IJIRAE International Journal of Innovative Research in Advanced Engineering ISSN: 2349-2163
Volume 1 Issue 4 (May 2014) http://ijirae.com

Detection of Spoofing attackers in wireless network

Raju M. Shingade
IV Semester, M-Tech, Dept of Computer
VJTI College Mumbai
rajshingade@gmail.com

Abhishek V. Mane (M.S)
Assistant Professor, Dept of Computer
VJTI College Mumbai
abhishekmane01@gmail.com

Abstract— Spoofing attacks effectively damage the networks performance and easy to launch by many tools available in market. The previous security approach to address spoofing attacks is to apply cryptographic authentication. However authentication method requires more infrastructures overhead. In this paper I propose the system of detecting spoofing attackers in wireless network by using spatial information associated with each node hard to falsify and not based on cryptography. This methodology can detect the attacks by spatial correlation received signal strength (RSS), inherited from multiple wireless node. To determine multiple spoofing attackers cluster based mechanisms are developed. I explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, I developed an integrated detection and localization system that can localize the positions of multiple attackers. The proposed methodology will obtain a reliable outcome that could be helpful in identifying and eliminating certain attacks.

Keywords— Wireless network security, cryptography, spoofing attack, attack detection

I. INTRODUCTION

Due to openness wireless network becomes target of most of the attacks. Due to the open-nature of these platforms, it will be particularly susceptible to spoofing attacks, where adversaries alter their network identifiers to those of legitimate entities. Spoofing attacks can be easily launched. As because of its open and shared nature of the wireless medium, where adversaries can perform passive monitoring of useful information of identity of user and then masquerade as another device using the collected identity. Spoofing attacks can further facilitate a variety of traffic injection attacks [1], [2], such as attacks on access control lists, rogue access point attacks, and eventually Denial-of-Service (DoS) attacks. Therefore it is important to detect spoofing attacks and prevent them and to prevent the attacks we have to first find out the attackers. Most previous approaches to find spoofing attacks required cryptographic methods. However the application of cryptographic methods requires reliable key distribution, management and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of the computational, distributional, infrastructural and management overhead. Existing 802.11 security techniques including Wired Equivalent Privacy (WEP), WiFi 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.

In this paper I propose a method for both detecting spoofing attacks, as well as locating the positions of adversaries performing the attacks.

II. SPOOFING ATTACK

Spoofing means, pretending to be something you are not. In Internet terms it means pretending to be a different Internet address from the one you really have in order to gain something. Spoofing attacks have different types like Email spoofing, DNS spoofing, ARP spoofing, WEB spoofing and IP spoofing we mainly focus on IP Spoofing. IP spoofing attack involves forging one's source address. It is the act of using one machine to impersonate another. Spoofing is an active security attack in which one machine on the network masquerades as a different machine. As an active attack, it disrupts the normal flow of data and may involve injecting data into the communications link between other machines.

III. EXISTING METHOD

The identity of a node can be verified through conventional security approaches are not always desirable. Adversaries can easily purchase low-cost devices and use these commonly available platforms to launch a variety of attacks. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. It is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address. It 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. The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network.

IV. PROPOSED METHOD

1) Detecting the presence of spoofing attacks
2) Determining the number of attackers when multiple adversaries masquerading as the same node identity
3) Localizing multiple adversaries and eliminate them

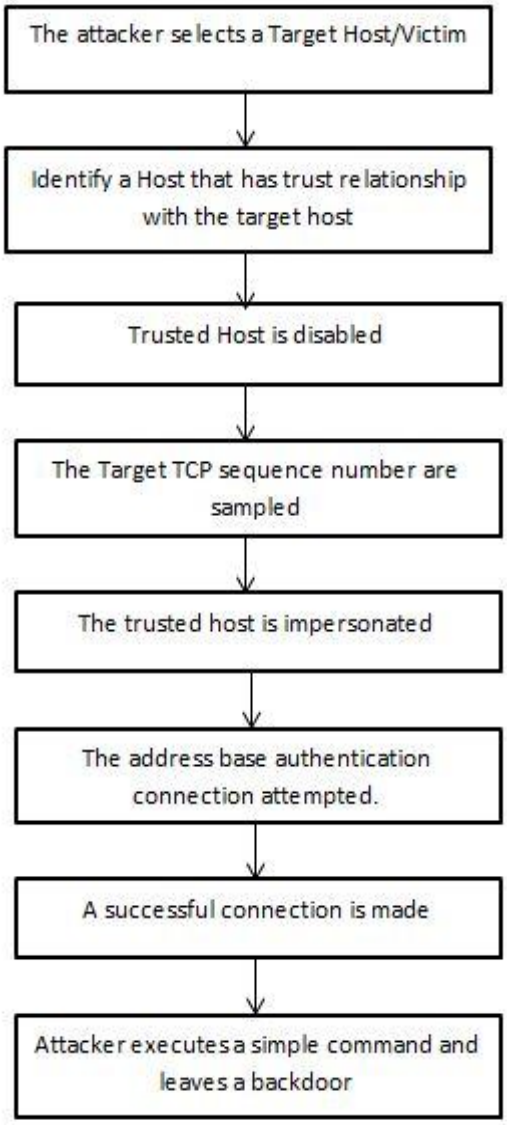

Fig. 1 Spoofing attack

V. MODULES

1) *Network configuration*
2) *Generalized attack detection model*
3) *Integrated detection and localization framework*
4) *Performance evaluation*

a) *Module Description*

1) Network configuration

The nodes are created and located in the simulation environment. The nodes are moved from one location to another location. The setdest command is used to give the movement to a node. The Random way point mobility model is used in our simulation. The nodes are using Omni-antenna to send and receive the data. The signals are propagated from one location to another location by using Two Ray Ground propagation model. The Priority Queue is maintained between any of the two nodes as the interface Queue.

2) Generalized Attack Detection Model

The Generalized Attack Detection Model consists of two phases: attack detection, which detects the presence of an attack, and number determination, which determines the number of adversaries. The challenge in spoofing detection is to devise

strategies that use the uniqueness of spatial information, but not using location directly as the attackers' positions are unknown. RSS property is closely correlated with location in physical space and is readily available in the existing wireless networks. Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks is closely related to the transmitter's physical location and is governed by the distance to the landmarks. 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.

3) Integrated Detection and Localization Framework

In this module, an integrated system that can both detect spoofing attacks, determine the number of attackers, and localize multiple adversaries.
The traditional localization approaches are based on averaged RSS from each node identity inputs to estimate the position of a node. However, in wireless spoofing attacks, 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. The traditional method of averaging RSS readings cannot differentiate RSS readings from different locations and thus is not feasible for localizing adversaries. Different from traditional localization approaches, our integrated detection and localization system utilize the RSS medoids returned from SILENCE as inputs to localization algorithms to estimate the positions of adversaries. The return positions from our system include the location estimate of the original node and the attackers in the physical space. Handling adversaries using different transmission power levels. An adversary may vary the transmission power levels when performing spoofing attacks so that the localization system cannot estimate its location accurately.

4) Performance Evaluation

The performance of the proposed scheme is evaluated by plotting the graph. The parameter used to evaluate the performance is as follows:

- False positive Rate
- Spoofing Detection rate
- Throughput

These parameter values are recorded in the trace file during the simulation by using record procedure. The recorded details are stored in the trace file. The trace file is executed by using the Xgraph to get graph as the output.

VI. ALGORITHMS

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), and to multilateration (Bayesian Networks) .

RADAR-Gridded: The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from. 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.

Area Based Probability (ABP): ABP also utilizes an interpolated signal map. 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 Li, with i = 1...L, on the floor using

Bayes' rule:

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

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

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 2 shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex si is the RSS reading from the ith landmark; and the vertex Di represents the Euclidean distance between the location specified by X and Y and the ith landmark. The value of si follows a signal propagation model $si = b_{0i}+b_{1i} \log Di$, where b_{0i}, b_{1i} are the parameters specific to the ith landmark The distance $Di = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$ in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i,

y_i) of the ith landmark. The network models noise and outliers by modeling the s_i as a Gaussian distribution around the above propagation model, with variance τi: si~N(b_{0i} + b_{1i} logDi, τ_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.

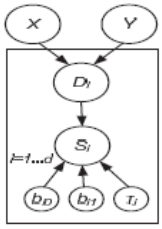

Fig 2. Bayasian graphical model in our study

VII. CONCLUSIONS

In this work, we proposed to use received signal strength 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 both detect the presence of attacks as well as determine the number of adversaries. 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 are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system. 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

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] [2] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access Points Vulnerabilities to Dos Attacks in 802.11 Networks,” Proc. IEEE Wireless Comm. and Networking Conf., 2004.
[3] [3] D. Faria and D. Cheriton, “Detecting Identity-Based Attacks in Wireless Networks Using Signalprints,” Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.
[4] [4] Q. Li and W. Trappe, “Relationship-Based Detection of Spoofing- Related Anomalous Traffic in Ad Hoc Networks,” Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.
[5] [5] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and Efficient Key Management in Mobile Ad Hoc Networks,” Proc. IEEE Int’l Parallel and Distributed Processing Symp. (IPDPS), 2005.
[6] [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] [7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength,” Proc. IEEE INFOCOM, Apr. 2008
[8] J. Yang, Y. Chen, and W. Trappe, “Detecting spoofing attacks in mobile wireless environments,” in Proc. IEEE SECON, 2009.
[9] J. Wright, “Detecting wireless LAN MAC address spoofing,” 2003, technical document. [Online]. Available: http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf
[10] NS2 Tutorial http://www.isi.edu/nsnam/ns

