

Identifying and Locating Multiple Spoofing Attackers using Cluster in Wireless Network

Pallavi Mohan Bhujbal¹ Galande Rupali B.² Hilal Sadhana D.³ Thorat Priyanka N.⁴
^{1,2,3,4}Student

^{1,2,3,4}Department of Computer Engineering

¹SPCOE, Otur Pune ^{2,3,4}JCOE, University of Pune, 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 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 (Wi-Fi) 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.

Key words: Wireless network security, spoofing attack, attack detection, localization

I. INTRODUCTION

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. Spoofing attacks can further facilitate a variety of traffic injection attacks, such as attacks on access control lists, rogue access point (AP) attacks, and eventually Denial-of-Service (DoS) attacks. A broad survey of possible spoofing attacks can be found. Moreover, 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 1) detect the presence of spoofing attacks, 2) determine the number of attackers, and 3) localize multiple adversaries and eliminate them. Most existing approaches to address potential spoofing attacks employ cryptographic schemes. However, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It

is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned.

II. LITERATURE SURVEY

A. Access Points Vulnerabilities To Dos Attacks In 802.11 Networks:

We describe possible denial of service attacks to infrastructure wireless 802.11 networks. To carry out such attacks only commodity hardware and software components are required. The results show that serious vulnerabilities exist in different access points and that a single malicious station can easily hinder any legitimate communication within a basic service set.

B. Detecting Identity Based Attacks In Wireless Networks Using Signal Prints:

Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a septic client or to create multiple illegitimate identities. For example, several link-layer services in IEEE 802.11 networks have been shown to be vulnerable to such attacks even when 802.11i/1X and other security mechanisms are deployed. In this paper we show that a transmitting device can be robustly indented by its signal print, a tuple of signal strength values reported by access points acting as sensors. We show that, deferent from MAC addresses or other packet contents, attackers do not have as much control regarding the signal prints they produce.

C. Detecting And Localizing Wireless Spoofing Attacks:

Wireless networks are vulnerable to spoofing attacks, which allows for many other forms of attacks on the networks. Although the identity of a node can be verified through cryptographic authentication, authentication is not always possible because it requires key management and additional infrastructural overhead. In this paper we propose a method for both detecting spoofing attacks, as well as locating the positions of adversaries performing the attacks.

D. Detecting 802.11 Mac Layer Spoofing Using Received Signal Strength:

MAC addresses can be easily spoofed in 802.11 wireless LANs. An adversary can exploit this vulnerability to launch a large number of attacks. For example, an attacker may masquerade as a legitimate access point to disrupt network services or to advertise false services, tricking nearby wireless stations. On the other hand, the received signal strength (RSS) is a measurement that is hard to forge arbitrarily and it is highly correlated to the transmitter's

location. Assuming the attacker and the victim are separated by a reasonable distance, RSS can be used to differentiate them to detect MAC spoofing, as recently proposed by several researchers.

By analyzing the RSS pattern of typical 802.11 transmitters in a 3-floor building covered by 20 air monitors, we observed that the RSS readings followed a mixture of multiple Gaussian distributions. We discovered that this phenomenon was mainly due to antenna diversity, a widely-adopted technique to improve the stability and robustness of wireless connectivity. This observation renders existing approaches ineffective because they assume a single RSS source. We propose an approach based on Gaussian mixture models, building RSS profiles for spoofing

E. Detecting Spoofing Attacks In Mobile Wireless Environments:

The flexibility and openness of wireless networks enables an adversary to masquerade as other devices easily. Identity-based spoofing attacks are serious network threats as they can facilitate a variety of advanced attacks to undermine the normal operation of networks. However, the existing mechanisms can only detect spoofing attacks when the victim node and the spoofing node are static. In this paper, we propose a method for detecting spoofing attacks in the mobile wireless environment, that is when wireless devices, such as the victim node and/or the spoofing node are moving. We develop the DEMOTE system, which exploits Received Signal Strength (RSS) traces collected over time and achieves an optimal threshold to partition the RSS traces into classes for attack detection. Further, our novel algorithm alignment prediction (ALP), when without the knowledge of spatial constraint of the wireless nodes, utilizes temporal constraints to predict the best RSS alignment of partitioned RSS classes for RSS trace reconstruction over time. Our approach does not require any changes or cooperation from wireless devices other than packet transmissions.

III. SYSTEM IMPLEMENTATION

A. Generalized Attack Detection Model:

Generalized Attack Detection Model (GADE) consists of two phases: *attack detection*, which detects the presence of an attack, and *number determination*, which determines the number of adversaries.

B. Determining The Number Of Attackers:

Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries.

Since it is not known that how many adversaries will use the same node identity to launch attacks, determining the number of attackers becomes a multi-class detection problem and is similar to determining how many clusters exist in the RSS readings.

C. IDOL: Integrated Detection And Localization Framework:

Integrated systems that can detect spoofing attacks, determine the number of attackers, and localize multiple adversaries.

1) Block Diagram:

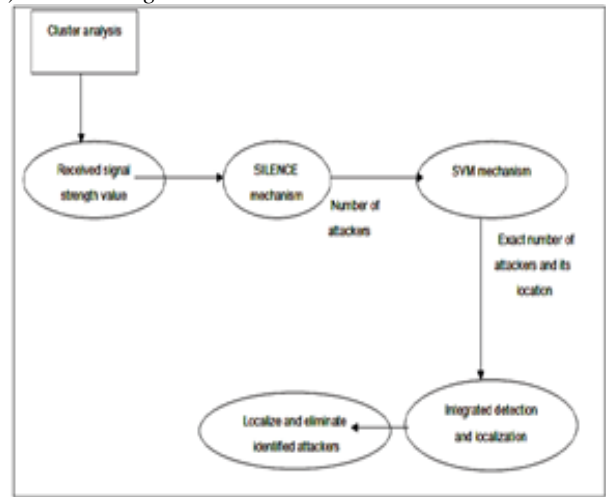


Fig. 1: Block diagram for System data Flow

2) Entity Relationship Diagram:

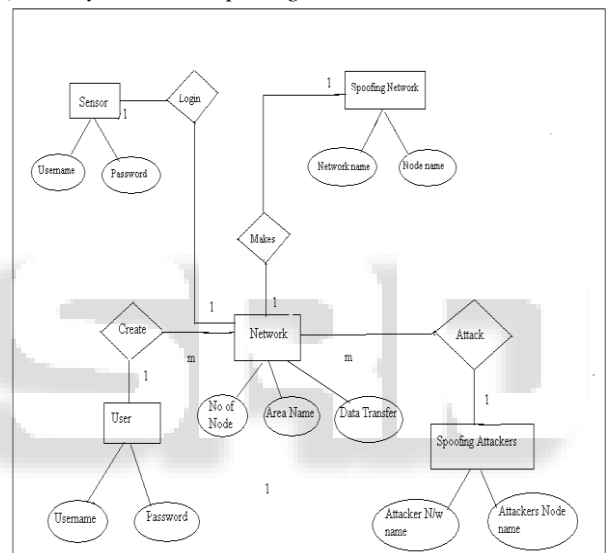


Fig. 2: Entity relationship diagram for Spoofing Attacks

ER-modeling is a data modeling technique used in software engineering to produce a conceptual data model of a information system. Diagrams created using this ER-modeling technique are called Entity-Relationship Diagrams, or ER diagrams or ERDs. So you can say that Entity Relationship Diagrams illustrate the logical structure of databases.

There are three basic elements in ER-Diagrams:

- Entities are the "things" for which we want to store information. An entity is a person, place, thing or event.
- Attributes are the data we want to collect for an entity.
- Relationships describe the relations between the entities.

ERDs show entities in a database and relationships between tables within that database. It is essential to have ER-Diagrams if you want to create a good database design. The diagrams help focus on how the database actually works.

IV. PROPOSED SYSTEM

- (1) The proposed system work is motivated from mitigating the limitations of previous schemes. In particular, the new system proposes a method in which the nodes are fixed as well as in movement. A reputation-based trust management scheme is designed to facilitate fast detection of compromised nodes. The key idea of the scheme is to detect untrustworthy zones and perform software attestation against nodes in these zones to detect and revoke the ones that are compromised.
- (2) Specifically, first divides the network into a set of zones, establish trust levels for each zone, and detect untrustworthy zones by using the Sequential Probability Ratio Test (SPRT). The SPRT decides a zone to be untrustworthy if the zone's trust is continuously maintained at low level or is quite often changed from high level to low level. once a zone is determined to be untrustworthy, the base station or the network operator.

V. MODULE DESCRIPTION

A. Spoofing Attack Detection:

In this module, spoofing attack detection is found out. To study Received Signal Strength (RSS), a property closely correlated with location in physical space and is readily available in the existing wireless networks. The RSS readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics.

The Received Signal Strength value vector as $s = (s_1, s_2, \dots, s_n)$ where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations. Generally, the RSS at the i 'th landmark from a wireless node is distributed as

$$S_i(d_j) [\text{dBm}] = P(d_0) [\text{dBm}] - 10\gamma \log(d_j/d_0) + X_i$$

Where, $P(d_0)$ represents the transmitting power of the node at the reference distance d_0 , d_j is the distance between the wireless node j and the i 'th landmark, and the path loss exponent, X_i is the shadow fading which is given as input. For simplicity, the wireless nodes have the same transmission power. If the received signal strength does not match in successive RSS values, then the node is said to be malicious.

B. Mobile Node Network Creation:

In this module, a form is generated which contains a text box to get node id and the id is saved in to "Nodes" table. During network creation, the nodes with id will be displayed in random X and Y position. The base station node is needing not be displayed as it is programmatically listens and updates the location information of all the nodes when they are in movement.

C. Mobile Movement (Random Walk) Within Given Speed:

In this module, all the nodes are roaming in any directions (their walk is updated by incrementing x-axis or y-axis or both at a movement with any number of pixels within the specified maximum limit. In practical situation, the nodes can move with their physical capabilities. For sake of

convenience, if the nodes reach the picture box limit, then they move in opposite direction so that they roam in the rectangular boundary of the picture box control.

VI. ALGORITHM AND PLATFORM

A. RADAR-Gridded:

The RADAR-Gridded algorithm is a scene-matching localization algorithm. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations. Given an observed RSS reading with an unknown location, RADAR returns the x, y of the nearest neighbor in the signal map to the one to localize, where "nearest" is defined as the Euclidean distance of RSS points in an N-dimensional signal space, where N is the number of landmarks.

In order to evaluate the generality of IDOL for localizing adversaries, we have chosen a set of representative localization algorithms ranging from nearest neighbor matching in signal space (RADAR), to probability-based (Area-Based-Probability), to multilateration (Bayesian Networks)

B. Receiver Operating Characteristic (ROC) Curve:

To evaluate an attack detection scheme we want to study the false positive rate P_{fa} and probability of detection P_d together. The ROC curve is a plot of attack detection accuracy against the false positive rate. It can be obtained by varying the detection thresholds. The ROC curve provides a direct means to measure the trade off between false-positives and correct detections.

VII. EXTENSION AND MATHEMATIC CALCULATION

A. Area Based Probability (ABP):

ABP also utilizes an interpolated signal map [16]. Further, the experimental area is divided into a regular grid of equal sized tiles. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading vector s . ABP then computes the probability of the wireless device being at each tile L_i , with $i = 1 \dots L$, on the floor using.

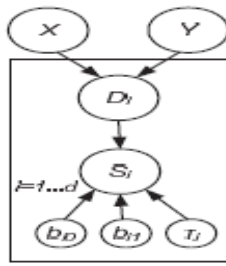
1) Bayes' Rule:

$$P(L_i|s) = \frac{P(s|L_i) \times P(L_i)}{P(s)} \quad (30)$$

Given that the wireless node must be at exactly one tile satisfying $\sum_{i=1}^L P(L_i|s) = 1$, ABP normalizes the probability and returns the most likely tiles/grids up to its confidence α .

B. Bayesian Networks (BN):

BN localization is a multilateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization. Figure 13 shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex s_i is the RSS reading from the i 'th landmark; and the vertex D_i represents the Euclidean distance between the location specified by X and Y and the i 'th landmark. The value of s_i follows a signal propagation model $s_i = b_{0i} + b_{1i} \log D_i$, where b_{0i} , b_{1i} are the parameters specific to the i 'th landmark.



Bayesian graphical model in our study

The distance $D_i = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$ in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the i 'th landmark. The network models noise and outliers by modeling the s_i as a Gaussian distribution around the above propagation model, with variance τ_i : $s_i \sim N(b_{0i} + b_{1i} \log D_i, \tau_i)$. Through Markov Chain Monte Carlo (MCMC) simulation, BN returns the sampling distribution of the possible location of X and Y as the localization result.

VIII. CONCLUSION

In this Wireless networks are used in Due to its proliferation of usage, there of spoofing attacks. In the proposed approach the presence of attacks as well as determine the number of adversaries as same node identity. It can localize any number of attackers and eliminate them. Determine the number of adversaries in particular, is a challenging task. This mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than methods under study, such as Silhouette Plot and System Evolution that use cluster analysis alone.

Further, based on the number of attackers determined by the mechanisms, our integrated detection and localization system can localize any number of a 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. The proposed methods can achieve over 90 to 98 percent Hit Rate and Precision when determining the number of attackers In future, based on the outcome of this model, e further to find ways to eliminate those identified multiple adversaries, from the wireless network. Thus way, wireless.

REFERENCES

[1] J. Bellardo And S. Savage, "802.11 Denial-Of-Service Attacks: Real Vulnerabilities And Practical Solutions," Proc. Usenix Security Symp., Pp. 15-28, 2003.

[2] Vulnerabilities And Practical Solutions," In Proceedings Of The Usenix Security Symposium, 2003, Pp. 15 – 28.

[3] 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.

[4] 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.

[5] J. Yang, Y. Chen, And W. Trappe, "Detecting Spoofing Attacks In Mobile Wireless Environments," In Proc. Ieee Secon, 2009.

[6] Jie Yang, Student Member, Ieee, Yingying (Jennifer) Chen, Senior Member, Ieee, Wade Trappe, Member, Ieee, And Jerry Cheng "Detection And Localization Of Multiple Spoofing Attackers In Wireless Networks-"Ieee Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.