Spoofing Attack Detection and Localization of Multiple Adversaries in Wireless Networks

S. Bhava Dharani, P. Kumar
Department of Computer Science and Engineering,
Nandha College of Technology, Erode, Tamilnadu, India

ABSTRACT

In wireless networks, Spoofing attacks are easy to launch but it degrades the performance of the networks. To identity an attacker node, it can be verified through cryptographic authentication, authentication is always not possible because it requires key management and additional infrastructural overhead. The proposed approach is used for 1) Detecting spoofing attacks 2) Determining the number of attackers when multiple adversaries masquerading the same node identity and 3) Localizing multiple adversaries. The proposed system uses spatial correlation of received signal strength (RSS) to detect the spoofing attacks. Cluster-based mechanisms are introduced to determine the number of attackers. In this paper, K-Nearest-Neighbor classifier (KNN) is proposed to improve the performance of determining the number of attacks. Finally, An Integrated Detection and Localization system is used to localize the positions of multiple attackers.

KEYWORDS: *Wireless network security, Spoofing attack, KNN, Localization*

I. INTRODUCTION

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. Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. 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. Among various types of attacks, spoofing attacks are especially easy to launch but it degrades its network performance.

Due to the openness of wireless networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device and creates multiple illegitimate identities. Spoofing is when an attacker pretends to be someone else in order gain access to restricted resources or steal information. An attacker can impersonate the Internet Protocol (IP) address of a legitimate user in order to get into their accounts. Spoofing attacker may send fraudulent emails and set up fake websites in order to capture user's login names, passwords, and account information. Another type of spoofing involves setting up a fake wireless access point and tricking victims into connecting to them through the illegitimate connection. Different spoofing attacks such as IP spoofing, E-mail spoofing and ARP spoofing, used to leverage. Man-in-the middle attacks against hosts on a computer network. For example IP spoofing is shown in Fig 1.

Attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message. The header of each IP packet contains the numerical source and destination address of the packet. The address where the packet was sent from is the source address. The header which can be forged, contains a different address, an attacker can make it appear that the packet was sent by a different machine. The traditional approaches to address spoofing attacks are to apply cryptographic authentication. However, cryptographic 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, it is not

always possible to deploy authentication. Thus, it is desirable to detect the presence of spoofing attacks and eliminate them from the network.

In this paper, we take different approaches by using the physical properties associated with wireless transmissions to detect spoofing. Detecting spoofing attacks and as well as localizing the positions of the adversaries performing the attacks, different schemes are used. In exiting system, matching rules of signal prints are used for spoofing detection. K-means cluster analysis to detect spoofing attacks. However, none of these schemes have the ability to determine the number of attackers when multiple adversaries use the same identity to launch attacks, which is the basis to localize multiple adversaries after attack detection. Existing approaches can only handle the case of a single spoofing attacker and cannot localize the attacker if the adversary uses different transmission power levels.

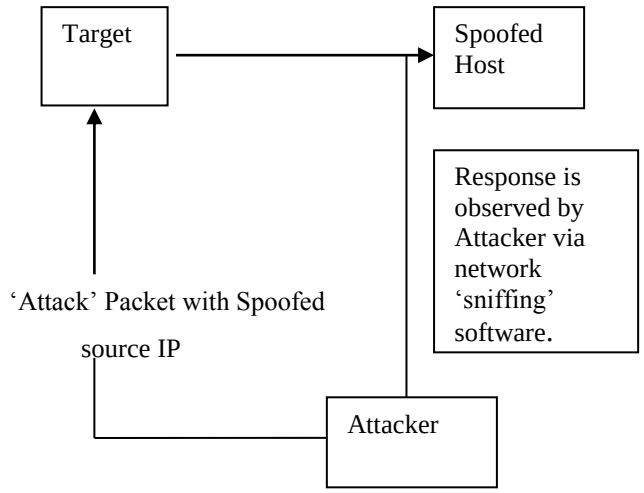

Figure 1. IP Spoofing

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. Employing Received Signal Strength (RSS) as a means to detect spoofing attacker will not require any additional cost to the wireless devices. They will merely use their existing communication methods, while the wireless network will use a collection of base stations to monitor received signal strength for the potential of spoofing. Since we are concerned with attackers who have different locations than legitimate wireless nodes, that utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries.

After detecting the spoofing attack we have to determine the number of attackers. To improve the performance of determining the number of attacks K-Nearest-neighbor classifier (KNN) are proposed. In exiting system Support Vector Machines (SVM) method are used. Compared to SVM, KNN is very simple and well understood. KNN classifiers can achieve good overall performance and are much faster than SVM to use. Indeed, the cost to train SVM for large-scale network is a clear drawback. Hence we are using KNN classifiers to improve the performance of determining the number of attacks If the spoofing attacks are determined to be present by the spoofing attack detector, we want to localize the multiple adversaries and further to eliminate the spoofing attackers from the network. Simulations are conducted to evaluate the performance of proposed work in terms of entropy variation and strength of attacks. Evaluate the effectiveness and efficiency of the proposed K-Nearest-Neighbor classifiers Attacks Detection and SVM. Based on the comparison and the results from the experiment shows that the proposed approach works better than the existing systems.

The rest of the paper is organized as follows. We place our work in the context of related research in Section 2.We describe the proposed system model in Section 3. We evaluate the performance analysis in Section 4. Finally, we conclude our work in Section 5.

II. RELATED WORK

Sheng et al (2008) presented approach, received signal strength (RSS) to distinguish wireless devices for spoofing detection. Initially, the signal strength of a received frame is measured at the receiver's

antenna. The attacker is from its victim, their RSS patterns differ significantly. It is difficult to detect spoofing attack. Since an attacker can manipulate its transmission power with a dense array of AMs, to mimic the RSS pattern of the victim to one AM and also it is inherently difficult to fool the majority of these AMs which have different radio environment. It represents the readings of received Signal Strength for any given transmitter/AM pair as a Gaussian Mixture Models (GMM). A RSS profiling algorithm based on the Expectation-Maximization (EM) learning algorithm for GMMs. The RSS profile is once established for a transmitter in normal conditions, any significant differences in the RSS patterns is considered as a potential spoofing attack. MAC spoofing is using "air monitors" (AMs) and these devices are used to passively sniff wireless traffic, without cooperation from access points (APs) or client stations.

Wu et al (2005) presented a secure and efficient key management (SEKM) framework. It builds a Public Key Infrastructure (PKI) by applying a secret sharing approach and an underlying multicast server group. In SEKM, the server cluster creates a certification authority (CA) view and it provides certificate update service for all nodes, together with the servers themselves. A ticket based scheme is introduced for efficient certificate service. Additionally, an efficient server cluster updating scheme is introduced. In fact, any cryptologic means that is ineffective if the key management is weak. Key management could be a central side for security in networks.

Arora et al (2008) proposed to use the node's "spatial signature," together with Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) to authenticate messages in wireless networks. However, none of these techniques are capable of determining the number of attackers when there are multiple adversaries collaborating to use the same identity to launch malicious attacks and also does not have the ability to localize the positions of the adversaries after attack detection.

Li et al (2006) introduced a security layer which used forge-resistant relationships for detecting spoofing attacks based on the packet traffic together with traffic pattern. The MAC sequence number has also been used to perform spoofing detection. The sequence number and the traffic pattern, these both can be manipulated by an adversary as long as the adversary learns the traffic pattern under normal conditions.

Brik et al (2008) focused on building fingerprints of Wireless LAN by extracting radiometric signatures like frequency magnitude; I/Q origin offset and phase errors, to defend against attacks. Further there is overhead associated with wireless channel response and radiometric signature extraction in wireless networks.

Xiao (2007) proposed approaches which utilized physical properties associated with wireless transmission to combat attacks in wireless networks. Based on the fact that, in space, wireless channel response decorrelates quite rapidly, a channel-based authentication scheme was proposed to discriminate between transmitters at different locations and thus to detect spoofing attacks in wireless networks.

Jie Yang et al (2013) proposed Support Vector Machines (SVM) to classify the number of the spoofing attackers. Using SVM is that it can combine the intermediate results (i.e., features) from different statistic methods to build a model based on training data to predict the number of adversaries. Particularly, SVM is a set of kernel-based learning methods for data classification that involves a training phase and a testing phase. Each data instance in the training set consists of a target value (i.e., class label) and several attributes (i.e., features). But when we used SVM method to classify the number of the spoofing attackers, the performance is not good and also it requires additional cost for large-scale network.

III. SYSTEM MODEL

3.1 Received signal strength based spatial correlation

Spoofing detection is to devise strategies that use the uniqueness of spatial information, but not using the location directly because the attacker's positions are unknown. RSS is a property closely correlated with location in physical space and is readily available in the wireless network. Even though it was affected by random noise, multipath effects, and environmental bias, received signal strength measured at a set of landmarks reference points with known locations is closely associated with the transmitter's physical location and is governed by the distance to the landmarks. The RSS readings at the different physical location are distinctive, whereas the RSS readings at same locations

in physical space are similar. Thus, the RSS readings present strong spatial correlation characteristics. The RSS value vector as S = {S1, S2…..Sn} where n is the number of landmarks/access points that monitors the RSS of the wireless nodes and know their locations.

3.2 Spoofing Attack Detection and Determining the number of Attackers

To perform spoofing attack detection, the RSS-based spatial correlation inherited from wireless nodes is used. And also the RSS readings from a wireless node may fluctuate and should cluster together. Especially, the RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space, where as the RSS readings from different locations over time should form different clusters in signal space. The PAM technique is a popular iterative descent clustering algorithm.

The PAM technique is more robust in the presence of noise and outliers. Hence the PAM method is more suitable in determining clusters from RSS streams, which may be unreliable and fluctuating over time due to random noise and environmental bias. The number of attackers will cause failure in localizing the multiple adversaries. Since we do not know how many adversaries will use the same node identity to launch spoofing attacks and determining the number of attackers becomes a multiclass detection problem and is similar to determining how many clusters exist in the RSS readings. The minimum distance between two clusters is large indicating that the clusters are from different physical locations. The minimum distance between the returned clusters to make sure the clusters are produced by attackers instead of RSS variations and outliers.

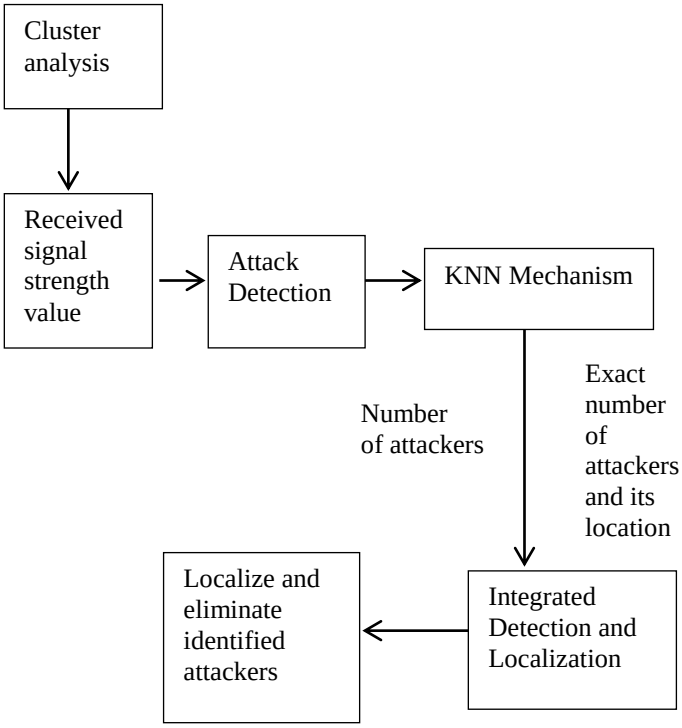

Figure 2. System Model

3.3 K- Nearest-Neighbor classifiers

To improve the performance of determining the number of attackers, K- Nearest Neighbor classifiers (KNN) are used, that are based on learning by analogy. That is, by comparing a given new node with known node that is similar to it. The known node is described by N attributes. Each node represents a point in an N-dimensional space. In this way, the entire known node is stored in an N-dimensional pattern space. When given an unknown node, a k-nearest-neighbor classifier searches the pattern space for the k known node that are closest to the unknown node. This k known node are the k nearest neighbor of the unknown node. For k-nearest-neighbor Classification, the unknown node is assigned the most common class among its k nearest neighbors.

3.4 Integrated Detection and Localization Framework

Integrated systems that can detect spoofing attackers, determine the number of attackers, and localize the multiple adversaries. Especially when attackers using different transmission power levels, traditional localization techniques are based on averaged RSS from each node identity inputs to estimate the position of a node. 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 location. The traditional technique of averaging RSS readings cannot totally differentiate RSS readings from different locations and therefore it is not feasible for localizing adversaries. Different from traditional localization techniques, our integrated detection and localization system utilize the RSS medoids as inputs to localization algorithms to estimate the positions of adversaries. The return positions from our system include the location for estimation of the original node and also the attackers with in the physical space.

IV. PERFORMANCE ANALYSIS

Finally the proposed approaches are illustrated and evaluated to compare the performance of all the approaches. Simulations are conducted to analyze the performance of proposed work in terms of entropy variation and strength of attacks. We evaluate the effectiveness and efficiency of the proposed K- Nearest-Neighbor classifiers and SVM. Based on the comparison and the results from the experiment shows that the proposed approach works better than the existing systems.

V. CONCLUSION

In this work, Received Signal Strength (RSS) can be used to detect the spoofing attack. After detecting the spoofing attack, we have to determine the number of adversaries. Since multiple adversaries can use the same identity node to launch the attack, determining the number of adversaries could be a significantly difficult drawback. We proposed a mechanism K-Nearest-Neighbor classifier that employs the minimum distance testing in addition to cluster analysis to achieve higher accuracy of determining the number of attackers than other methods. Simulations are conducted to analyze the performance of proposed work in terms of entropy variation and strength of attacks. By evaluating the effectiveness and efficiency of the proposed K-Nearest-Neighbor classifiers (KNN) and existing SVM method, based on the comparison and the results from the experiment shows that our proposed approach works better than the existing systems. If the spoofing attacks are determined to be present by the spoofing attack detector, we want to localize the multiple adversaries and further to eliminate the spoofing attackers from the network. Finally**,** we localized the positions of multiple attackers by using an Integrated Detection and Localization system.

REFERENCES

[1] Brik V, Banerjee S, Gruteser M and Oh S,(2008) "Wireless Device Identification with Radiometric Signatures," Proceedings of International Conference on Mobile Computing and Networking, pp.116-127.

[2] Chen Y, Trappe W and Martin R,(2007) "Attack Detection in Wireless Localization," Proceedings of IEEE INFOCOM.

[3] Fabrice Colas and Pavel Brazdi,(2006) "Comparison of SVM and Some Older Classification Algorithms in Text Classification Tasks," ACM/Springer Wireless Networks, Volume 217, pp.169-178.

[4] Jie Yang, Yingying Chen, Wade Trappe and Jerry Cheng,(2013)"Detection and Localization of Multiple Spoofing Attackers in Wireless Networks," IEEE Transactions on Parallel and Distributed systems, Volume. 24.

[5] Li Q and Trappe W,(2006) "Relationship-Based Detection of Spoofing - Related Anomalous Traffic in Ad Hoc Networks", IEEE Communication Social Conference on Sensor, Mesh and Ad Hoc Communication and Networks (SECON).

[6] Sang L and Arora A,(2008) "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proceedings of IEEE INFOCOM, pp. 2137- 2145, 2008.

[7] Sheng Y, Chen G, Kotz D and Campbell A,(2008)"Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proceedings of IEEE INFOCOM.

[8] Wool A,(2005)"Lightweight Key Management for IEEE 802.11 Wireless Lan with Key Refresh and Host Revocation," Springer Wireless Networks, volume 11, no. 6, pp. 677-686.

[9] Wu B, Fernandez E and Magliveras S,(2005) "Secure and Efficient Key Management in Mobile Ad Hoc Networks," IEEE International Parallel and Distributed Processing Symposium (IPDPS).

[10] Xiao L and Trappe W, (2007) "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Proceedings of IEEE International Conference on Communications (ICC), pp. 4646-4651.

[11] Yang J, Chen Y and Trappe W, (2009) "Detecting Spoofing Attacks in Mobile Wireless Environment," Proceedings of IEEE Communication Social Conference on Sensor, Mesh and Ad Hoc Communication and Networks (SECON).