International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 5, Sep – Oct 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Detection and Localization of Multiple Spoofing Attackers Using Power Levels

Nagabhushan Hiremath[1] , Amruta H V[2]

[1]Computer Science, Sheshadripuram Degree College, Tumkur
[2]Computer Science, Bangalore

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 detecting spoofing attack;determining the number of attackers when multiple adversaries masquerading as the same node identity; and 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 multiclass detection problem. Cluster-based mechanisms are developed to determine the number of 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 percent Hit Rate and Precision when determining the number of attackers.

Keywords: Wireless network security, spoofing attack, attack detection, localization.

I. INTRODUCTION

Due to the openness of the wireless transmission medium, adversaries can monitor any amount of transmission. Further, adversaries can easily purchase low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with little effort. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. For instance, in an 802.11 network, it is easy for an attacker to collect 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), WiFi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames—an attacker can still spoof management to cause significant impact on networks. Spoofing attacks can further facilitate a variety of traffic injection attacks [1], [2], such as attacks on access control lists, rogue access point (AP) attacks and denial of-service (DoS) attacks. A broad survey of possible spoofing attacks can be found in [3], [4]. 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 [5], [6]. 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. In this work, we propose to use received signal strength (RSS)-based spatial correlation, a physical property associated with each

wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Since we are concerned with attackers who have different locations than legitimate wireless nodes, utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries.

II. RELATED WORK

The works related to problem are outlined as follows:

Recently, security has become a hot research topic in mobile ad hoc networks. Several secure routing protocols have been proposed in the literature. SEAD (Hu et al., 2002), and SAODV (Zapata, 2002) address security attacks in routing protocols and propose different means to counter particular threats. However, almost all of them rely on the existence of a public-key management system.

Luo and Lu (2004) proposed a localized key management scheme called URSA. In their scheme all nodes are servers. The advantage of this scheme is the efficiency and secrecy of local communication as well as system availability; on the other hand, it reduces system security, especially when nodes are not well protected physically. One problem is that when the threshold k is much larger than the network degree d, nodes will have to keep moving to get their certificates updated. The second critical issue is convergence in the share updating phase. Another critical issue is that too much off-line configuration is required before accessing the networks.

G. Zhou, T. He, S. Krishnamurthy, and J.A. Stankovic (2006) In this paper, we investigate the impact of radio irregularity on wireless sensor networks. Radio irregularity is a common phenomenon which arises from multiple factors, such as variance in RF sending power and different path losses depending on the direction of propagation. From our experiments, we discover that the variance in received signal strength is largely random; however, it exhibits a continuous change with incremental changes in direction.

Data sharing is required in most academic research but is not ubiquitous. Most funding agencies, institutions, and publication venues have policies regarding data sharing ecause transparency and openness are considered by many to be part of the scientific method. A number of funding agencies and science journals require authors of peer-reviewed papers to share any supplemental information (raw data, statistical methods or source code) necessary to audit or reproduce published research. A great deal of scientific research is not subject to data sharing requirements, and many of these policies have liberal exceptions. In addition, in certain situations agencies and institutions prohibit or severely limit data sharing to protect proprietary interests, national security, and patient/victim confidentiality.
Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell(2008)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.

III. OVERVIEW OF TECHNIQUES

1. **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.
2. **Determining the number of attackers**
   In accurate 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.
3. **IDOL: Integrated detection and localization framework**

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

multiple adversaries.

4. **Data flow diagram**

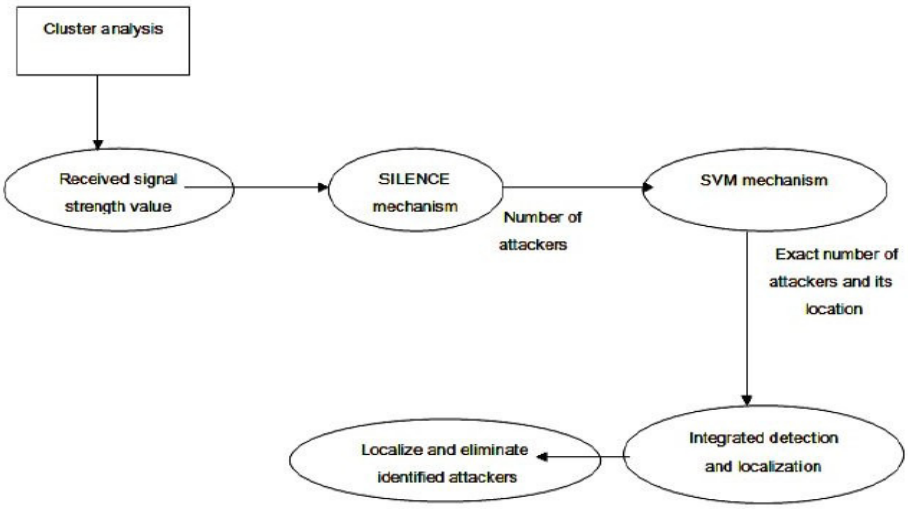

Fig 1: Data Flow Diagram

IV. PROPOSED SYSTEM

The proposed system uses received signal strength (RSS)-based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Since the concern is on the attackers who have different locations than legitimate wireless nodes, utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. An added advantage of employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves.

V. ALGORITHMS

In order to evaluate the generality of IDOL for localizing adversaries, 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) are chosen.

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.

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 vectors. ABP then computes the probability of the wireless device being at each tile Li, with i = 1...L, on the floor using Bayes' Rule,

$$P(L_i|s) = P(s|L_i) * p(L_i) / P(s)$$

be at exactly one tile satisfying $\sum_{i=1}^{L} P(Li|s) = 1$

Given that the wireless node must
probability and returns the most likely tiles/grids up to its confidence α.

ABP normalizes the

Bayesian Networks (BN):

BN localization is a multi lateration 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 = b0i+b1i logDi, where b0i, b1i are the parameters specific to the ith landmark.

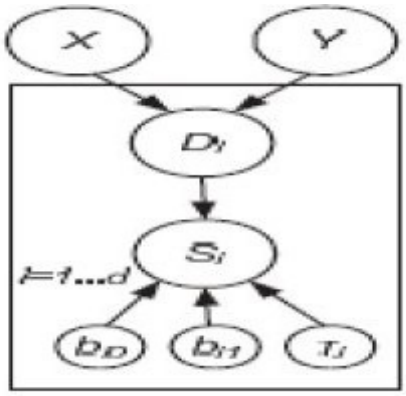

Figure 2 Bayesian graphical model in our study

VI. CONCLUSION

This work, 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. This approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that any number of attackers can be localized and can eliminate them. Determining the number of adversaries is a particularly challenging problem. This paper uses 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, Support Vector Machines (SVM) based mechanism is used to further improve the accuracy of determining the number of attackers present in the system.

REFERENCES

[1] Jie Yang, Yingying Chen, and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" in IEEE 2012.

[2] 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.
[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] 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.
[5] Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in *Proc. IEEE SECON*, 2006.
[6] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in *Proc. IEEE IPDPS*, 2005.
[7] 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.
[8] 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.
[9] J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in *Proc. IEEE SECON*, 2009.
[10] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wirelss spoofing attacks," in *Proc. IEEE SECON*, May 2007.
[11] 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.
[12] V.Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures".
[13] P.Bahl and V.N.Padmanabhan, "RADAr: An in-Building RF-Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.
[14] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc.IEEE INFOCOM, Apr.2007
[15] L.Sang and A.Arora, "Spatial Signatures for Lightweight Security in wireless Sensor Networks",Proc. IEEE INFOCOM, pp.2137-2145,2008.

