International Journal of scientific research and management
(IJSRM) ||Volume||2||Issue||4 ||Pages|| 773-777 ||2013||
Website: www.ijsrm.in ISSN (e): 2321-3418

Localization of Multiple Spoofing attackers at different power levels in wireless networks

Madana Chitran.R[1], Muthuraj.S[2]

[1]Gnanamani College of Technology, Department of Computer Science and Engineering,
Namakkal 637018, India
madan2k4@gmail.com

[2]Gnanamani College of Technology, Department of Computer Science and Engineering,
Namakkal 637018, India
muthuraj027@gmail.com

Abstract: The performance of networks can be impact due to attackers in wireless networks. In wireless networks easy to attack and hack the data. We must to prevent or stop wireless network from the attackers. Earlier it can identify the attackers using spatial correlation of received signal strength from wireless nodes, determine the number of attackers using support vector machines for single adversaries, and it can identify the location for single adversaries. We propose to determine the number of attackers when there are multiple adversaries masquerading as the same identity by using support vector networks, which can achieve higher detection rate and more accuracy compare to previous methods. If adversaries enter any anonymous node to communicate network, that node is identified and filtered. Additionally it can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

Keywords: Spoofing attacks, adversary, DoS, MAC Address

1. Introduction

Our scope is do detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods grounded on RSS-based spatial correlations among normal devices and adversaries and also detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels. In this approaches to address potential spoofing attacks employ cryptographic schemes. 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. 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. 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.

2. Related Work

Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific 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 [1]. Many wireless networks are susceptible to spoofing attacks.

Conventionally, ensuring the identity of the communicator and detecting an adversarial presence is performed via device authentication. Unfortunately, full-scale authentication is not always desirable as it requires key management and more extensive computations. In this paper, we propose non cryptographic mechanisms that are complementary to authentication and can detect device spoofing with little or no dependency on cryptographic keys. We introduce forge-resistant relationships associated with transmitted packets, and forge-resistant consistency checks, which allow other network entities to detect anomalous activity. We then provide several practical examples of forge-resistant relationships for detecting anomalous network activity.

We explore the use of monotonic relationships in the sequence number fields, the use of a supplemental identifier field that evolves in time according to a reverse one-way function chain, and the use of traffic statistics to differentiate between anomalous traffic and congestion [2]. 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 [6].Accurately positioning nodes in wireless and sensor networks is important because the location of sensors is a critical input to many higher-level networking tasks. However, the localization infrastructure can be subjected to non-cryptographic attacks, such as signal attenuation and amplification that cannot be addressed by traditional security services.

We propose several attack detection schemes for wireless localization systems. We first formulate a theoretical foundation for the attack detection problem using statistical significance testing. Next, we define test metrics for two broad localization approaches: multi alteration and signal strength. We then derived both mathematical models and analytic solutions for attack detection for any system that utilizes those approaches [9].

3. Detection System approach

3.1 ATTACK MODEL-GAD

We consider the spoofing nodes to be either mobile or static. When both the victim node and the spoofing node are static, spoofing attacks can be detected by using the techniques in previous works. For detecting the mobility of wireless devices, we can use existing metrics, such as the variance of RSS. Thus it is possible to distinguish the mobile nodes from the static nodes in wireless networks.

We deploy traffic observers or use the access points (APs)

directly that are at fixed locations to record the Received Signal Strength of packets in the network. When a spoofing attack is conducted, we assume that the victim node, whose identity is cloned by the adversary, is also present in the network. In addition, when the attacker is moving around, we assume that the attacker is not moving together with the victim node, which means that the victim node and the spoofing node have different movement patterns. It is a reasonable assumption because it requires bigger efforts for an attacker to move together with the victim node by tracing the victim node in all the time intervals. , if the spoofing device is co-moving with the victim node, the attacker also increases the possibility of exposing itself to the victim node. We note that under the case that the spoofing attack is present in a different network region of the victim node, a high-level domain management server should be able to

detect the attack since the same node identity has appeared in more than one networks.

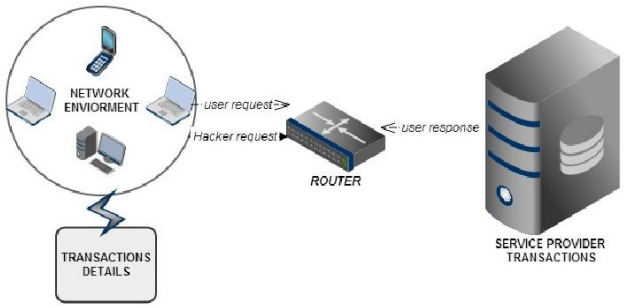

Fig 1 System Design

This algorithm is used statistical characterization of the percentage that the number of attackers can be accurately determined over all possible testing attempts with mixed number of attackers. Associated with a specific number of attackers, i, we define the Hit Rate HR_i as $HR_i = N_{true} / P_i$ Where N_{true} is the true positive detection of class c_i. Let N_{false} be the false detection of the class c_i out of the negative class N_i that do not have i number of attackers. We then define the false positive rate FP_i for a specific number of attackers of class c_i as $FP_i = ¼N_{false} / N_i$. Then, the Precision is defined as $Precision_i = N_{true} / N_{true} + N_{false}$.

3.2 Received Signal Strength

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. We propose to study RSS, a property 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 (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks [17]. 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. We define the RSS value vector as $s = \{s_1, s_2, \ldots s_n\}$ where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their locations.

3.3 Attack Detection

The RSS readings over time from the same physical location will belong to the same cluster points in the n-dimensional signal space, while the RSS readings from different locations over time should form different clusters in signal space. Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node (i.e., spoofing node or victim node). Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space.

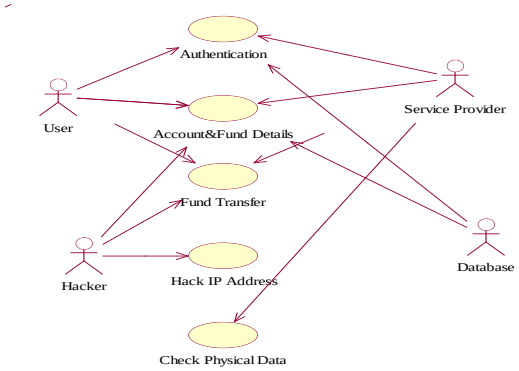

Fig2 Use case diagram

In this work, we utilize the Partitioning Around Medoids Method to perform clustering analysis in RSS. The PAM Method is a popular iterative descent clustering algorithm. Compared to the popular K-means method , The PAM method is more robust in the presence of noise and outliers. determining clusters from RSS streams, which can be unreliable and fluctuating over time due to random noise and environmental bias

4. Experimental Validation

4.1 Different power levels

If a spoofing attacker sends packets at a different transmission power level from the original node, based on our

cluster analysis there will be two distinct RSS clusters in signal space We varied transmission power for an attacker from 15 dBm to 0 dBm. We found that in all cases Dm is larger than normal conditions. When the spoofing attacker used transmission power of 10 dB to send packets, whereas the original node used 15 dB transmission power level. We observed that the curve of Dm under the different transmission power level shifts to the right indicating larger Dm values. Thus, spoofing attacks launched by using different transmission power levels will be detected effectively in GADE.

4.2 Support Vector Machines

Provided the training data collected during the offline training phase, we can further improve the performance of determining the number of spoofing attackers. In addition, given several statistic methods available to detect the number of attackers, such as System Evolution. By using this method we can achieve a higher detection rate.

Table 1
Hit rate, Precision, F-Measure

Attackers	2	3	4
802.11 network Hit rate	99.57	97.51	96.58
802.11 network , Precision	99.28	94.69	84.83
802.11 network F-Measure	99.28	97.98	92.84

In this section, we explore using Support Vector Machines to classify the number of the spoofing attackers. The advantage of 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 accurately predict the number of attackers. Particularly, SVM is a set of kernel-based learning methods for data classification, which 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). For example, for spoofing detection, we can use a target value of "þ1" to label the result if there are two attackers and a value of "_1" to label the result if the number of attackers is not 2. Furthermore, the features can be the difference of the partition energy and merge energy from System Evolution, or the minimum distance between two clusters from SILENCE, or the combination of them. The goal of SVM is to produce a model from the training set to predict the target value of data instances (i.e., the testing data).

CONCLUSION

This system 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 networks. 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. Our approach can 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, 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.

References

[1] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signal prints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[2] Qing Li and Wade Trappe, "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships," IEEE Transactions On Information Forensics And Security, Vol. 2, No. 4, December 2007.

[3] 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.

[4] 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.

[5] 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.

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

[8] 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.

[9] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.

[10] D.Madigan, E. Elnahrawy, R. Martin, W. Ju, P. Krishnan, and A.S. Krishnakumar, "Bayesian Indoor Positioning Systems," Proc. IEEE INFOCOM, pp. 324-331, Mar. 2005.

Author Profile

Madana Chitran .R received the B.E. degree in Computer science and Engineering from Muthayammal Engineering college, Affiliated to Anna University, Chennai, in 2007 He is working towards the M.E degree in Computer Science and Engineering from Gnanamani College of Technology, Affiliated to Anna University, Chennai since September 2012. His research area includes Data Base Management Systems and Computer Networks.

Muthuraj.S received the M.TECH degree in Computer Science and Engineering from Prist University in 2012, Received B.TECH degree in the Information Technology from Kongu Engineering College, Affiliated to Anna University, Chennai in 2006. Now working as Assistant Professor in Gnanamani College of Technology. His research area include Data Base Management Systems