IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. V (May-Jun. 2014), PP 61-65
www.iosrjournals.org

A Study of Various Spoofing Attacks and Attackers in Wireless Networks.

Miss.Shweta[1], Asst. Prof Bhavana.S[2], Asst. Prof Shailaja Shastri[3]
[1] *Department of Computer Science and Engineering, VTU PG Center, Gulbarga, Karnataka, India*
[2]*Department of Computer Science and Engineering, VTU PG Center, Gulbarga, Karnataka, India*
[3]*Department of Computer Science and Engineering, Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, 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 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 work 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.

Yi and Kravets (2004) provided a composite trust model. In their scheme they combine the central trust and the fully distributed trust models. This scheme takes advantage of the positive aspects of two different trust systems. Actually, it is a compromise between security and flexibility. Some authentication metrics, such as confidence value, are introduced in order to glue two trust systems..

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.

F. Ferreri, M. Bernaschi, and L. Valcamonici(2004), The Distributed Denial-of-Service (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets. In this paper, we propose an interdomain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers

III. Proposed system

The proposed work deals with implementation of

- The proposed system used Inter domain packet filter architecture, a system that can be constructed solely based on the locally exchange 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 the 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.

Techniques used to improve the performance:

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

As we do not know 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 system

In this section we present our integrated system that can both detect spoofing attacks, determine the number of attackers, and localize multiple adversaries. The experimental results are presented to evaluate the effectiveness of our approach, especially when attackers using different transmission power levels.

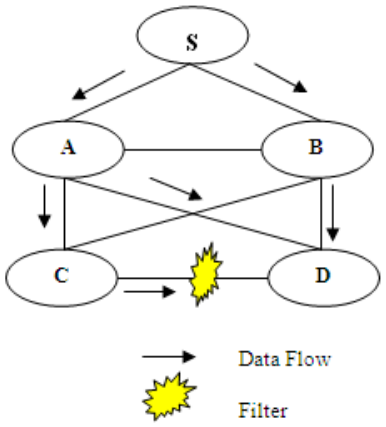
A Path Identification Mechanism from source to destination

Constructing Routing Table:

Each node maintaining routing table which contain the information about the neighbor node. In wireless networks classes that provide automatic reconfiguration, adjusting power levels and channel assignments to optimize coverage while minimizing contention between neighbors.

Finding feasible path:

In this module we are find out the feasible path for the corresponding destination. For that first we find out the possible path. To find out the possible path we are using the BGP(Border Gateway protocol).Each has the address of neighboring node address. The communication between the node as shown below in fig 1.1



- Sending packet from source S to D

Fig 1.1. Data Flow Diagram

Constructing Inter-Domain Packet Filters:

In this module we design the interdomain packet filter. Each and every node has packet filter .it takes the possible path as input. The destination node act as interdomain packet filter. The filter knows what is the feasible path .it segregate what is valid packet and what is spoofed packet.

Receiving the valid packets:

After filtering the invalid packets all the valid packets will reaches the destination.The transmission power levels when performing spoofing[8] attacks so that the localization system cannot estimate its location accurately. Detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 98% and determining the number of network.

IV. Algorithms

In order to evaluate the location, we have chosen a set of representative localization algorithms such as signal space-RADAR to probability-based- Area-Based Probability to multiple -Bayesian Networks.

RADAR-Gridded: It is the algorithm used for 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): It utilizes an interpolated signal map . Further, the experimental area is divided into a regular grid of equal size. ABP assumes the distribution of RSS for 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, using
Bayes' rule:

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

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

Bayesian Networks: It is the algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization. Figure1.3 shows the basic Bayesian Network used. 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 $si = b_{0i}+b_{1i}$ logDi, where b_{0i}, b_{1i} are the parameters specific to the ith landmark.

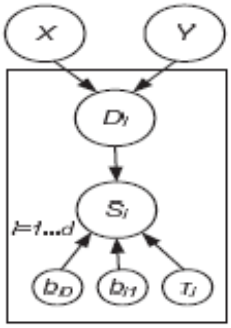


Fig 1.2. Bayesian graphical model

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). The network models noise and outliers by modeling the s_i as a Gaussian distribution around the above propagation model, with variance τi: $si \sim N(b_{0i}+b_{1i}\ \text{logDi}, \tau_i)$,BN returns the sampling distribution of the possible location of X and Y.

V. 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 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, 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, is 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 test-beds through both an 802.11network (Wi-Fi) and an 802.15.4 (Zig-Bee) 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 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]. 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.