanism by testing multiple pairs of identities with the same pair of senders. Finally, we will investigate using physical layer network coding to detect other stealth attacks on wireless networks.

References

[1] R. A. Bazzi and G. Konjevod. On the establishment of distinct identities in overlay networks. In *Proceedings of ACM PODC*, pages 312–320, 2005.

[2] D. Charles, K. Jain, and K. Lauter. Signatures for network coding. *Int. J. Inf. Coding Theory*, 1(1):3–14, 2009.

[3] B. Danev and S. Capkun. Transient-based identification of wireless sensor nodes. In *Proc. of IPSN*, pages 25–36, 2009.

[4] M. Demirbas and Y. Song. An rssi-based scheme for sybil attack detection in wireless sensor networks. In *Proceedings of WoWMoM*, pages 564–570, 2006.

[5] J. Dong, R. Curtmola, and C. Nita-Rotaru. Practical defenses against pollution attacks in intra-flow network coding for mesh networks. In *ACM WiSec*, pages 111–122, 2009.

[6] J. R. Douceur. The sybil attack. In *the First International Workshop on Peer-to-Peer Systems*, pages 251–260, 2002.

[7] D. B. Faria and D. R. Cheriton. Detecting identity-based attacks in wireless networks using signalprints. In *Proceedings of ACM WiSe*, pages 43–52, 2006.

[8] P. Golle, D. Greene, and J. Staddon. Detecting and correcting malicious data in vanets. In *Proc. ACM international workshop on Vehicular ad hoc networks*, pages 29–37, 2004.

[9] J. Hamkins. An analytic technique to separate cochannel FM signals. *IEEE Tran. on Comm.*, 48(11):2980–2989, 2000.

[10] Y. Hao, D. Goeckel, Z. Ding, D. Towsley, and K. K. Leung. Achievable rates for network coding on the exchange channel. In *IEEE Milcom*, pages 1–7, 2007.

[11] L. Hong and K. Ho. Classification of bpsk and qpsk signals using an antenna array. *Circuits, Systems, and Signal Processing*, 24(4):343–361, 2005.

[12] R. Jenkins. Isaac. In *Third International Workshop on Fast Software Encryption*, pages 41–49, 1996.

[13] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293–315, 2003.

[14] S. Katti, S. Gollakota, and D. Katabi. Embracing wireless interference: analog network coding. In *ACM SigComm*, pages 397–408, 2007.

[15] M. Larrea, C. Martin, and J. Astrain. Fault-tolerant aggregator election & data aggregation in wireless sensor networks. *Int. J. Commun. Netw. Distrib. Syst.*, 3(2):93–115, 2009.

[16] R. Latif and M. Hussain. Hardware-based random number generation in wireless sensor networks. In *Int. Conf. on Advances in Infor. Secu. & Assurance*, pages 732–740, 2009.

[17] L. Lazos and R. Poovendran. Serloc: Robust localization for wireless sensor networks. *ACM Trans. Sen. Netw.*, 1(1):73–100, 2005.

[18] J. Newsome, R. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: Analysis and defenses. In *Proceedings of IEEE IPSN*, pages 259–268, 2004.

[19] B. Parno, A. Perrig, and V. Gligor. Distributed detection of node replication attacks in sensor networks. In *IEEE Symposium on Security and Privacy*, pages 49–63, 2005.

[20] W. Pu, C. Luo, B. Jiao, and F. Wu. Natural network coding in multi-hop wireless networks. In *IEEE ICC*, pages 2388–2392, 2008.

[21] K. Römer. Time synchronization in ad hoc networks. In *ACM MOBIHOC*, pages 173–182, 2001.

[22] H. Song, S. Zhu, and G. Cao. Attack-resilient time synchronization for wireless sensor networks. In *Proc. of IEEE MASS*, pages 765–772, 2005.

[23] V. Stankovic, L. Fagoonee, A. Moinian, and S. Cheng. Wireless full-duplex communications based on network coding. In *Proc. of Annual Allerton Conference*, 2007.

[24] B. Xiao, B. Yu, and C. Gao. Detection and localization of sybil nodes in vanets. In *Workshop on Dependability in wireless ad hoc networks and sensor networks*, pages 1–8, 2006.

[25] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway. A survey of key management schemes in wireless sensor networks. *Comput. Commun.*, 30:2314–2341, 2007.

[26] S. Zhang, S. C. Liew, and P. P. Lam. Physical-layer network coding. In *ACM MobiCom*, pages 358–365, 2006.

[27] S. Zhang, S. C. Liew, and L. Lu. Physical layer network coding schemes over finite and infinite fields. In *IEEE GLOBECOM*, pages 1–6, 2008.