Identity-Based Localization Attacks in Wireless Networks

S.Vinothkumar*
PG Scholar
SNS College of Engineering, Coimbatore
hansumvino@gmail.com

S.Boopathy
Assistant Professor
SNS College of Engineering, Coimbatore
boopathytekh@gmail.com

Abstract- Wireless networks are helpless to identity based attacks, as well as spoofing and Sybil attacks, which allow for many other form of attacks on the networks. Even though the identity of a node can be confirmed through cryptographic authentication, authentication is not always probable, because it require key management and additional infrastructural overhead. A method for detect both spoofing and Sybil attacks by using the similar set of technique. A generalized attack detection model that utilize the spatial correlation of usual signal strength innate from wireless nodes. We provide a theoretical analysis of our approach. We then get the check statistics for detection of identity based attacks by using the *K*-means algorithm. Our bother detector is robust when handling the situations of attackers that use dissimilar transmission power levels to attack the detection scheme. We further depict how we integrated our attack detector into a real time indoor localization system, It can also localize the position of the attackers. The positions of the attackers can be restricted using point based localization algorithms with the same errors as in the normal case. We further evaluated our method through experimentation in two real office buildings using equally an IEEE 802.11 network and an IEEE 802.15.4 network. it is probable to detect wireless identity based attacks with together a high detection rate and a low false positive rate, thereby provide a strong evidence of the success of the attack detector utilizing the spatial correlation of RSS and the attack localizer.

Index Terms- Identity-based attack, localization, received signal strength (RSS), sensor network, spoofing attack, Sybil attack, transmission power, wireless network.

I. INTRODUCTION

As additional Wireless and sensor networks are deployed, they will increasingly turn into tempting target for malicious attacks. Due to the common nature of the wireless medium, attackers can meet useful identity information through passive monitoring and more exploit the identity information to open identity based attacks, the two mainly harmful but simple to launch attacks: 1) spoofing attacks and 2) Sybil attacks. In identity based spoofing attacks, an enemy can forge its identity to pretext as another device or even create several illegitimate identities in the networks. For instance, in an IEEE 802.11, it is very easy for an attacker to adjust its Media Access Control address of network interface card to another device through vendor full NIC drivers or open source NIC drivers. In addition, by masked as an authorized wireless access point or an authorized client, an attacker can open denial-of-service attacks, bypass access control mechanisms, or untruly advertise services to wireless clients.

In Sybil attacks, a Sybil node can fake diverse identities to ruse the network with many fake nodes. The Sybil attack can notably ease the network performance by defeat group based voting technique and fault tolerant schemes. Therefore, identity based attacks will have a grave impact to the normal operation of wireless and sensor networks. It is pleasing to detect the presence of identity based attacks and remove them from the network.

The address identity based attacks is to relate cryptographic authentication. However, authentication requires extra infrastructural overhead and computational power related with distributing and maintain cryptographic keys. The partial power and resources existing to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In this paper, we take a different approach by using the physical properties associated with wireless transmissions to detect identity-based attacks. In particular, we utilize the received signal strength (RSS) measured across a set of land-marks (i.e., reference points with known locations) to perform detection of identity-based attacks. We focus on static nodes, which are common for most identity-based attacks scenarios [4]. Our scheme can detect both spoofing and Sybil attacks by using the same set of techniques and does not add any overhead to the wireless devices and sensor nodes.

We formulate a generalized attack-detection model by using statistical significance testing. We then provide theoretical analysis of exploiting the spatial correlation of the RSS inherited from wireless nodes for attack detection. In our theoretical analysis, we derivative the mathematical relationship among the distance of RSS in signal space and the node distance in physical space. We then residential the analytical expression of the detection rate, false positive rate, and accuracy of seminal whether two nodes live at the same location based on the RSS distance in signal space. In addition, we consequent the optimal threshold that can reduce the detection errors. The theoretical analysis provide both the theoretical support for detect identity based attacks by using the spatial correlation of RSS and the logical results on detection effectiveness.

By examining the clustering things of RSS over time in signal space, we create that the distance among the centroids of clusters resulting by the *K*-means algorithm in signal space is a good quality test sign for effective attack detection. we residential a mechanism called difference of two, which utilize the difference of RSS between landmarks to assist detect Sybil attacks launched by a Sybil node that varies its transmission power levels to ruse the attack detection scheme. Thus, our bother detector is robust to detect identity based attacks that use dissimilar transmission power levels.

Detecting the company of identity based attacks in the network provide first order information to defending beside attackers. learning the physical location of the attackers allow the network administrators to use a wide range of defense strategies. We discover the position of the adversaries by integrating our attack detector into a real time indoor localization system. The cluster analysis based attack detector is not detailed to any RSS based localization algorithms and is thus general. Two kinds of algorithms, area and point-based algorithms, The centroid of the clusters that are return by the attack detector in signal space as the say to the localization system, the positions of the attackers can be local with the similar relative estimation errors as below normal conditions.

To assess the effectiveness of attack detector, we conduct experiments by using equally an IEEE 802.11 network and an IEEE 802.15.4 in two real office house environments. we have build an indoor localization system that can jail any transmitting devices on the floor in real time. We evaluate the act of our attack detector by using a detection rate and receiver operating characteristic curve. The performance of the attack detector is in line with the logical results, suggestive of that our attack detector is highly useful with more than 95 percentage detection rates and less than 5 percentage false positive rates.

when using the centroids of clusters return by the attack detector in signal space, a large family of localization algorithms reach the similar performance as when using the averaged RSS in usual localization attempts. for spoofing attacks, the distance among the local results of the spoofing node and the original node is straight proportional to the true distance among the two nodes, thereby given that strong data of the effectiveness of together our detection scheme and our move toward of localizing the positions of the adversary.

The viability and threats of identity based attacks and their impact. create the detection problem of identity based attacks, offer theoretical analysis of using the spatial correlation of RSS for attack exposure, and plan our cluster analysis based attack detector for equally spoofing and Sybil attacks. Express our evaluation metrics in Section IV and present our experimental methodology. The performance evaluation of detect spoofing and Sybil attacks respectively. We begin the real time localization system and there how we can find the positions of the attackers. Section IX describe the prior research in addressing spoofing and Sybil attacks

II. FEASIBILITY OF ATTACKS

A. Spoofing Attacks

Attackers can collect useful self information during passive monitoring and use the identity information to open identity based spoofing attacks in wireless and sensor networks. For instance, in an 802.11, it is simple for a wireless device to obtain a valid MAC address and pretense as another device. The IEEE 802.11 protocol set provide insufficient identity verification throughout message exchange, counting most control and management frames. The adversary can use this weakness and call for various services as if it were one more user. Identity based spoofing attacks are a grave threat in the network, since they represent a form of identity concession and can ease a series of traffic injection attacks, including spoofing based DoS attacks.

An adversary can open a deauthetication attack. After a client choose an AP for outlook communication, it must authenticate itself to the AP before the communication meeting starts. mutually the client and the AP are allowed to clearly ask for de authentication to Avoid the existing authentication connection with all other. Unfortunately, this deauthentication message is not real. Therefore, an attacker can spoof this deauthentication message, also on behalf of the client [6]. The adversary can tirelessly repeat this attack and completely avoid the client from transmitting or receiving.

An attacker can use identity spoofing and launch the mischief AP attack next to the wireless network. In the scoundrel AP attack, the adversary first sets up a rogue AP with the similar MAC address and service set identifier as the lawful AP but with a stronger signal. When a station enter the reporting of the rogue AP, the evasion network configuration will make the station by design relate with the rogue AP, which has a stronger signal. Then, the enemy can take actions to pressure the communication. For example, it can direct forged traffic to the associated station or drop the needs made by the station. Aside from the basic packet flooding attacks, the adversary can create use of identity spoofing to execute more sophisticated flooding attacks on APs, such as probe request, authentication request, and association request flooding attacks [7].

B. Sybil Attacks

The term *Sybil attack* was signify an attack where the attacker, a Sybil node, tries to forge many identities in the background of peer-to-peer distributed systems. Sybil attacks are particularly simple to launch in wireless sensor networks where the communication standard is open and broadcast. By broadcasting messages with many identifications, a Sybil node can fix the vote on group based decisions and also harshly disrupt network middleware services [9].

By using a single node to near many identities in the network, the Sybil attack can significantly decrease the effectiveness of fault tolerant schemes such as repeated mechanisms [1], distributed storage [2], multipath routing [3], and topology maintenance [10]. The Sybil attack can beat the redundancy mechanisms, storage partitions, and routing algorithms by making the mechanisms consider that they are using many nodes but are, in fact, using a single Sybil node.

The identity based attacks, spoofing and Sybil attacks, will considerably impact the network performance. The conventional approaches to address identity based attacks utilize authentication. The application of authentication require reliable key distribution, maintenance mechanisms. It is not always attractive to apply authentication because of its infrastructural, management overhead. And also, cryptographic method are susceptible to node cooperation, which is a serious anxiety, because most wireless nodes are easily available, allowing their memory to be simply scanned.

It is attractive to use properties that do not need overheads and changes on nodes and cannot be damaged even when nodes are compromised. We use RSS, a property that is linked with the transmission and reception of communication, as the basis for detecting identity based attacks. Employing RSS as a means of detect spoofing and Sybil attacks will not need any additional cost to the wireless devices themselves. they will merely use their offered communication methods, whereas the wireless network will utilize a collection of APs to monitor RSS for the potential of identity based attacks. Our techniques will touch the problem of the unreliable time varying nature of RSS [11]. These technique will also address the issue when an attacker varies its transmission power to open attacks and trick the system.

III. ATTACK DETECTOR

We devise the attack detection problem using significance testing. We then give a theoretical analysis on our RSS based attack detection. We expand the test statistics for attack detection and present the discovery philosophy for spoofing and Sybil attacks.

A. Formulation of Attack Detection

RSS is widely available in deployed wireless communication networks, and its values are intimately correlated with location in physical space. RSS is a ordinary physical property used by a broadly diverse set of localization algorithms [16]. Inspite of its several level localization accuracy, using RSS is an striking approach, because it can reclaim the existing wireless infrastructure, and it is enough to meet the accuracy requirement of most applications. For example, during health care monitoring, a doctor may only need to know in which room the track patient reside. We thus derive an attack detector for identity based attacks by utilize properties of the RSS.

B. Theoretical Analysis of the Spatial Correlation of RSS

Even though artificial by random noise, and multipath effects, the RSS calculated at a set of landmarks is closely linked to the transmitter's physical location and is govern by the distance to the landmarks [17]. The RSS readings at dissimilar locations in physical space are characteristic. Thus, the RSS readings present burly spatial correlation characteristics.

C. Detection Philosopy

1. Detecting Spoofing Attacks

Distance among Wireless Nodes: In a spoofing attack, when a spoofing node is lock to an original node, the resulting test statistic will not be big and may involve the decision of attack detection, whereas in a Sybil attack, when two wireless nodes are lock to each other, a small test statistic will be obtain. This condition may misinform our attack detector to decide the presence of a Sybil attack. The distance among two nodes affect the performance of our attack detector.

IV. EVALUATION OF DETECTING SPOOFING ATTACKS

A. Determining the Threshold of Test Statistics

Based on the analysis, it is key to choose the fitting threshold τ , which will let the attack detector to be healthy to false detections. The thresholds describe the critical region for the significance testing. In our experiments, the entry is obtained through experiential training of the K-means algorithm

B. Detecting Attacks Using Different Transmission Power Levels

If an attacker sends packets at a transmission power level that is dissimilar from the original node with the similar identity, there will be two different RSS clusters in signal space.

C. Detection Results

The estimate of the effectiveness of the attack detector in detecting spoofing attacks.

1) Effectiveness of Attack Detector: The detection rate and false positive rate for both the 802.11 and 802.15.4 networks under dissimilar threshold settings. The results are cheering, showing that for false positive rates less than 5%, the detection rates are more than 95%. Even when the false positive rate goes to zero, the detection rate is still more than 92% for both the 802.11 and 802.15.4 networks.

detection rate and false-positive rate for the 802.11 network when the spoofing attacker varies its transmission power level to launch attacks. In our experiments, the attacker used transmission power of 10 dB to send packets, whereas the original node used 15 dB of transmission power. Compared with Table I, Table II shows that we can achieve a higher detection rate when the

attacker uses different trans-mission power levels. Thus, our attack detector can effectively detect the spoofing attacks that are launched by using different transmission power levels.

V. EVALUATION OF DETECTING SYBIL ATTACKS

A. Determining the Threshold of Test Statistics

Similar to detecting spoofing attacks, the thresholds define the critical region for the significance testing. In detecting Sybil attacks, the thresholds through empirical training for our attack detector. During the offline phase, we collected the RSS readings across a set of locations over the experimental area and obtained the distance between two centroids in signal space for each node

VI. LOCALIZING ADVERSARIES

The identity-based attack is determined to be present by the attack detector, we want to localize the adversaries and to eliminate the attackers from the network. In this section, we present a real-time localization system that can be used to locate the positions of the attackers. We then describe the localization algorithms for estimating the adversaries' position. The experimental results are presented to evaluate the effectiveness of our approach.

A. Localization System

The general-purpose localization system to perform real-time indoor positioning. This system is designed with fully distributed functionality and easy-to-plug-in localization algorithms. It is built around four logical components: 1) Transmitter; 2) Landmark; 3) Server; and 4) Solver.

Transmitter: Any device that transmits packets can be localized. Oftentimes, the application code does not need to be altered on a sensor node to localize it.

Landmark: The Landmark component listens to the packet traffic and extracts the RSS reading for each transmitter. It then forwards the RSS information to the Server component. The Landmark component is stateless and is usually deployed on each landmark or AP with known locations.

Server: A centralized server collects RSS information from all the Landmark components. The identity-based detection is performed at the Server component. The Server component summarizes RSS information such as averaging or clustering and then forwards the information to the Solver component for localization estimation.

Solver: The Solver component takes the input from the Server component, performs the localization task by utilizing the localization algorithms that are plugged in, and returns the localization results back to the Server component.

VII. CONCLUSION

A method for detecting identity-based attacks, including spoofing and Sybil attacks, and localizing the adversaries in wireless and sensor networks. In contrast to traditional identity-oriented authentication methods, our RSS-based approach does not add additional overhead to the wireless devices and sensor nodes. We formulated the identity-based detection problem as a statistical-significance-testing problem. We then provided theoretical analysis of exploiting the spatial correlation of RSS inherited from wireless nodes for attack detection. We further utilized the K-means cluster analysis to derive the test statistic. Our attack detector is robust to detect attacks that are launched by adversaries that use different transmission power levels. In addition, we have built a real-time localization system and integrated our K-means attack detector into the system to locate the positions of the attackers and, as a result, to eliminate the adversaries from the network.

The effectiveness and generality of our attack detector and attacker localizer in both the 802.11 and 802.15.4 networks in two real office building environments. The performance of the K-means attack detector is evaluated in terms of detection rates and ROC curves. Our attack detector has achieved high detection rates, i.e., more than

95%, and low false-positive rates, i.e., less than 5%. Moreover, our DoT mechanism is highly effective in detecting a Sybil attack that uses different transmission power levels.

Locating the positions of the attackers, we have utilized both the point- and area-based algorithms in our real-time localization system. We found that the performance of the system, when localizing the adversaries that use the results of the K-means cluster analysis, are about the same as localizing under normal conditions. In particular, in spoofing attacks, the distance between the spoofing node and the original node can be estimated with a median error of 10 ft. the generic across different localization algorithms and networks. Therefore, our experimental results provide strong evidence of the effectiveness of our approach in detecting identity-based attacks and localizing the positions of the adversaries.

REFERENCES

[1] Q. Zhang, P. Wang, D. Reeves, and P. Ning, “Defending against Sybil attacks in sensor networks,” in Proc. 25th IEEE ICDCSW, Jun. 2005, pp. 185–191.

[2] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in Proc. OSDI, 1999, pp. 173–186.

[3] A. Banerjea, “A taxonomy of dispersity routing schemes for fault-tolerant real-time channels,” in Proc. ECMAST, May 1999, vol. 26, pp. 129–148.

[4] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC-layer spoofing using received signal strength,” in Proc. IEE INFOCOM, Apr. 2008, pp. 1768–1776.

[5] J. Bellardo and S. Savage, “802.11 denial-of-service attacks: Real vulner-abilities and practical solutions,” in Proc. USENIX Security Symp., 2003, pp.15–28.

[6] W. A. Arbaugh, N. Shankar, Y. Wan, and K. Zhang, “Your 802.11 wireless network has no clothes,” IEEE Wireless Commun., vol. 9, no. 6, pp.44–51, Dec. 2002.

[7] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access points vulnerabili-ties to DoS attacks in 802.11 networks,” in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 634–638.

[8] J. R. Douceur, “The Sybil attack,” in Proc. 1st IPTPS, Mar. 2002, pp.251–260.

[9] M. Demirbas and Y. Song, “An RSSI-based scheme for Sybil attack detection in wireless sensor networks,” in Proc. Int. Workshop Adv. Experimental Activities Wireless Netw. Syst., 2006, pp. 564–570.

[10] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, “Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks,” ACM Wireless Netw. J., vol. 8, no. 5, pp. 481–494, Sep. 2002.

[11] G. Zhou, T. He, S. Krishnamurthy, and J. A. Stankovic, “Models and solutions for radio irregularity in wireless sensor networks,” ACM Trans. Sensor Netw., vol. 2, no. 2, pp. 221–262, May 2006.

[12] A. Krishnakumar and P. Krishnan, “On the accuracy of signal-strength-based location estimation techniques,” in Proc. IEEE INFOCOM, Mar. 2005, pp. 642–650.

[13] P. Bahl and V. N. Padmanabhan, “RADAR: An in-building RF-based user location and tracking system,” in Proc. IEEE INFOCOM, Mar. 2000, pp.775–784.

[14] M. Youssef, A. Agrawal, and A. U. Shankar, “WLAN location deter-mination via clustering and probability distributions,” in Proc. 1st IEEE PerCom, Mar. 2003, pp. 143–150.

[15] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R. P. Martin, “The robust-ness of localization algorithms to signal-strength attacks: A comparative study,” in Proc. DCOSS, Jun. 2006, pp. 546–563.

[16] T. Roos, P. Myllymaki, H. Tirri, P. Misikangas, and J. Sievanen, “A probabilistic approach to WLAN user location estimation,” Int. J. Wireless Inf. Netw., vol. 9, no. 3, pp. 155–164, Jul. 2002.

[17] Y. Chen, J. Francisco, W. Trappe, and R. P. Martin, “A practical approach to landmark deployment for indoor localization,” in Proc. 3rd IEEE SECON, Sep. 2006, pp. 365–373.

[18] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, “A survey of various propagation models for mobile communication,” IEEE Antennas Propag. Mag., vol. 45, no. 3, pp. 51–82, Jun. 2003.

[19] A. Goldsmith, Wireless Communications. New York: Cambridge Univ. Press, 2005.

[20] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables. New York: Dover, 1965.