Detecting, Determining and Localizing Multiple Spoofing Attackers in Wireless Networks

D. Srikala [1], Siva Reddy [2]

[1] M.Tech, Global College of Engineering & Technology, Kadapa, Andhra Pradesh, India.

[2]M.Tech, Assistant Professor, Global College of Engineering & Technology, Kadapa, Andhra Pradesh, 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, I 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 the same node identity; and 3) localizing multiple adversaries. I propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. I 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. When the training data are available, 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. I 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 100 percent 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— Wireless network security, spoofing attack, attack detection, localization.

Manuscript received August, 2014. ***D. Srikala****, Student of M.Tech, Global College of Engineering & Technology, Kadapa, Andhra Pradesh, India. Email:mvpriya910@gmail.com*

Siva Reddy*, Assistant Professor, Global College of Engineering & Technology, Kadapa, Andhra Pradesh, India. Email: venkatasiva.cme@gmail.com*

I. INTRODUCTION

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing and eliminate them from the network. The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational poIr

associated with distributing, and maintaining cryptographic keys. Due to the limited poIr 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. In this paper, I take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, I propose a scheme for both detecting spoofing attacks, as Ill as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes. By analyzing the RSS from each MAC address using K-means cluster algorithm, I have found that the distance betIen the centroids in signal space is a good test statistic for effective attack detection. I then describe how I integrated our K-means spoofing detector into real-time indoor localization system. Our K-means approach is general in that it can be applied to almost all RSS-based localization algorithms. For two sample algorithms, I show that using the centroids of the clusters in signal space as the input to the localization system, the positions of the attackers can be localized with the same relative estimation errors as under normal conditions. To evaluate the effectiveness of ur spoofing detector and attack localizer, I conducted experiments using both an 802.11 network as Ill as an 2.15.4 network in a real office building environment. In particular, I have built an indoor localization system that can localize any transmitting devices on the floor in real-time. I evaluated the performance of the K-means spoofing detector using detection rates and receiver operating characteristic curve. I have found that our spoofing detector is highly effective with over 95% detection ratesand under 5% false positive rates. Further, I observed that, when using the centroids in signal space, a broad family of localization algorithms achieves the same performance as when they use the averaged RSS in traditional localization attempts.

II. SCOPE OF THE PAPER

The scope of this paper is to detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries. The transmitted information from server is send to client in secure manner. If an intruder comes during transaction server discover and localize that specific system.

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

Formulate the problem of determining the number of attackers as a multiclass detection. Preside over a secure and efficient key management framework that builds a public key infrastructure by applying a secret sharing scheme and an underlying multicast server group. Cluster-based mechanisms are developed to determine the number of attackers. Explore using the support vector machines method to further improve the accuracy of determining the number of attackers. By utilizing physical properties associated with transmission to combat attacks in networks. Determining the number of attackers when there are multiple adversaries collaborating to use the same identity to launch malicious attacks. This approach can accurately localize multiple adversaries. In this paper, I take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, I propose a scheme for both detecting spoofing attacks, as Ill as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes.

V. PROPOSED METHODOLOGY

1) Detecting spoofing attacks.

2) Determining the number of attackers when multiple adversaries masquerading as the same node identity and

3) Localizing multiple adversaries.

VI. WORKING OF RSS

By analyzing the RSS from each MAC address using K-means cluster algorithm, I have found that the distance between the centroids in signal space is a good test statistic for effective attack detection. I then describe how I integrated our K-means spoofing detector into a real-time indoor localization system. Our K-means approach is general in that it can be applied to almost all RSS-based localization algorithms. For two sample algorithms, I show that using the centroids of the clusters in signal space as the input to the localization system, the positions of the attackers can be localized with the same relative estimation errors as under normal conditions.

VII. RELATED WORKS

The traditional approach to prevent spoofing attacks is to use cryptographic-based authentication. Wu et al. have introduced a secure and efficient key management (SEKM) framework. SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. Wool implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. An authentication framework for hierarchical, ad hoc sensor networks is proposed. However, the crypto-graphic authentication may not be always applicable because of the limited resources on wireless devices and lacking of a fixed key management infrastructure in the wireless network.

Recently, new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed. Based on the fact that wireless channel response decorrelates 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. Brik et al. 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. Li

and Trappe 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 to perform 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 works using RSS to defend against spoofing attacks are most closely related to us. Faria and Cheriton proposed the use of matching rules of signal prints for spoofing detection. Sheng et al. modeled the RSS readings using a Gaussian mixture model. Sang and Arora proposed to use 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.

Turning to studying localization techniques, in spite of its several meter-level accuracy, using RSS is an attractive approach because it can reuse the existing wireless infrastructure and is highly correlated with physical locations. Dealing with ranging methodology, range-based algorithms involve distance estimation to land-marks using the measurement of various physical properties such as RSS, Time Of Arrival (TOA), Time Difference Of Arrival (TDOA), and direction of arrival (DoA). Whereas range-free algorithms use coarser metrics to place bounds on candidate positions. Another method of classification describes the strategy used to map a node to a location. Lateration approaches use distances to landmarks, while angulation uses the angles from landmarks. Scene matching strategies use a function that maps observed radio properties to locations on a preconstructed signal map or database. Further, Chen et al. proposed to perform detection of attacks on wireless localization and Yang et al. proposed to use the direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. In this work, I choose a group of algorithms employing RSS to perform the task of localizing multiple attackers and evaluate their performance in terms of localization accuracy.

Our work differs from the previous study in that I use the spatial information to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore, our work is novel because none of the exiting work can determine the number of attackers when there are multiple adversaries masquerading as the same identity. Additionally, our approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

VIII. LITERATURE SURVEY

The convenience of 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols This paper provides an experimental analysis of such 802.11-specific attacks their practicality, their efficacy and potential low-overhead implementation changes to mitigate the underlying vulnerabilities.

2) 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.

3) 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 indentured by its signal print, a topple 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. Moreover, using measurements in a tested network, we demonstrate that signal prints are strongly correlated with the physical location of clients, with similar values found mostly in close proximity. By tagging suspicious packets with their corresponding signal prints, the network is able to robustly identify each transmitter independently of packet contents, allowing detection of large class of identity-based attacks with high probability.

4) Secure and Efficient Key Management in Mobile Ad Hoc Networks :

In mobile ad hoc networks, due to unreliable wireless media, host mobility and lack of infrastructure, providing secure communications is a big challenge. Usually, cryptographic techniques are used for secure communications in wired and wireless networks. Symmetric and asymmetric cryptography have their advantages and disadvantages. In fact, any cryptographic means is ineffective if its key management is weak. Key management is also a central aspect for security in mobile ad hoc networks. In mobile ad hoc networks, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. We propose a secure and efficient key management (SEKM) framework for mobile ad hoc networks. SEKM builds a public key infrastructure (PKI) by applying a secret sharing scheme and using an underlying multi-cast server groups. We give detailed information on the formation and maintenance of the server groups. In SEKM, each server group creates a view of the corticated authority (CA) and provides corticated update service for all nodes, including the servers themselves. A ticket scheme is introduced for efficient corticated service. In addition, an efficient server group updating scheme is proposed. The performance of SEKM is evaluated through simulation.

5) Nightlight Key Management for IEEE 802.11 Wireless Lanes With Key Refresh and Host Revocation :

The IEEE 802.11 Wireless LAN standard has been designed with very limited key management capabilities, using up to 4 static, long term, keys, shared by all the stations on the LAN. This design makes it quite difficult to fully revoke access from previously-authorized hosts. A host is fully revoked when it can no longer eavesdrop and decrypt traffic generated by other hosts on the wireless LAN. This paper proposes WEP∗, a right weight solution to the host-revocation problem. The key management in WEP∗ is in the style of pay-TV systems: The Access Point periodically generates new keys, and

these keys are transferred to the hosts at authentication time. The fact that the keys are only valid for one re-key period makes host revocation possible, and scalable: A revoked host will simply not receive the new keys. Clearly, WEP∗ is not an ideal solution, and does not address all the security problems that IEEE 802.11 suffers from. However, what makes WEP∗ worthwhile is that it is 100% compatible with the existing standard. And, unlike other solutions, WEP∗ does not rely on external authentication servers. Therefore, WEP∗ is suitable for use even in the most basic IEEE 802.11 LAN configurations, such as those deployed in small or home offices. A WEP∗ prototype has been partially implemented using free, open-source tools.

6) 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. Through experiments from an office building environment, we show that DEMOTE achieves accurate attack detection both in signal space as well as in physical space using localization and is generic across different technologies including IEEE 802.11 b/g and IEEE 802.15.4.

7) 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. We first propose an attack detector for wireless spoofing that utilizes K-means cluster analysis. Next, we describe how we integrated our attack detector into a real-time indoor localization system, which is also capable of localizing the positions of the attackers. We then show that the positions of the attackers can be localized using either area-based or point-based localization algorithms with the same relative errors as in the normal case. We have evaluated our methods through experimentation using both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network. Our results show that it is possible to detect wireless spoofing with both a high detection rate and a low false positive rate, thereby providing strong evidence of the effectiveness of the K-means spoofing detector as well as the attack localizer.

8) An Authentication Framework for Hierarchical Ad Hoc Sensor Networks :

Hierarchical architectures are more and more widely adopted for organizing wireless sensor networks. In such architectures, middle-tier nodes take important roles, and preventing a malicious node from impersonating a

middle-tier node and injecting falsified messages becomes critical. In this paper, we propose an energy efficient, distributed scheme to secure the multicast messages from the middle-tier nodes. Our scheme does not require a priori knowledge about the hierarchical relation between middle-tier nodes and lowest-tier nodes, and is adaptive to changes of this relation. Extensive simulations are conducted to evaluate our scheme, and the results show that the scheme is energy efficient.

9) Wireless Device Identification with Radiometric Signatures :

We design, implement, and evaluate a technique to identify the source network interface card (NIC) of an IEEE 802.11 frame through passive radio-frequency analysis. This technique, called PARADIS, leverages minute imperfections of transmitter hardware that are acquired at manufacture and are present even in otherwise identical NICs. These imperfections are transmitter-septic and manifest themselves as artifacts of the emitted signals. In PARADIS, we measure differentiating artifacts of individual wireless frames in the modulation domain, apply suitable machine-learning classification tools to achieve significantly higher degrees of NIC identification accuracy than prior best known schemes. We experimentally demonstrate effectiveness of PARADIS in differentiating between more than 130 identical 802.11 NICs with accuracy in excess of 99%. Our results also show that the accuracy of PARADIS is resilient against ambient noise and fluctuations of the wireless channel. Although our implementation deals exclusively with IEEE 802.11, the approach itself is general and will work with any digital modulation scheme.

10) Number-Based MAC Address Spoof Detection :

The exponential growth in the deployment of IEEE 802.11 based wireless LAN (WLAN) in enterprises and homes makes WLAN an attractive target for attackers. Attacks that exploit vulnerabilities at the IP layer or above can be readily addressed by intrusion detection systems designed for wired networks. However, attacks exploiting link-layer protocol vulnerabilities require a deferent set of intrusion detection mechanism. Most link-layer attacks in WLANs are denial of service attacks and work by spoofing either access points (APs) or wireless stations. Spoofing is possible because the IEEE 802.11 standard does not provide per-frame source authentication, but can be effectively prevented if a proper authentication is added into the standard. Unfortunately, it is unlikely that commercial WLANs will support link-layer source authentication that covers both management and control frames in the near future. Even if it is available in next-generation WLANs equipments, it cannot protect the large installed base of legacy WLAN devices. This paper proposes an algorithm to detect spoofing by leveraging the sequence number field in the link-layer header of IEEE 802.11 frames, and demonstrates how it can detect various spoofing without modifying the APs or wireless stations. The false positive rate of the proposed algorithm is zero, and the false negative rate is close to zero. In the worst case, the proposed algorithm can detect a spoofing activity, even though it can only detect some but not all spoofed frames.

IX CONCLUSION

In this work, I 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. I provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. I derived the test statistic based on the cluster analysis of RSS readings. Our approach can both detect the presence

of attacks as Ill as determine the number of adversaries, spoofing the same node identity, so that I can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. I 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, I 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 poIr 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) 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) D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signal prints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

4) 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.

5) A. Wool, "Nightlight Key Management for IEEE 802.11 Wireless Lanes With Key Refresh and Host Revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.

6) J. Yang, Y. Chen, and W. Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.

7) Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

8) M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

9) V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008.

10) F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

11) L. Sang and A. Arora, "Spatial Signatures for Nightlight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.

12) P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

13) T. Roos, P. Myllymaki, H.Tirri, P. Misikangas, and J. Sievanen, "A probabilistic approach to WLAN user location estimation," +International Journal of Wireless Information Networks, vol. 9, no. 3, pp. 155–164, July 2002.