Interactive Wormhole Detection in Large Scale Wireless Networks

Weichao Wang*
University of Kansas

Aidong Lu†
University of North Carolina at Charlotte

Abstract

Wormhole attacks in wireless networks can severely deteriorate the network performance and compromise the security through spoiling the routing protocols and weakening the security enhancements. This paper develops an approach, Interactive Visualization of Wormholes (IVoW), to monitor and detect such attacks in large scale wireless networks in real time. We characterize the topology features of a network under wormhole attacks through the node position changes and visualize the information at dynamically adjusted scales. We integrate an automatic detection algorithm with appropriate user interactions to handle complicated scenarios that include a large number of moving nodes and multiple wormhole attackers. Various visual forms have been adopted to assist the understanding and analysis of the reconstructed network topology and improve the detection accuracy. Extended simulation has demonstrated that the proposed approach can effectively locate the fake neighbor connections without introducing many false alarms. IVoW does not require the wireless nodes to be equipped with any special hardware, thus avoiding any additional cost. The proposed approach demonstrates that interactive visualization can be successfully combined with network security mechanisms to greatly improve the intrusion detection capabilities.

Keywords: Interactive Detection, Wormhole Attacks, Visualization on Network Security, Wireless Networks, Topology Visualization

Index Terms: C.2.0 [Computer-Communication Networks]: General—Security and protection; H.5.2 [Information Systems]: Information Interfaces and Presentation—User interfaces;

1 Introduction

Intrusion Detection System (IDS) in wireless networks [42] has played an important role in network security by providing an additional level of protection to the network topology and applications beyond the traditional security mechanisms such as encryption and authentication. It detects the attacks and isolates the malicious nodes by matching the patterns of known intrusions or discovering the anomalies [5, 12, 13, 16] in the network activities. Its application environments cover almost all wireless networking scenarios such as ad hoc networks [42], wireless LANs [8], and sensor networks [5, 12]. A good survey can be found in [43].

With the fast increases in the scale, available bandwidth, and protocol diversity in wireless networks, the intrusion detection mechanisms must discover the patterns of the known attacks or the anomalies caused by the unknown intrusions from a continuous, multivariate data flow in real time. Therefore, effective representation of the data is essential for users to understand the hidden information and for IDS to preserve the detection accuracy and efficiency. Visualization techniques, which enable the derivation of insights from massive and dynamic data, provide a powerful tool to satisfy these requirements. In addition to information representation, the visualization techniques also provide highly interactive interfaces to accelerate visual analytics. There has been pioneer research on visualization for computer security. The adopted methods include multiresolution of the data details [2], visual correlation among different parts of the data [14, 35], and time-varying patterns [15, 28].

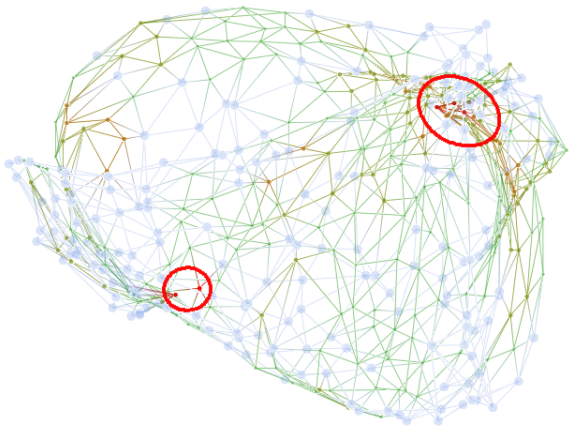


Figure 1: Visualization for wormhole detection. The two red circles indicate suspicious regions. We have combined interactive visualization into the wormhole monitoring, representation, and detection processes to analyze the potential wormhole attack regions in a large scale wireless network.

Most of the existing IDS approaches depend on the measurements of some network parameters (e.g. packet delivery ratio, end to end delay) to identify the attacks. Therefore, the detection capabilities will be restricted by the acquiring delay and accuracy of these measurements. Since many attacks on wireless networks target at the network topology (e.g. neighbor discovery and routing), new approaches are expected to detect such attacks based on more direct "evidences".

In this paper, we explore the development of approaches that can detect attacks on wireless networks directly based on their impacts on the network topology. To demonstrate the proposed method, we choose a specific attack, wormhole attack [10, 18, 30], as the research problem. In a wormhole attack, the malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate fake neighbor connections, thus spoiling the routing protocols and weakening some security enhancements. The impacts of wormhole attacks on the reconstructed topology of a 2D wireless network are illustrated in Figure 1. The simulation results in [17, 21] have shown that when there are more than two wormholes in the network, more than 50% of the data packets will be attracted to the fake neighbor connections and get discarded.

A preliminary approach, MDS-VoW, to wormhole detection using visualization techniques was proposed by Wang and Bhargava in [39]. The approach uses multidimensional scaling (MDS) to reconstruct the topology of a wireless network and locates the wormholes and fake neighbor connections by identifying the distortions in the reconstruction result. Although effective as a proof-of-concept prototype, MDS-VoW has several deficiencies when it is

*e-mail: weichaow@eecs.ku.edu
†e-mail: alu1@uncc.edu

IEEE Symposium on Visual Analytics Science and Technology 2006
October 31 - November 2, Baltimore, MD, USA
1-4244-0592-0/06/$20.00 © 2006 IEEE

applied to real wireless environments. First, the authors only evaluate MDS-VoW in a network containing a few hundreds of nodes. Its performance and accuracy in a larger scale environment (e.g. thousands of nodes) remain undetermined. Second, MDS-VoW assumes that all nodes are static. Therefore, its detection capability in mobile wireless networks has not been investigated. Finally, the experimental results focus on the scenarios when only one wormhole exists in the network while the research in [17, 21] has demonstrated that multiple wormholes put more severe impacts on the network performance.

The method introduced in this paper, Interactive Visualization of Wormhole (IVoW), provides a visual approach through which the users can detect multiple wormholes in a large scale, dynamic wireless network. It first reconstructs the network topology based on the measured distances among neighboring nodes. To reduce the network reconstruction overhead caused by node movement, incremental multidimensional scaling [4, 40] is adopted. Adaptable representation of the reconstruction result with attack-dependent level-of-detail will assist the users to identify the "suspicious areas" under wormhole attack. Multiple rounds of detection with false-alarm reduction methods will help improve the detection accuracy when multiple wormholes coexist in the system.

As we will demonstrate, the proposed visualization approach can effectively identify the fake neighbor connections. The contributions of the research can be summarized as follows: (1) We characterize the topology features of the network under wormhole attacks and present a real time visualization approach to effectively visualize and monitor topology changes. (2) We integrate interactive visualization into multiple steps of intrusion detection procedures, including monitoring, detection, and representation. This approach significantly accelerates the detection procedure by taking advantage of the visual analysis abilities of human expertise. (3) IVoW directly uses the topology information to detect attacks on wireless networks, thus avoiding the overhead and inaccuracy caused by the network measurements. (4) The proposed approach does not depend on any special hardware, thus avoiding any additional deployment cost.

The remainder of the paper is organized as follows: Section 2 provides the background of wireless networking, how wormhole attacks are conducted, and the research challenges. Section 3 reviews the previous research efforts that contribute to our approach. In section 4, an overview of IVoW is described. Three principal components of the proposed mechanism, efficient network reconstruction, adaptive visualization, and interactive wormhole detection, are described in detail in section 5, 6, and 7, respectively. Section 8 presents the experimental results. Finally, section 9 concludes the paper and discusses future extensions.

2 Background

In a wireless network, the nodes communicate with each other through radio transmissions. A simplified model to describe the connectivity among wireless nodes is the unit disk graph [9]: a pair of nodes u and v can directly communicate to each other if the Euclidean distance between them is shorter than r, where r is defined as the communication range. Since the neighbor relations among wireless nodes may change because of various reasons such as node movement, device malfunction, battery exhaustion, and unreliable transmission medium, a node must be able to detect its active neighbors dynamically. A widely adopted approach is to let the mobile node periodically broadcast a short message containing its identity (called 'beacon' packet) and the neighbors receiving this packet will add the node into the neighbor lists. The awareness of localized network topology and route choices are usually based on the correct establishment of and updates to the neighbor list.

The features of wireless communication enable the malicious nodes to conduct wormhole attacks. As shown in Figure 2, when a

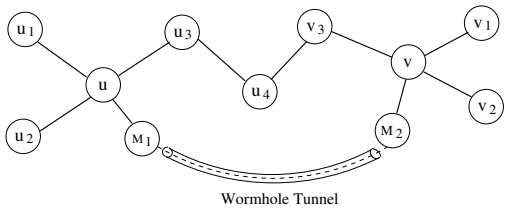


Figure 2: Wormhole attack between a pair of nodes u and v.

legitimate node u in the network sends out a beacon, the malicious node $M1$ can use its antenna to eavesdrop the packet, and tunnel it through a dedicated long range channel to its colluder $M2$. When $M2$ retransmits the beacon, another legitimate node v will receive this packet and add u into its neighbor list. Fake neighbor connections are generated through wormholes. Later when data packets need to go through the wormhole, the malicious nodes may choose to discard them. Therefore, a wormhole fabricates a fake connection between u and v that is under the control of the attackers.

Wormhole attacks are difficult to detect since the malicious nodes only eavesdrop and retransmit the beacons. The adoption of a stronger encryption or authentication method will not solve the problem since the attackers act as the clone of the legitimate nodes. At the same time, the fake "short" path between u and v may attract many data packets from their neighborhood, thus deteriorating the delivery ratio and network performance. Therefore, new approaches must be developed to stop these attacks.

3 Related Work

3.1 MDS and Its Applications in Wireless Networks

Multi-dimensional scaling was originally a technique developed in the behavioral and social science for studying the relationship among objects. The inputs to MDS are the measures of the difference or similarity between object pairs [11]. The output of MDS is a layout of the objects in a low-dimensional space. In this paper, the input is the distance matrix between the wireless nodes. The mechanism can reconstruct the network and calculate a virtual position for every node. We adopt the classical metric MDS in the proposed mechanism since the distances are measured in a Euclidean space. More details of MDS can be found in [11] and [38].

MDS has been adopted to solve the localization and positioning problems in wireless networks. In [37], a solution using classical metric MDS is proposed to achieve localization from mere connectivity information. The algorithm is more robust to measurement errors and requires fewer anchor nodes than previous approaches. A distributed mechanism for sensor positioning using MDS has been presented in [19]. It develops a multi-variate optimization-based iterative algorithm to calculate the positions of the sensors. Another approach [6] to sensor network localization adopts semi-definite programming relaxation to minimize the errors for fitting the distance measurements.

3.2 Wormhole Detection in Wireless Networks

Wormhole attacks on mobile wireless networks were independently discovered in [10], [18], and [30]. Below we describe several approaches that have been developed to defend against such attacks.

If the wireless nodes are equipped with directional antennas [17], a pair of nodes can examine the directions of the received signals from each other and a shared third node to confirm the neighbor relation. In [18], extra information is added into a packet to restrict its transmission distance. In geographical leashes, the location information and loosely synchronized clocks together verify the neighbor relation. In temporal leashes, the packet transmission distance is calculated based on the propagation delay and signal transmission speed. In addition to the approach using scientific visualization

[39], a wormhole prevention mechanism based on graph theory is proposed in [31]. Using the geometric random graphs induced by the communication range constraint of the nodes, the researchers present the necessary and sufficient conditions for detecting and defending against wormholes. They also present a defense mechanism based on local broadcast keys.

3.3 Distance Estimation between Wireless Nodes

Since MDS uses the measured distances among wireless nodes that can hear each other as inputs to reconstruct the network, we shortly introduce several distance estimation methods. The existing solutions include using received signal strength [22], Time-of-Arrival and Time Difference of Arrival [32, 36], and triangulation [29].

One point that we have to clarify is that the measured distances cannot be directly used to prevent wormholes. For example, if the received signal strength is used to estimate the distance, the receiver cannot distinguish the resent packet from the real beacon. Similarly, if the nodes use the propagation delay of acoustic signals to measure the distance, the malicious nodes can easily hide the tunneling delay if radio transmission is used in the wormhole.

3.4 Visualization for Computer Security

With the fast development of computer security mechanisms, the scale and complexity of the security data put ever-increasing challenges to the representation and understanding of the information. Visualization techniques have been adopted by the researchers to bridge the gap. For example, it is usually difficult for the system administrators to read a text-based log file recording the traffic patterns and anomalies that happened in the past twenty-four hours. The researchers have developed mechanisms that can provide an overview of the traffic patterns of thousands of hosts [3]. The latest approaches provide a more scalable representation capability that can cover multiple class-B IP address ranges and the intrusion alarms in them [2, 20, 23].

Network scans are probably the most common and versatile intrusions. Researchers have developed a visualization methodology to characterize the scans based on their patterns and wavelet scalograms [28]. Another approach uses IP address and port number histographs to detect and analyze the scan attacks [35]. VisFlowConnect-IP [41] achieves detection of anomalous traffic through a link-based network flow visualization tool.

Under many conditions, the security data acquired from different methods must be investigated jointly to improve the detection accuracy and efficiency. The research efforts in [14] provide a visual correlation between the host processes and network traffic. In both [28] and [35], the approaches can identify the similarity among different scan attacks or NetFlow signatures.

While many visualization approaches to network security require large amounts of finely detailed, high-dimensional data, several mechanisms focus on the big picture. For example, the mechanism in [25] takes very coarsely detailed data to help uncover interesting security events. The mechanism in [33] overcomes the scalability issues inherent in visualizing massive networks through sampling. In [15], low level textual data are provided in the context of a high-level, aggregated graphical display. Disparate logs are also visualized to show the correlation of network alerts based on what, when, and where [24].

4 Overview

An overview of IVoW is illustrated in Figure 3. After deployment, a wireless node will estimate the distances to the other nodes that it can hear and send the measurement results to IVoW. Some fake neighbor connections through wormholes may be included. Encryption and authentication methods can be adopted to protect the integrity of the information and prevent impersonation.

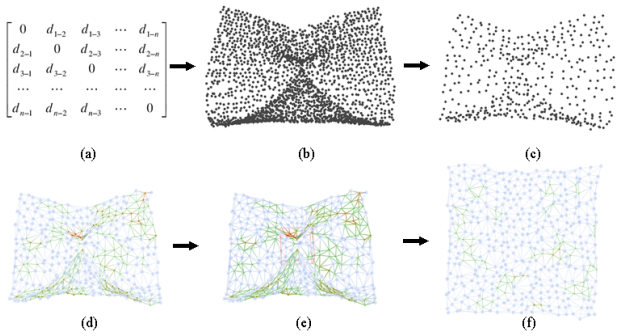


Figure 3: System overview: A distance matrix (a) acquired from a large scale wireless network is used to reconstruct the 3D positions of the nodes using incremental MDS method (b), and modified through our feature point sampling (c), feature line selection (d), primitive assignments (d), and interactive detection (e) to defend against the wormhole attacks (f).

The proposed approach will use the measurements to build the distance matrix and reconstruct the network topology using incremental MDS. A normalized *wormhole indicator* value will be calculated for every node to identify those "suspicious areas" under wormhole attack (section 5).

When the scale of the network and number of nodes are considered, the user may be overwhelmed by the information in the visualization. We integrate the feature element selection and attribute assignment methods to develop an adaptive visualization method. Only a part of carefully chosen nodes and their neighbor relations are illustrated while the network topology is preserved so that the suspicious areas under attack can be easily located (section 6).

The proposed mechanism takes advantage of the expertise of the users to accelerate the wormhole detection procedure and improve the accuracy. A set of interaction interfaces are designed to allow the users to identify the suspicious areas and activate more complicated detection methods. Therefore, interactive visualization not only helps improve information understanding but also assists problem solving through visual analysis (section 7).

5 Efficient Network Reconstruction

5.1 Fast Network Reconstruction

The proposed mechanism uses MDS to reconstruct the network layout. First, every pair of nodes that can hear each other will estimate the distance between them and report it to IVoW. The mechanism will calculate the average value and put the result at the suitable positions in the distance matrix. After that, a classical shortest-path algorithm, such as Dijkstra's algorithm, can be used to calculate the shortest distance between every node pair. Using the distance matrix, MDS can rebuild the network and a virtual position for every node will be generated.

The computation complexity of traditional MDS is n^3 when there are n nodes in the network. If IVoW reconstructs the whole network from scratch after every neighbor relation change, the computation overhead will become overwhelming when n is large, thus impacting the scalability and efficiency of the proposed mechanism. To achieve efficient network reconstruction, we propose to adopt the incremental MDS proposed in [4, 7, 26, 40].

The fast network reconstruction method is based on [7, 26], whose computation complexity is n^2. Since the distances among wireless nodes seldom experience radical changes, the reconstruction result of the previous round is a good initial layout of the nodes. Single scaling will then be executed for the nodes whose neighbor relations change. The final step runs several MDS iterations upon the entire node set to refine their positions. An example of incremental MDS is illustrated in Figure 4.

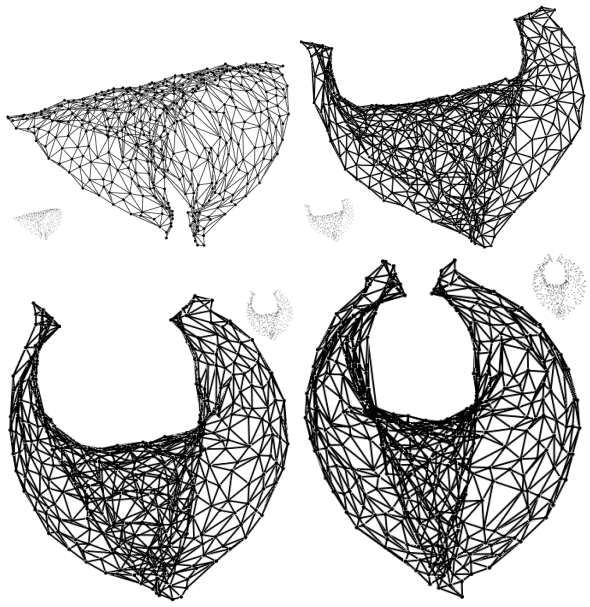


Figure 4: Example of incremental MDS: a pair of nodes slowly move to each other, thus leading to changes in network topology.

5.2 Estimating Wormhole Indicator Value for Wireless Nodes

The analysis in [39] has shown that the wormholes can be viewed as an extra force that will lead to the distortions: the distances and angles among the neighboring nodes in the reconstructed network will be very different from the values in the real layout. Subsequent research [21] has shown that the distortions in angles can be used to locate the fake neighbor connections.

For every angle formed by three neighboring nodes u_1, u_2, and v with v as the vertex, two values can be determined: (1) $\theta_{M-u_1vu_2}$, which can be calculated based on the measured distances among them; (2) $\theta_{R-u_1vu_2}$, which can be acquired from the reconstructed network. The distortions in angles can be measured by the difference between these two values.

We define a new variable *wormhole indicator* (*wi*) for every node v based on the differences in angles:

$$wormhole\ indicator(v) = \frac{\sum \theta_{diff-u_ivu_j}}{q(q-1)}; (i,j = 1 \cdots q, i \neq j)$$

$$\theta_{diff-u_ivu_j} = \begin{cases} 0, & if\ ||\theta_{M-u_ivu_j} - \theta_{R-u_ivu_j}|| \leq \theta_{th}; \\ 1, & if\ ||\theta_{M-u_ivu_j} - \theta_{R-u_ivu_j}|| > \theta_{th}. \end{cases} \quad (1)$$

where v, u_i and u_j are neighbors, and q is the degree of connectivity of v. From the definition we find that *wormhole indicator* is a normalized variable with the value range [0,1].

θ_{th} in equation 1 represents the threshold that is used to distinguish the changes in angles caused by the distance measurement inaccuracy from the distortions caused by the wormholes. We adopt a format of $c \cdot \frac{d_{err}}{0.5r}$ for θ_{th}, in which d_{err} represents the distance measurement inaccuracy, r is the communication range, and c is a constant. When the distance estimation errors are not large, $\frac{d_{err}}{0.5r}$ roughly describes the change in angles caused by the inaccuracy. Our simulation shows that a value not smaller than 4 should be assigned to c to preserve the detection accuracy.

While the *wormhole indicator* values measure the impacts of the wormholes within a single network reconstruction, we also take the time factor into consideration by monitoring the distance changes among the node pairs in different reconstructions. If a pair of nodes were far away from each other in the previous reconstruction and suddenly become neighbors, the link between them will be examined carefully to prevent wormholes.

6 Adaptive Network Visualization

With the reconstructed topology and initial wormhole indicator values, we can visualize a wireless network to monitor and detect wormhole attacks. In this section, we describe our feature element selection and attribute assignment methods to effectively visualize a large scale wireless network.

Intuitively, we use points to represent wireless nodes, lines to strengthen the network topology, and rendering settings to reveal the intrusion detection information. This point-and-line based visualization method is developed to satisfy the real-time rendering requirement and to provide an effective framework for illustrating network topology and security information.

Choosing a suitable resolution is one major problem for visualizing a large scale network topology. It is difficult to observe any abnormality when there are a large number of points and lines overlapping on the screen. Multiple rendering resolutions can be used to alleviate this problem. However, it is not practical for users to adjust the suitable resolution manually, since the interaction would be too tedious for a real-time network monitoring task. Therefore, we propose to develop a self-adapted visualization method to automatically select sample points and lines.

6.1 Feature Points Selection

We select feature points based on their wormhole indicator values and location information to reduce the overlapping issue and preserve major topology features. Next, we discuss our ideal point distance measurement based on wormhole indicator values, the location information calculation, and our feature point selection procedure.

Since the wormhole indicator is one significant feature for monitoring and detecting network attacks, we use this value to adjust the ideal point distance for each node. We draw all the points whose indicator values are larger than the threshold δ_{wi}, which is defined in the previous work [39] and can be adjusted by users, and keep a large point distance D_l for points with low indicator values. This results in a low point density on smoother surfaces and more detailed changes for abnormal regions. Practically, we use 5% of the rendering space width as D_l.

$$dis(v) = \begin{cases} D_l \times (1 - \frac{wi(v)}{\delta_{wi}}), if\ wi(v) < \delta_{wi} \\ 0, if\ wi(v) \geq \delta_{wi} \end{cases} \quad (2)$$

We also include the location information in the selection procedure for preserving the network topology shape, including a boundary indicator and a surface roughness measurement. We adopt the approach proposed by Rao et al. [34] to identify the boundary nodes of the network and assign their boundary indicators to '1'. We intend to select these points since they are important to represent the shape of the entire network. For each node v in the reconstructed topology, its normal direction $\overrightarrow{v}$ can be calculated using the best fitted plane within a local region [39]. If the set of neighbors of v is represented as N_v, the surface roughness value can be calculated using the average normal direction changes, as $rough(v) = \sum_{u \in N_v} \frac{(1 - \overrightarrow{v} \cdot \overrightarrow{u})}{2q}$, where q is the number of neighbors in N_v. We intend to keep higher point density for rough surfaces, since they are more likely to contain abnormal information.

The feature value of a node is calculated as the weighted sum of the three factors: wormhole indicator, boundary indicator, and roughness value. We keep the sum of the weights $w_{wi} + w_b + w_r = 1$ for saving the normalization process and we use 0.5, 0.3, 0.2 for w_{wi}, w_b and w_r respectively, favoring the wormhole indicator values.

$$Feature(v) = w_{wi} \cdot wi(v) + w_b \cdot bound(v) + w_r \cdot rough(v) \quad (3)$$

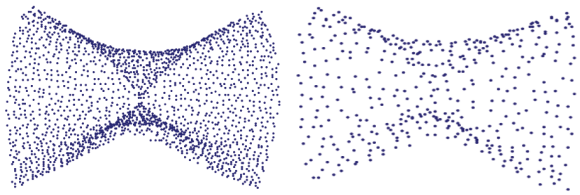


Figure 5: Point density is reduced to a smaller scale for clarity through feature point selection.

The procedure to select feature points can be viewed as choosing a point subset that approximates the ideal point distances and achieves the maximum feature sum value. Since a greedy algorithm produces very similar results in representing the topology information, we adopt a fast algorithm by using the following selecting and updating phases.

A node with the maximum feature value is first selected through traversing the point list and added to the feature point set. Then, we update feature values of all the local points by a factor according to the distance d to the selected point using $\overline{Feature}(v) = f(v) \times Feature(v)$, where

$$f(v) = \begin{cases} 1, if\ d \geq dis(v) \\ (\frac{d}{dis(v)})^2, if\ d < dis(v) \end{cases} \quad (4)$$

We repeat this process until all the remaining points have been modified at least by a factor of $f(\frac{dis(v)}{2})$. This ensures the completeness of the network topology.

We can further accelerate this selection process by selecting multiple points at each time. For the points whose feature values are larger than $\delta_{wi}/2$, we randomly select multiple points into the feature set. We can also directly use the point distance from the original distance matrix in section 5 to accelerate this process. As shown in Figure 5, the point density is reduced to a smaller scale for clarity.

6.2 Feature Lines Selection

We use feature lines to further strengthen the topology information by connecting selected feature point pairs. Since a wireless network usually forms a highly connected topology, we cannot illustrate every neighbor pair because of the intersecting issue. Instead, we select a small number of lines that can be used to enhance the major topology features.

To generate a succint line drawing, we summarize three criteria for selecting feature lines.

- Intersection: Any two lines should not intersect on a smooth surface.
- Connectivity: At least one line is connected to each feature point.
- Cell areas: Small areas composed by the surrounding lines should be avoided for better representation.

Under these three criteria, we choose feature lines by using Delaunay triangulation algorithm [27]. Our first two criteria are satisfied automatically and the third criterion can be approximated from the Delaunay triangulation, since it maximizes the minimum angle of all the triangles. The result of 3D Delaunay triangulation method is used to select the feature lines between the corresponding point pairs. As shown in Figure 6, the selected feature lines enhance the main surface information in the network topology.

6.3 Attributes Assignment

To effectively visualize the network features, we assign the rendering attributes, including size, color, and transparency, for the selected feature points and lines according to the wireless node properties.

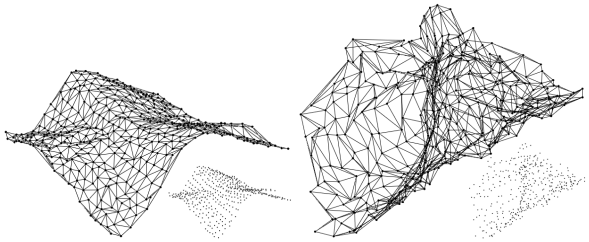


Figure 6: The automatically selected feature lines can significantly enhance the visualized network topology.

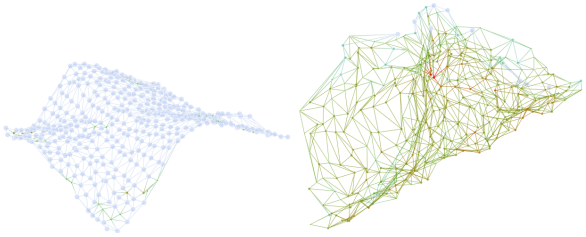


Figure 7: The primitive attributes are adjusted for effectively visualizing the node properties. Red color suggests potential attack regions.

The point size is adjusted to represent the local point density. Since the feature point selection process changes the original point density, we use the ideal feature point distance to approximate real point density, which is decided from the wormhole indicator value. Here max_{size} represents the maximum point size in the rendering and we use 10 in our system.

$$size(v) = \begin{cases} 1 + max_{size} \times (1 - \frac{wi(v)}{\delta_{wi}}), if\ wi(v) < \delta_{wi} \\ 1, if\ wi(v) \geq \delta_{wi} \end{cases} \quad (5)$$

Therefore, larger points represent smoother surfaces in the visualization; while smaller points indicate more abrupt changes in the topology.

The point color is assigned from blue to red to reveal the wormhole indicator value from low to high.

$$color(v) = wi(v) * C_{red} + (1 - wi(v)) * C_{blue} \quad (6)$$

The point transparency is also calculated from its indicator as $wi(v)^{P_t}$, since the users are most interested in the potential attacked regions. P_t is set as 1.5 in our implementation. The transparent points also allow the users to see through a complex topology, as shown in Figure 7.

The line attributes are simply adjusted according to the attributes of the neighbor points, since we mainly use their positions to suggest the network topology. Their color and transparency are interpolated linearly between the two connecting points. We use the same thin line width to render all the lines for the least overlapping.

7 Interactive Wormhole Detection

We propose to integrate interactive visualization with intrusion detection algorithms to accelerate the detection process and improve the algorithm accuracy. Our previous work achieves a high success ratio at detecting wormhole attacks in an experimental environment. Problems occur when we apply the mechanism to networks at a larger scale. As shown in Figure 11 (a), the detection accuracy can decrease drastically with an increasing environment complexity caused by multiple attackers. Therefore, we develop an interactive visualization system to handle these large, complex wireless environments. The following describes our interface design and an interactive detection procedure for wormhole detections.

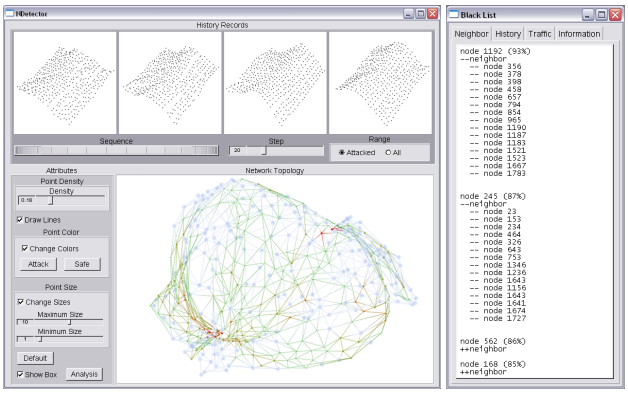


Figure 8: Our wormhole detection interface. The left top locates the history window, left bottom includes parameter window and topology interaction window, and the right lists the identities and information of the potential attackers.

7.1 Interface Design

We combine the tasks of monitoring and detecting wormhole attacks into one unique system interface. Our basic idea is to visualize the network topology and potential attacks in a manner that is convenient for users to associate all the relevant information.

As shown in Figure 8, our interface is composed of three windows: topology window (bottom middle), target window (right), and history window (top left). The topology window visualizes the current network topology, where users can interact with the topology with several routine tasks, including zooming, rotating, and selecting region-of-interest. The target window lists the nodes whose wormhole indicator values are larger than the threshold δ_{wi}. We also collect the information of each node for analysis, such as neighbor relationships, traffic history, etc. On the top left, we arrange a history window that illustrates the network topologies of the previous several time steps for observing the topology changes.

7.2 Interactive Detection

To handle a large, complex network environment, we need to integrate user interaction with our wormhole detection and visualization methods. Our approach is to use the user inputs to guide the automatic detection procedure for further analysis. This allows the users to achieve a high success ratio with only a limited amount of simple interactions.

During the detection, the users are only required to draw a cube roughly around their region-of-interest. This cube is located by the left, back, top corner and the right, front, bottom corner. These two 3D points can be specified through the combined inputs of mouse movement and hot keys. Generally, only several operations are required to achieve a satisfying detection result.

Once the region-of-interest is located, the system will automatically process the interaction information, provide detailed analysis results, and use this information to update the network topology for further detection. Let us define the nodes within the region-of-interest as candidate nodes. Since these user selected candidate nodes may indicate the existence of wormholes, we propose a progressive procedure to analyze them automatically.

First, we reconstruct the network topology without all the candidate nodes and calculate the stress value s_1 of MDS.

Second, we sort all the candidate nodes in a decreasing order based on their numbers of neighbors. A node with the maximum neighbor number will be added back into the network and we use incremental MDS to fast reconstruct a new topology, which produces the stress value s_2.

Third, the change between the current and previous topologies is measured by using their stress values as $\frac{s_2-s_1}{s_1}$. If the change is below a threshold (10%), the candidate point is viewed as a "good" node, will be added back to the network, and we go back to step 2. Otherwise, at least one of its neighbor connections belongs to a wormhole. We continue to step 4.

Fourth, since all the neighbor connections of the candidate point are independent, we reconstruct the network topology using incremental MDS by adding each neighbor line back and compare the topology change from the previous step. For each line causing the stress value to increase beyond the threshold, a warning packet will be sent to both nodes connected by this line to indicate that this is a false connection and should be removed immediately.

Figure 9 illustrates our detection procedure, which successfully analyzes and identifies all the attacked regions in a distorted network topology. Only several simple user interactions are involved in handling complex wormhole attacks.

8 Experimental Results

The detection accuracy of the proposed mechanism is evaluated through simulation. We use the network simulator *ns*2 [1], which is widely adopted by the wireless networking investigators. To enable the comparison between IVoW and MDS-VoW and demonstrate the improvements, we adopt a relatively small scale wireless network. We assume that 600 nodes are randomly and roughly uniformly deployed in a square area with the size of $2km \times 2km$. The communication range among wireless nodes is $r = 180m$ and the average degree of connectivity is 10.35.

The same network topology and wormhole attack scenarios are provided to both mechanisms. The detection accuracy is measured by the false alarm rate. Two parameters are of special interest: the fraction of detected wormholes, and the number of real neighbor connections that are wrongly labeled as wormholes. Every data point in the following figures represents the average value over 15 trials under different network setups.

8.1 Robustness against Distance Estimation Errors

Since the network reconstruction is conducted based on the measured distances among wireless nodes, the measurement accuracy has a direct impact on the detection capability. In our simulation, we model the distance estimation errors as uniform noises. If the accurate distance between two nodes is d $(d \leq r)$ and the error rate is e_m, a random value drawn from the uniform distribution $[d \times (1-e_m),\ min(r,\ d \times (1+e_m))]$ will be used as the measured distance. We examine different values of e_m from 0 to 80%. We assume that one wormhole exists in the network and the victims of the attack are randomly selected. The simulation results are illustrated in Figure 10.

The results show that IVoW greatly improves the detection accuracy when the distance estimation errors are relatively large. The improvements are primarily realized through the user interactions. They take advantage of the expertise and judgements of the user to drastically reduce the size of the suspicious area so that a more complicated detection method described in section 7.2 can be applied to a localized network.

8.2 Detection Accuracy under Multiple Wormholes

One of the advantages of IVoW is that it can detect the fake neighbor connections when there are multiple wormholes in the network. In the second group of experiments, we fix the value of e_m at 40% and examine the detection accuracy of the proposed mechanism when the number of wormholes changes. The victims of the attacks are randomly and independently selected as long as the distance between the two ends of a wormhole is longer than the communication range. The results are illustrated in Figure 11.

The improvements are more obvious in this group of experiments. Through the user interactions, the detection procedure can

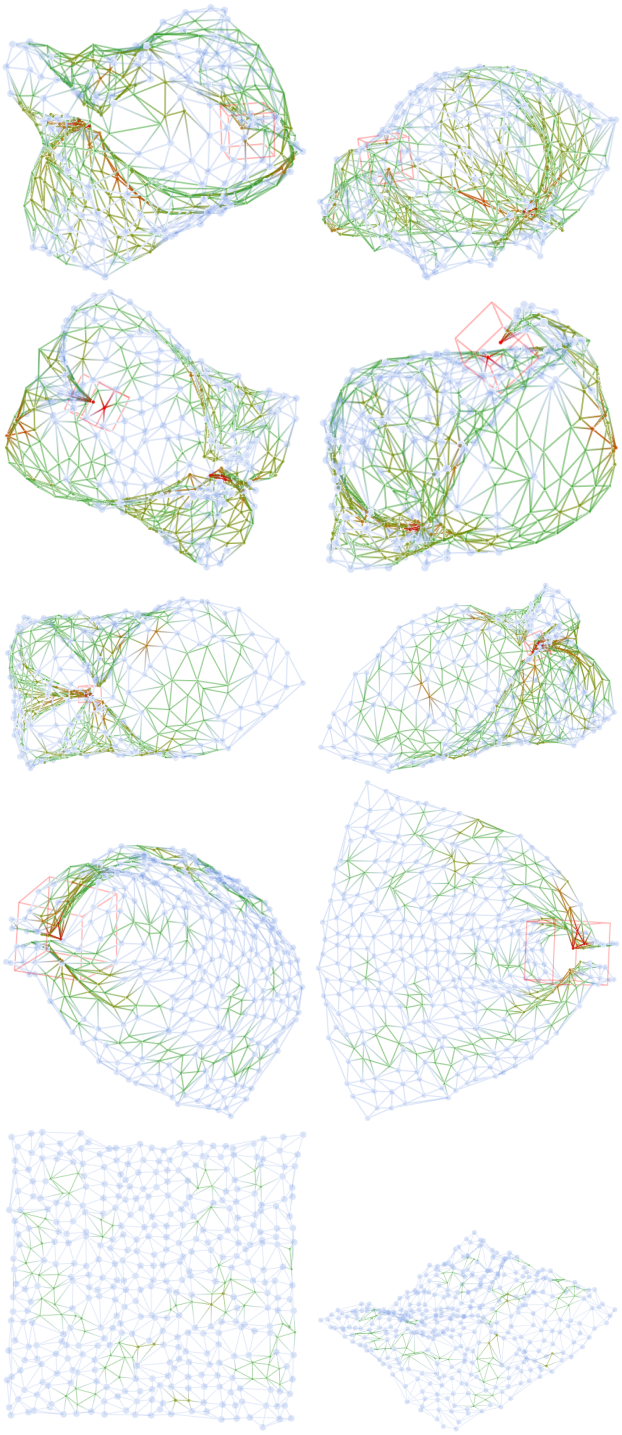
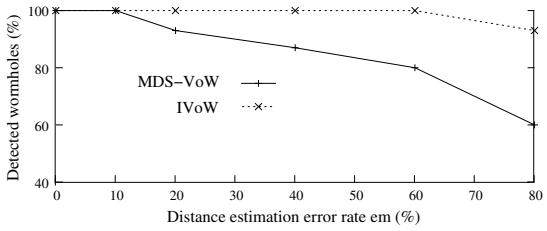
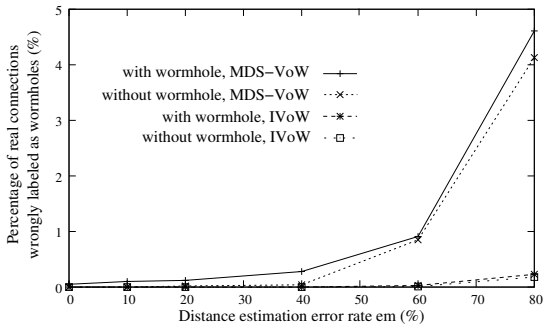


Figure 9: The interactive wormhole detection procedure is shown from top to bottom with two views for each user input and the consequent detection result. A user simply draws a transparent red cube around a potential attack region and a progressive algorithm is performed to analyze the details.



(a) improvements in detection accuracy of IVoW (compared to MDS-VoW)



(b) reduction in false positive alarms of IVoW (compared to MDS-VoW)

Figure 10: Detection accuracy of IVoW under different distance estimation error rates.

locate the suspicious areas more accurately and the impacts of multiple wormholes on the detection accuracy are reduced. From the results in Figure 10 and 11, we find that the user interactions can improve both the wormhole detection efficiency and accuracy, and the proposed mechanism is robust against the distance estimation errors and multiple wormholes.

9 Conclusions and Future Work

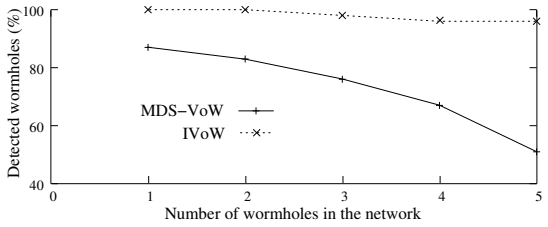
In this paper, we propose an approach that integrates visual representation, user interaction, and automatic analysis algorithms to defend against wormhole attacks in wireless networks. Through integrating interactive visualization into multiple steps of IVoW including representation, monitoring, and detection, we show that visualization can not only be used to improve information understanding, but also be combined with domain knowledge and user expertise to solve problems through visual analysis.

While the detection of one kind of attack is investigated in depth, the basic ideas presented here can be extended to deal with other aspects of network security. For example, the anomalies in the localized neighbor relations caused by the fake identities can be used to detect Sybil attacks. If the reconstructed network topology is monitored together with the traffic flows, the black holes of data transmission in wireless networks can be located. The visualization techniques and interaction interfaces enable the users to analyze and manage the networks with an ever-increasing scale and complexity. Furthermore, directly applying the network topology information to attack detection avoids the overhead and inaccuracy caused by the parameter measurement procedures.

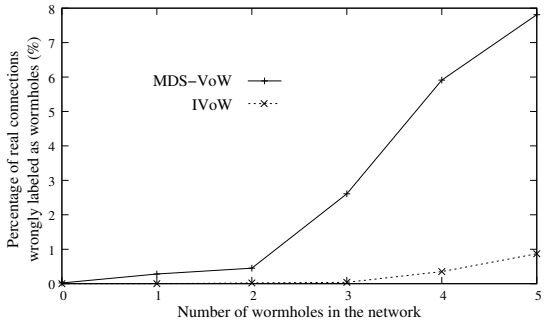
To better evaluate the proposed approach, we will investigate its detection accuracy by applying it to real large scale wireless network environments such as underwater sensor networks, in which the nodes can move freely in 3D spaces. We plan to investigate visualization of other attacks based on the connectivity information among wireless nodes. A more generic attack detection framework integrating visualization and interaction techniques will be developed to enforce wireless network security.

References

[1] *IEC Workshop on Internet Simulations with the NS simulator*, 2000.



(a) improvements in detection accuracy of IVoW (compared to MDS-VoW)



(b) reduction in false positive alarms of IVoW (compared to MDS-VoW)

Figure 11: Detection accuracy of IVoW when the number of wormholes increases.

[2] K. Abdullah, C. Lee, G. Conti, J. Copeland, and J. Stasko. IDS rainstorm: Visualizing IDS alarms. In *Proc. of VizSEC*, 2005.

[3] R. Ball, G. Fink, A. Rathi, S. Shah, and C. North. Home-centric visualization of network traffic for security administration. In *Proc. of ACM VizSEC/DMSEC*, 2004.

[4] W. Basalaj. Incremental multidimensional scaling method for database visualization. In *Visual Data Exploration and Analysis VI (Proc. SPIE, volume 3643)*, 1999.

[5] V. Bhuse and A. Gupta. Anomaly intrusion detection in wireless sensor networks. *Journal of High Speed Networks*, 1(15), 2006.

[6] P. Biswas and Y. Ye. Semidefinite programming for ad hoc wireless sensor network localization. In *Proc. of ACM/IEEE IPSN*, 2004.

[7] M. Chalmers. A linear iteration time layout algorithm for visualizing high dimensional data. In *Proc. IEEE Visualization*, pages 127–132, 1996.

[8] M. Chirumamilla and B. Ramamurthy. Agent based intrusion detection and response system for wireless LANs. In *Proc. of IEEE International Conference on Communications*, pages 492–496, 2003.

[9] B. Clark, C. Colbourn, and D. Johnson. Unit disk graphs. *Discrete Mathematics*, 86(1–3):165–177, 1990.

[10] B. Dahill, B. Levine, E. Royer, and C. Shields. A secure routing protocol for ad hoc networks. University of Massachusetts, Tech Report CS-02-32, 2001.

[11] M. Davison. *Multidimensional Scaling*. John Wiley and Sons, 1983.

[12] W. Du, L. Fang, and P. Ning. LAD: Localization anomaly detection for wireless sensor networks. In *Proc. of International Parallel and Distributed Processing Symposium*, 2005.

[13] W. Fan, M. Miller, S. Stolfo, W. Lee, and P. Chan. Using artificial anomalies to detect unknown and known network intrusions. *Knowledge and Information Systems*, 6(5), 2004.

[14] G. Fink, P. Muessig, and C. North. Visual correlation of host processes and traffic. In *Proc. of VizSEC*, 2005.

[15] J. Goodall, P. Rheingans, W. Lutters, and A. Komlodi. Preserving the big picture: Visual network traffic analysis with TNV. In *Proc. of VizSEC*, 2005.

[16] J. Hall, M. Barbeau, and E. Kranakis. Using mobility profiles for anomaly based intrusion detection in mobile networks. In *Proc. of Wireless and Mobile Security Workshop*, 2005.

[17] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Proc. of NDSS*, 2004.

[18] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *Proc. of IEEE INFOCOM*, 2003.

[19] X. Ji and H. Zha. Sensor positioning in wireless ad-hoc sensor networks with multidimensional scaling. In *Proc. of INFOCOM*, 2004.

[20] A. Komlodi, P. Rheingans, U. Ayachit, J. Goodall, and A. Joshi. A user-centered look at glyph-based security visualization. In *Proc. of VizSEC*, 2005.

[21] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia, and B. Bhargava. Low-cost attacks against packet delivery, localization and time synchronization services in under-water sensor networks. In *Proceedings of ACM Wireless Security (WiSe)*, pages 87–96, 2005.

[22] A. Ladd, K. Bekris, A. Rudys, G. Marceau, L. Kavraki, and D. Wallach. Robotics-based location sensing using wireless Ethernet. In *Proceedings of ACM MobiCom*, 2002.

[23] K. Lakkaraju, W. Yurcik, A. Lee, R. Bearavolu, Y. Li, and X. Yin. Nvisionip: Netflow visualizations of system state for security situational awareness. In *Proceedings of ACM VizSEC/DMSEC*, 2004.

[24] Y. Livnat, J. Agutter, S. Moon, R. Erbacher, and S. Foresti. A visualization paradigm for network intrusion detection. In *Proceedings of the IEEE Information Asssurance Workshop*, pages 92–99, 2005.

[25] J. McPherson, K. Ma, P. Krystosk, T. Bartoletti, and M. Christensen. Portvis: A tool for port-based detection of security events. In *Proc. of ACM VizSEC/DMSEC*, 2004.

[26] A. Morrison, G. Ross, and M. Chalmers. A hybrid layout algorithm for subquadratic multidimensional scaling. In *Proc. IEEE Symposium on Information Visualization*, pages 152–158, 2002.

[27] E. P. Mücke. A robust implementation for three-dimensional delaunay triangulations. In *Proceedings of the 1st International Computational Geometry Software Workshop*, pages 70–73, 1995.

[28] C. Muelder, K. Ma, and T. Bartoletti. A visualization methodology for characterization of network scans. In *Proc. of VizSEC*, 2005.

[29] D. Niculescu and B. Nath. Ad hoc positioning system (APS) using AoA. In *Proceedings of IEEE INFOCOM*, 2003.

[30] P. Papadimitratos and Z. Haas. Secure routing for mobile Ad Hoc networks. In *Proc. of SCS CNDS*, 2002.

[31] R. Poovendran and L. Lazos. A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. accepted to appear in *ACM Journal on Wireless Networks (WINET)*, 2006.

[32] N. Priyantha, A. Chakraborty, and H. Padmanabhan. The cricket location support system. In *Proc. of ACM MobiCom*, pages 32–43, 2000.

[33] D. Rafiei and S. Curial. Effectively visualizing large networks through sampling. In *Proc. of IEEE Visualization*, 2005.

[34] A. Rao, S. Ratnasamy, C. Papadimitriou, S. Shenker, and I. Stoica. Geographic routing without location information. pages 96–108, 2003.

[35] P. Ren, Y. Gao, Z. Li, Y. Chen, and B. Watson. IDGraphs: Intrusion detection and analysis using histographs. In *Proc. of VizSEC*, 2005.

[36] A. Savvides, C. Han, and M. Srivastava. Dynamic fine-grained localization in ad-hoc networks of sensors. In *Proc. of MobiCom*, 2001.

[37] Y. Shang, W. Ruml, Y. Zhang, and M. Fromherz. Localization from mere connectivity. In *Proceedings of ACM MobiHoc*, 2003.

[38] W. Torgeson. Multidimensional scaling of similarity. *Psychometrika*, 30:379–393, 1965.

[39] W. Wang and B. Bhargava. Visualization of wormhole attacks in sensor networks. In *Proc. of ACM Workshop on Wireless Security*, 2004.

[40] M. Williams and T. Munzner. Steerable, progressive multidimensional scaling. In *Proceedings of InfoVis*, 2004.

[41] W. Yurcik. VisFlowConnect-IP: A link-based visualization of netflows for security monitoring. In *18th Annual FIRST Conference on Computer Security Incident Handling*, 2006.

[42] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *Proc. of ACM MobiCom*, pages 275–283, 2000.

[43] Y. Zhang, W. Lee, and Y. Huang. Intrusion detection techniques for mobile wireless networks. *Wireless Networks Journal*, 9(5), 2003.