International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 10, October 2014)

Identity Based Detection of Spoofing Attackers in Wireless Networks and Practical Solutions

M.Venkateshwarlu
M.Tech CSE Scholar
SRTIST
Nalgonda, TS, India

P.Rajendra Prasad
Assistant Professor & M.Tech In charge (CSE)
SRTIST
Nalgonda, TS, India

T.Madhu
Associate Professor & HOD
SRTIST
Nalgonda, TS, India

Dr.T.Siva Sankar Reddy
Principal & Professor
SRTIST
Nalgonda, TS, India

Abstract: **Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. In this paper, we propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for (1) detecting spoofing attacks; (2) determining the number of attackers when multiple adversaries masquerading as a same node identity; and (3) localizing multiple adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. We then formulate the problem of determining the number of attackers as a multi-class detection problem. Cluster-based mechanisms are developed to determine the number of attackers. When the training data is available, we explore using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers. We evaluated our techniques through two testbeds using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings. Our experimental results show that our proposed methods can achieve over 90% Hit Rate and Precision when determining the number of attackers. Our localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.**

Keywords: **Wifi, Spoofing, Wireless, RSS, MAX, WEP, WPA, ISP**

1. INTRODUCTION

The wireless transmission medium, adversaries can monitor any transmission. In various types of attacks, identity based spoofing attacks are especially easy to launch and can cause significant damage to network performance. In 802.11 networks, it is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an ifconfig command to masquerade as another device. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA),or 802.11i (WPA2), such methodology can only protect data frames - an attacker can still spoof management or control frames to cause significant impact on networks.

IDS watch the wired and wireless network from the inside and report or alarm depending on how they evaluate the network traffic they see. They continually monitor for access points to the network and are able, in some cases, to do comparisons of the security controls defined on the access point with pre-defined company security standards and either reset or closedown any non conforming AP's they find. The distinction between placing IDS sensors on both wired and wireless networks is an important one as large corporate networks can be worldwide.IDS systems can also identify and alert to the presence of unauthorized MAC addresses on the networks. This can be an invaluable aid in tracking down hackers.

Spoofing attacks can further facilitate a variety of traffic injection attacks, such as attacks on access control lists, rogue access point attacks, and eventually Denial-of-Service (DoS) attacks. A broad survey of possible spoofing attacks can be found in a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as network resource utilization attack and denial-of-service attack quickly. Therefore, it is important to detect the presence of spoofing attacks, determine the number of attackers, and localize multiple adversaries and eliminate them.

The main contributions of our work are: GADE: a generalized attack detection model that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods grounded on RSS-based spatial correlations among normal devices and adversaries; and IDOL: an integrated detection and localization system that can both detect attacks as well as find he positions of multiple adversaries even when the adversaries vary their transmission power levels. The Partitioning around Medoids (PAM) cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multi-class detection problem. We further developed a mechanism called SILENCE for testing Silhouette Plot and System Evolution with minimum distance of clusters, to improve the accuracy of determining the number of attackers. Additionally, when the training data is available, we propose to use Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers.

The fact that wireless channel response de-correlates quite rapidly in space, a channel-based authentication scheme was proposed to discriminate between transmitters at different locations, and thus to detect spoofing attacks in wireless networks focused on building fingerprints of 802.11b WLAN NICs by extracting radiometric signatures, such as frequency magnitude, phase errors, and I/Q origin offset, to defend against identity attacks. However, there is additional overhead associated with wireless channel response and radiometric signature extraction in wireless networks. In WSN network introduced a security layer that used forge-resistant relationships based on the packet traffic, including MAC sequence number and traffic pattern, to detect spoofing attacks. The MAC sequence number has also been used in performs of spoofing detection. Both the sequence number and the traffic pattern can be manipulated by an adversary as long as the adversary learns the traffic pattern under normal conditions.

The node's "spatial signature", including Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) to authenticate messages in wireless networks. However, none of these approaches are capable of determining the number of attackers when there are multiple adversaries collaborating to use the same identity to launch malicious attacks. Further, they do not have the ability to localize the positions of the adversaries after attack detection.

MAC Address spoofing: MAC addresses can be easily changed through device drivers, effective attacks can be implemented with some equipment available on the market. IEEE 802.11 facing many security threats, which represented by a class of attacks which can be known as masquerading attacks. With such tools, the attacker modifies either the MAC or the IP address of the victim in order to adopt another identity in the network. By this technique the intruder will be able to operate as a trust worthy node and can advertise incorrect routing information to other participants of the network. Another example is creation of loops in the routing computation which result in unreachable nodes.
To prevent and secure the network from spoofing, the specialist divided the techniques into three categories:

1. Sequence number analysis: by modifying the MAC address header, so each device will have a serial number (SN)
2. Transceiver fingerprinting: where each radio transceiver has its unique shape and pattern.
3. Signal strength analysis: This depends on the strength of the coming signals from the clients.

Physical Layer: Physical layer is hard to frog and not easy as the MAC address; because the information in this layer is inherent to radio characteristics and the physical environment, in addition it is used to differentiate devices. Hall uses the frequency-domain patterns of the transient portion of radiofrequency (RF) signals, as a fingerprint, to uniquely identify a transceiver

Existing System: In the present system Ingress and Egress are

- Ingress – An ISP prohibits receiving from its stub connected networks packets whose source address does not belong to the corresponding stub network address space
- Egress – A router or a firewall which is the gateway of a stub network filters out any packet whose source address does not belong to the network address space.

Present system is having the following disadvantages are: Allows Spoofing within a stub network, not self defensive, Effective only when implemented by large number of networks, Deployment is costly, Incentive for an ISP is very low

2. LITERATURE SURVEY

2.1. Supporting Anonymous Location Queries in Mobile Environments with Privacy grid: This paper presents PrivacyGrid - a framework for supporting anonymous location-based queries in mobile information delivery systems. The PrivacyGrid framework offers three unique capabilities. First, it provides a location privacy protection preference profile model, called location P3P, which allows mobile users to explicitly define their preferred location privacy requirements in terms of both location hiding measures (e.g., location k-anonymity and location l-diversity) and location service quality measures (e.g., maximum spatial resolution and maximum temporal resolution). Second, it provides fast and effective location cloaking algorithms for location k-anonymity and location l-diversity in a mobile environment. We develop dynamic bottom-up and top-down grid cloaking algorithms with the goal of achieving high anonymization success rate and efficiency in terms of both time complexity and maintenance cost. A hybrid approach that carefully combines the strengths of both bottom-up and top-down cloaking approaches to further reduce the average anonymization time is also developed. Last but not the least, PrivacyGrid incorporates temporal cloaking into the location cloaking process to further increase the success rate of location anonymization. We also discuss PrivacyGrid mechanisms for supporting anonymous location queries. Experimental evaluation shows that the PrivacyGrid approach can provide close to optimal location k-anonymity as defined by per user location P3P without introducing significant performance penalties.

2.2. On the Value of a Random Minimum Weight Steiner Tree: Consider a complete graph on n vertices with edge weights chosen randomly and independently from an exponential distribution with parameter 1. Fix k vertices and consider the minimum weight Steiner tree which contains these vertices. We prove that with high probability the weight of this tree is $(1 + o(1))(k − 1)(\log n − \log k)/n$ when $k = o(n)$ and $n\to\infty$. 1.

2.3. Random Key Predistribution Schemes for Sensor Networks: Key establishment in sensor networks is a challenging problem because asymmetric key cryptosystems are unsuitable for use in resource constrained sensor nodes, and also because the nodes could be physically compromised by an adversary. We present three new mechanisms for key establishment using the framework of pre-distributing a random set of keys to each node. First, in the q-composite keys scheme, we trade off the unlikeliness of a large-scale network attack in order to significantly strengthen random key predistribution's strength against smaller-scale attacks. Second, in the multipath-reinforcement scheme, we show how to strengthen the security between any two nodes by leveraging the security of other links. Finally, we present the random-pairwise keys scheme, which perfectly preserves the secrecy of the rest of the network when any node is captured, and also enables node-to-node authentication and quorum-based revocation.

2.4. *Enhancing Base Station Security in Wireless Sensor Networks:* Wireless sensor networks that are deployed in applications such as battlefield monitoring and home sentry systems face acute security concerns, including eavesdropping, forgery of sensor data, denial of service attacks, and the physical compromise of sensor nodes. Sensor networks are often organized hierarchically, with a base station serving as a gateway for collecting data from a multi-hop network of resourceconstrained sensor nodes. Prior work that has focused on securing the routing between sensor nodes has assumed that the base station is sufficiently powerful to defend itself against security threats. This paper considers strategies for securing the sensor network against a variety of threats that can lead to the failure of the base station, which represents a central point of failure. First, multipath routing to multiple destination base stations is analyzed as a strategy to provide tolerance against individual base station attacks and/or compromise. Second, confusion of address and identification fields in packet headers via hashing functions is explored as a technique to help disguise the location of the base station from eavesdroppers. Third, relocation of the base station in the network topology is studied as a means of enhancing resiliency and mitigating the scope of damage.

2.5. *Intrusion Tolerance and Anti- Traffic Analysis Strategies for Wireless Sensor Networks:* Wireless sensor networks face acute security concerns in applications such as battlefield monitoring. A central point of failure in a sensor network is the base station, which acts as a collection point of sensor data. In this paper, we investigate two attacks that can lead to isolation or failure of the base station. In one set of attacks, the base station is isolated by blocking communication between sensor nodes and the base station, e.g. by DOS attacks. In the second attack, the location of the base station is deduced by analyzing data traffic towards the base station, which can lead to jamming and/or discovery and destruction of the base station. To defend against these attacks, two secure strategies are proposed. First, secure multi-path routing to multiple destination base stations is designed to provide intrusion tolerance against isolation of a base station. Second, anti-traffic analysis strategies are proposed to help disguise the location of the base station from eavesdroppers. A performance evaluation is provided for a simulated sensor network, as well as measurements of cryptographic overhead on real sensor nodes.

3. PRPOSED SYSTEM

The proposed System used Inter domain Packet filters (IDPFs) architecture, a system that can be constructed solely based on the locally exchanged BGP updates. Each node only selects and propagates to neighbors based on two set of routing policies. They are Import and Export Routing policies. The IDPFs uses a feasible path from source node to the destination node, and a packet can reach to the destination through one of its upstream neighbors. The training data is available; we explore using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries. The Cluster Based wireless Sensor Network data received signal strength (RSS) based spatial correlation of network Strategy. A physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks.

Advantages of Proposed System:

- Damage Reduction under SPM Defense is high
- Client Traffic
- Comparing to other methods the benefits of SPM are more.
- SPM is generic because their only goal is to filter spoofed packets.

4. IMPLEMENTATION

MODULES:

- Blind & Non-Blind Spoofing
- Man in the Middle Attack
- Constructing Routing Table
- Finding Feasible path
- Constructing Inter-Domain Packet Filters
- Receiving the valid packets

4.1. Blind & Non-Blind Spoofing:

- Spoofing detection is to devise strategies that use the uniqueness of spatial information.
- In location directly as the attackers' positions are unknown network RSS, a property closely correlated with location in physical space and is readily available in the wireless networks.
- The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive.

- The number of attackers when there are multiple adversaries masquerading as the same identity.

4.2. Man in the Middle Attack:

- Localization is based on the assumption that all measurements gathered received signal strength (RSS) are from a single station and, based on this assumption, the localization algorithm matches a point in the measurement space with a point in the physical space.
- The spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node.
- RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space.

4.3. Constructing Routing Table:

- The channel frequency response is sensitive to each multipath. An impulse in the time domain is a constant in the frequency domain, and thus a change to a single path may change the entire multiple tone link of Network.
- In wireless networks classes that provide automatic reconfiguration of APs, adjusting power levels and channel assignments to optimize coverage while minimizing contention between neighbors.
- The RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space.

4.4. Finding feasible path (Attack Computation):

- Converting the large dataset into medium format for the computation purpose.
- In this medium the rows consists of http request and columns consists of time for a particular user (IP address).
- Received Signal Strength Indicator Formula,

$$P(d)[dBm] = P(d_0)[dBm] - 10\gamma \log_{10}\left(\frac{d}{d_0}\right)$$

  - The RSS stream of a node identity may be mixed with RSS readings of both the original node as well as spoofing nodes from different physical locations.

4.5. Constructing Inter-Domain Packet Filters:

- The clustering algorithms cannot tell the difference between real RSS clusters formed by attackers at different positions and fake RSS clusters caused by outliers and variations of the signal strength.
- The minimum distance between two clusters is large indicating that the clusters are from different physical locations.
- The minimum distance between the returned clusters to make sure the clusters are produced by attackers instead of RSS variations and outliers.

4.6. Receiving different Transmission Power:

- The transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately.
- The CDF of localization error of RADAR-Gridded and ABP when adversaries using different transmission power levels.
- In detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98% and determining the number of network.

5. INPUT & OUTPUT DESIGN

5.1. ***Input Design:*** The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- ➢ What data should be given as input?
- ➢ How the data should be arranged or coded?
- ➢ The dialog to guide the operating personnel in providing input.
- ➢ Methods for preparing input validations and steps to follow when error occur.

Objectives

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. .When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

5.2. ***Output Design:*** A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
1. Select methods for presenting information.
2. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

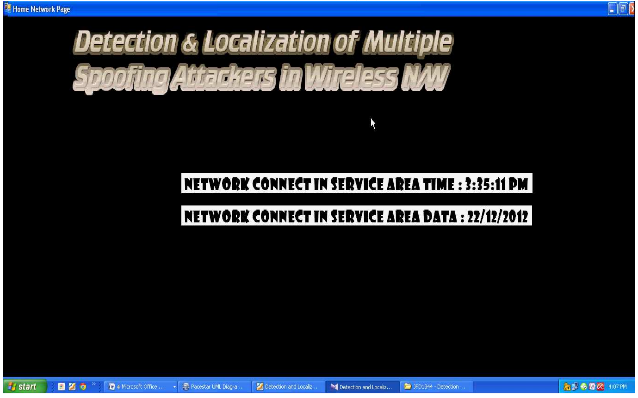
- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

6. CONCLUSION

In this work, we proposed to use received signal strength (RSS) based spatial correlation, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. We provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. We derived the test statistic based on the cluster analysis of RSS readings. Our approach can detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. We developed SILENCE, a mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution, that use cluster analysis alone. Additionally, when the training data is available, we explored using Support Vector Machines (SVM) based mechanism to further improve the accuracy of determining the number of attackers present in the system. To validate our approach, we conducted experiments on two testbeds through both an 802.11network (WiFi) and an 802.15.4 (ZigBee) network in two real office building environments. We found that our detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98% and determining the number of adversaries, achieving over 90% hit rates and precision simultaneously when using SILENCE and SVM-based mechanism. Further, based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.

1. SCREEN SHOTS

Home Page:



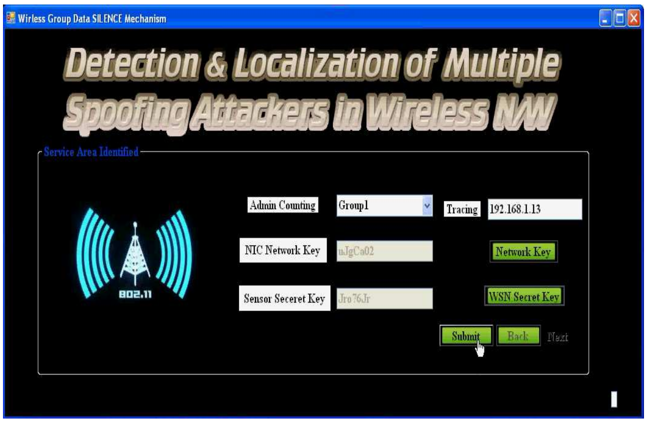
Home Network Page

Detection & Localization of Multiple Spoofing Attackers in Wireless N/W

NETWORK CONNECT IN SERVICE AREA TIME : 3:35:11 PM

NETWORK CONNECT IN SERVICE AREA DATA : 22/12/2012

Data License Mechanism:



Wirless Group Data SILENCE Mechanism

Detection & Localization of Multiple Spoofing Attackers in Wireless N/W

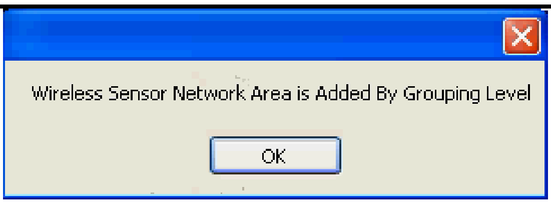
Service Area Identified

Admin Counting: Group1

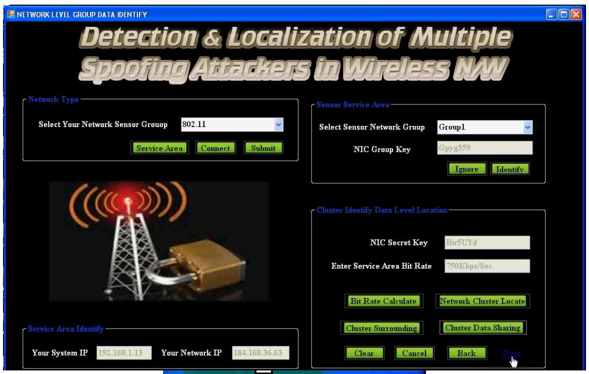
Tracing: 192.168.1.13

NIC Network Key: uJgCa02

Sensor Seceret Key: Jro76Jr


Wireless Sensor Network Area is Added By Grouping Level

Network Level:


NETWORK LEVEL GROUP DATA IDENTIFY

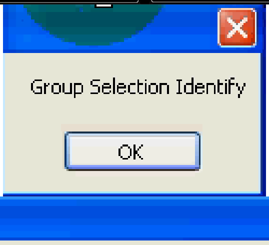
Detection & Localization of Multiple Spoofing Attackers in Wireless N/W

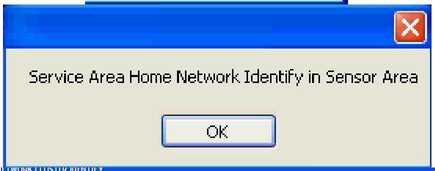
Network Type
Select Your Network Sensor Grouop: 802.11

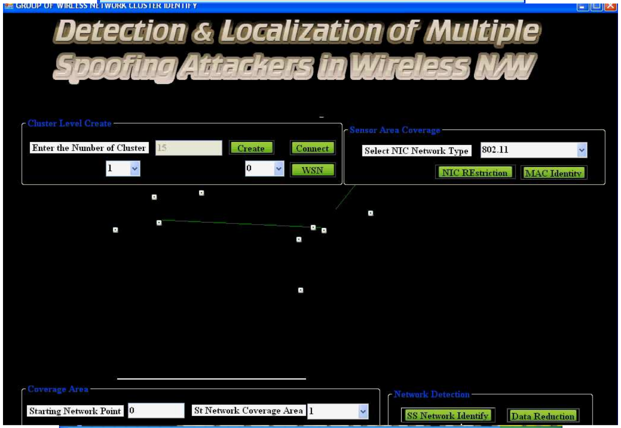
Sensor Service Area
Select Sensor Network Group: Group1
NIC Group Key: Gpyg359

Cluster Identify Data Level Location
NIC Secret Key: Bir5UYd
Enter Service Area Bit Rate: 750Kbps/Sec

Service Area Identify
Your System IP: 192.168.1.13
Your Network IP: 184.168.36.63


Group Selection Identify


Service Area Home Network Identify in Sensor Area


GROUP OF WIRLESS NETWORK CLUSTER IDENTIFY

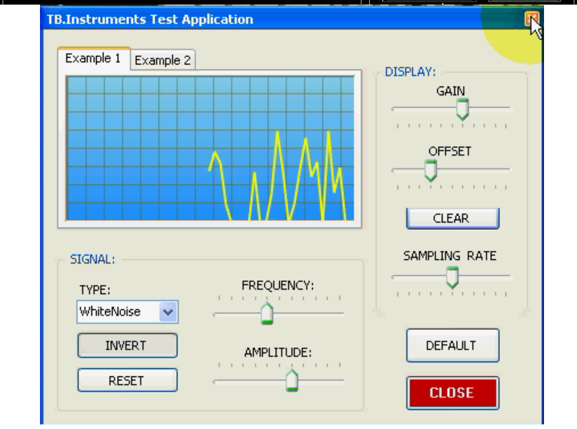
Detection & Localization of Multiple Spoofing Attackers in Wireless N/W

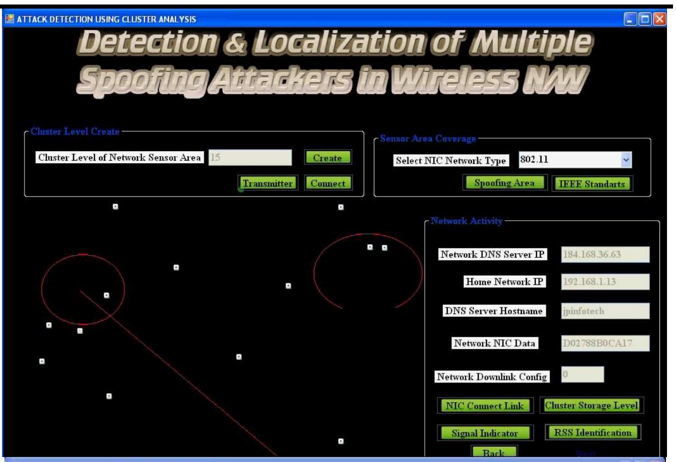
Cluster Level Create
Enter the Number of Cluster: 15
1
0

Sensor Area Coverage
Select NIC Network Type: 802.11

Coverage Area
Starting Network Point: 0
St Network Coverage Area: 1

Network Detection


TB.Instruments Test Application

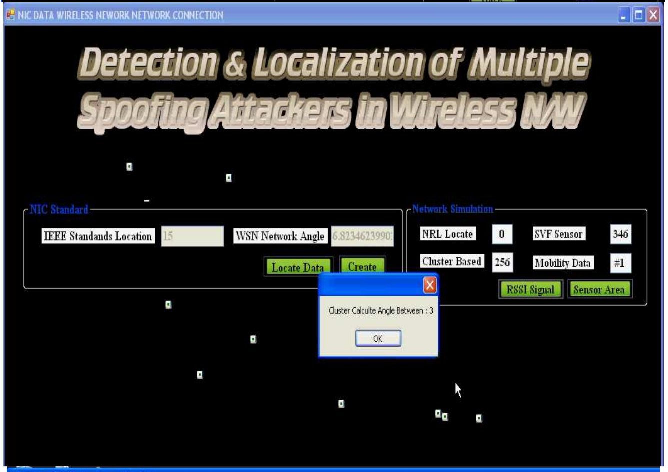

ATTACK DETECTION USING CLUSTER ANALYSIS

Detection & Localization of Multiple Spoofing Attackers in Wireless N/W

Cluster Level Create
Cluster Level of Network Sensor Area: 15

Sensor Area Coverage
Select NIC Network Type: 802.11

Network Activity
Network DNS Server IP: 184.168.36.63
Home Network IP: 192.168.1.13
DNS Server Hostname: jpinfotech
Network NIC Data: D02788B0CA17
Network Downlink Config: 0

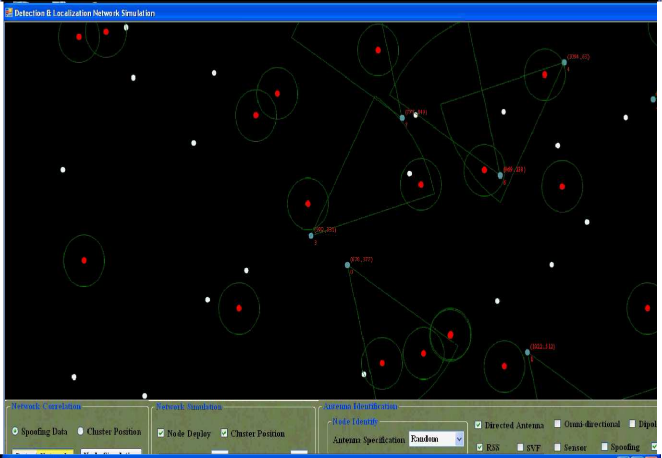

NIC DATA WIRELESS NEWORK NETWORK CONNECTION

Detection & Localization of Multiple Spoofing Attackers in Wireless N/W

NIC Standard
IEEE Standands Location: 15
WSN Network Angle: 6.82346239907

Network Simulation
NRL Locate: 0
SVF Sensor: 346
Cluster Based: 256
Mobility Data: #1

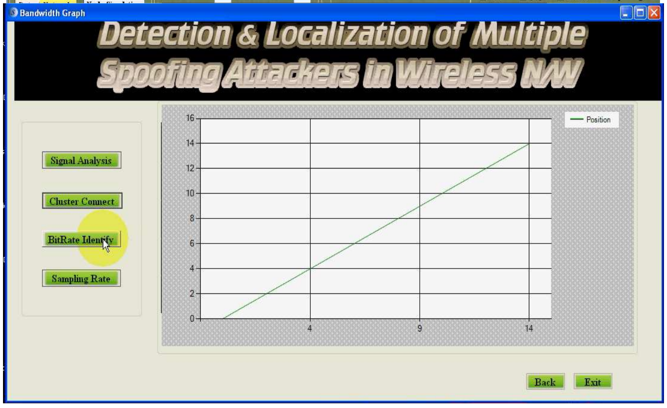
Cluster Calculte Angle Between : 3


Detection & Localization Network Simulation

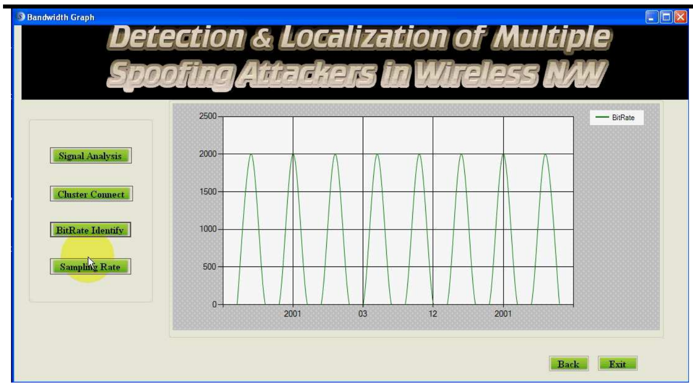
Network Correlation
● Spoofing Data ○ Cluster Position

Network Simulation
☑ Node Deploy ☑ Cluster Position

Antenna Identification
Node Identify
Antenna Specification: Random
☑ Directed Antenna □ Omni-directional □ Dipol
☑ RSS □ SVF □ Sensor □ Spoofing ☑


Bandwidth Graph

Detection & Localization of Multiple Spoofing Attackers in Wireless N/W



REFERENCES

[1]. J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulnerabilities and practical solutions,” in *Proceedings of the USENIX Security Symposium*, 2003, pp. 15 – 28.

[2]. F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access points vulnerabilities to dos attacks in 802.11 networks,” in *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2004.

[3]. D. Faria and D. Cheriton, “Detecting identity-based attacks in wireless networks using signalprints,” in *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, September 2006.

[4]. Q. Li and W. Trappe, “Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks,” in *Proc. IEEE SECON*, 2006.

[5]. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in *Proc. IEEE IPDPS*, 2005.

[6]. A. Wool, “Lightweight key management for ieee 802.11 wireless lans with key refresh and host revocation,” *ACM/Springer Wireless Networks*, vol. 11, no. 6, pp. 677–686, 2005.

[7]. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC layer spoofing using received signal strength,” in *Proc. IEEE INFOCOM*, April 2008.

[8]. J. Yang, Y. Chen, and W. Trappe, “Detecting spoofing attacks in mobile wireless environments,” in *Proc. IEEE SECON*, 2009.

[9]. Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wirelss spoofing attacks,” in *Proc. IEEE SECON*, May 2007.

[10]. M. bohge and W. Trappe, “An authentication framework for hierarchical ad hoc sensor networks,” in *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, 2003, pp. 79–87.

[11]. L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Fingerprints in the ether: using the physical layer for wireless authentication,” in *Proceedings of the IEEE International Conference on Communications (ICC)*, June 2007, pp. 4646–4651.

[12]. V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless device identification with radiometric signatures,” in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 116–127.

[13]. F. Guo and T. Chiueh, “Sequence number-based mac address spoof detection,” in *Recent Advances in Intrusion Detection*, 2006, pp. 309–329.

[14]. L. Sang and A. Arora, “Spatial signatures for lightweight security in wireless sensor networks,” in *The 27th Conference on Computer Communications, INFOCOM 2008.*, 2008, pp. 2137–2145.

[15]. P. Bahl and V. N. Padmanabhan, “RADAR: An in-building RF-based user location and tracking system,” in *Proc. IEEE INFOCOM*, 2000.

[16]. E. Elnahrawy, X. Li, and R. P. Martin, “The limits of localization using signal strength: A comparative study,” in *Proc. IEEE SECON*, Oct. 2004.

[17]. Y. Chen, J. Francisco, W. Trappe, and R. P. Martin, “A practical approach to landmark deployment for indoor localization,” in *Proc. IEEE SECON*, September 2006.

[18]. J. Yang and Y. Chen, “A theoretical analysis of wireless localization using RF-based fingerprint matching,” in *Proceedings of the Fourth International Workshop on System Management Techniques, Processes, and Services (SMTPS)*, April 2008.

[19]. P. Enge and P. Misra, *Global Positioning System: Signals, Measurements and Performance*. Ganga-Jamuna Pr, 2001.

[20]. Z. Yang, E. Ekici, and D. Xuan, “A localization-based anti-sensor network system,” in *26th IEEE International Conference on Computer Communications. INFOCOM 2007*, 2007, pp. 2396–2400.