ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

Mitigating Spoofing Attacks through Received Signal Strength in Wireless Networks

J.Saranya ,V.Pugazhenthi

PG Scholar, Dept of CSE, MAM College of Engineering, Trichy, Tamil Nadu, India

Associate professor, Dept of CSE, MAM College of Engineering, Trichy, Tamil Nadu, India

ABSTRACT: Spoofing Attack is one of the vulnerabilities in the networks in which the adversary assumes the identity of another node in the network and to establish a connection that will allow gaining access to the other hosts and their sensitive data. It will decrease the performance of the network and violate many security issues. With the open medium, distributed cooperation and constrained capabilities, the wireless nodes are more vulnerable to such type of attacks compared with wired networks. Even though the identity of a node can be verified through cryptographic mechanisms, the conventional security approaches are not always desirable because it requires key management and additional infrastructural overheads. The detection and localization of multiple attacks makes complex when the multiple number attackers spoofing attacks the mobile ad hoc attacks. In which the RSS and SVM deals with the spoofing attacks, it determines the number of attackers in the wireless network and identify the location of the spoofing attackers. However it localizes the spoofing attackers but it does not consider the legitimate users. After the process of localizing the attackers in the wireless network, the attackers may mitigate from the network without degrading the legitimate users. Observation of the behavior of the neighborhood which is performed by the normal network nodes is one of the common methods for detecting attacks in wireless networks. Local monitoring which also deals with the process of neighborhood analysis in multi hop wireless networks. This can be implemented by UnMASK. In this paper, propose the UnMASK (Utilizing Neighbor Monitoring for Attack Mitigation) that mitigate the multiple spoofing attackers without give distortions to the legitimate users in the networks.UNMASK uses as a fundamental building block the ability of a node to oversee its neighboring nodes' communication. On top of UNMASK, build a secure routing protocol, LSR, that provides additional protection against malicious nodes by supporting multiple node-disjoint paths. From that can analyze the nodes and neighbor node relations by means of communication over them. The experiments those are undergone to produce the results of mitigation of multiple spoofing after the detection and localization process.

KEY WORDS: Wireless network security, neighbor monitoring, secure routing, control attack, data attacks.

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.

Most existing approaches to address potential spoofingattacks employ cryptographic schemes [5], [6].It introduced a secure and efficient key management (SEKM) framework. SEKM builds a Public Key Infrastructure(PKI) by applying a secret sharing scheme and anunderlying multicast server group.The traditional approach to address spoofing attacks is to

ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

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.

Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and further utilize the identity information to launch identity-based attacks, in particular, the two most harmful but easy to launch attacks: 1) spoofing attacks and 2) Sybil attacks. In identity-based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks. For instance, in an IEEE 802.11 network, it is easy for an attacker to modify its Media Access Control (MAC) address of network interface card (NIC) to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless access point (AP) or an authorized client, an attacker can launch denial-of-service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

The works [3], [7], [14] using RSS to defend againstspoofing attacks are most closely related to this system. Received Signal Strength is widely available in deployed wireless communication networks, and its values are closely correlated with location in physical space. In addition, RSS is a common physical property used by a widely diverse set of localization algorithms. In spite of its several-meter-level localization accuracy, using RSS is an attractive approach, because it can reuse the existing wireless infrastructure, and it is sufficient 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 tracked patient resides. 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. The RSS readings at different locations in physical space are distinctive.

This work, choose agroup of algorithms employing RSS to perform the task of localizing multiple attackers and evaluate their performancein terms of localization accuracy. This approach can accurately localize multiple adversaries even when the attackers varying their transmissionpower levels to trick the system of their true locations.

II. RELATED WORK

IEEE 802.11 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. WEP, a lightweight 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. The traditional approach to prevent spoofing attacks is to use cryptographic-based authentication [5], [6], [10]. Recently, new approaches utilizing physical propertiesassociated with wireless transmission to combat attacks inwireless networks have been proposed. Based on the factthat wireless channel response de-correlates quite rapidly inspace, a channel-based authentication scheme was proposed

to discriminate between transmitters at different locations,and thus to detect spoofing attacks in wireless networks [11].Brik et al. [12] focused on building fingerprints of 802.11bWLAN NICs by extracting radiometric signatures, such asfrequency magnitude, phase errors, and I/Q origin offset, todefend against identity attacks. However, there is additionaloverhead associated with wireless channel response andradiometric signature extraction in wireless networks. Liand Trappe [4] introduced a security layer that used forge resistantrelationships based on the packet traffic, includingMAC sequence number and traffic pattern, to detectspoofing attacks.

ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

The works [3], [7], [14] using RSS to defend againstspoofing attacks are most closely related to us. Faria andCheriton [3] proposed the use of matching rules ofsignalprints for spoofing detection. Sheng et al. [7] modeledthe RSS readings using a Gaussian mixture model. Sang andArora [14] proposed to use the node's "spatial signature,"including Received Signal Strength Indicator (RSSI) and LinkQuality Indicator (LQI) to authenticate messages in wirelessnetworks. However, none of these approaches are capable of determining the number of attackers when there are multipleadversaries collaborating to use the same identity to launchmalicious attacks. Further, they do not have the ability tolocalize the positions of the adversaries after attack detection.

Several localization algorithms and evaluate their robustness to attacks where an adversary attenuates or amplifies the signal strength at one or more landmarks. They propose several performance metrics that quantify the estimator's precision and error, including Holder metrics, which quantify the variability in position space for a given variability in signal strength space. They then conduct a trace-driven evaluation of several point-based and area based algorithms, where They measured their performance as They applied attacks on real data from two different buildings. They found the median error degraded gracefully, with a linear response as a function of the attack strength. They also found that area-based algorithms experienced a decrease and a spatial-shift in the returned area under attack, implying that precision increases though bias is introduced for these schemes. Thelocalization techniques, in spite of itsseveral meter-level accuracy, using RSS [15], [16], [17], [18] isan attractive approach because it can reuse the existingwireless infrastructure and is highly correlated withphysical locations.

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. By analyzing the RSS pattern of typical 802.11 transmitters in a 3-floor building covered by 20 airmonitors, they observed that the RSS readings followed a mixture of multiple Gaussian distributions. They discovered that this phenomenon was mainly due to antenna diversity, a widely-adopted technique to improve the stability and robustness of wireless connectivity. This observation renders existing approaches ineffective because they assume a single RSS source. On Gaussian mixture models, building RSS profiles for spoofing detection. Experiments on the same tested show that method is robust against antenna diversity and significantly outperforms existing approaches. At a 3% false positive rate, They detect 73.4%, 89.6% and 97.8% of attacks using the three proposed algorithms, based on local statistics of a single AM, combining local results from AMs, and global multi-AM detection, respectively.

III. CLUSTER ANALYSIS

The theoretical support of usingthe RSS-based spatial correlation inherited from wirelessnodes to perform spoofing attack detection. It also showedthat the RSS readings from a wireless node may fluctuate andshould cluster together. In particular, the RSS readings overtime from the same physical location will belong to the samecluster points in the n-dimensional signal space, while theRSS readings from different locations over time should formdifferent clusters in signal space. Here illustrated thisImportant observation in Fig. 1, which presents RSS readingvectors of three landmarks (i.e., n ¼ 3) from two differentphysical locations. Under the spoofing attack, the victim andthe attacker are using the same ID to transmit data packets,and the RSS readings of that ID is the mixture readingsmeasured from each individual node (i.e., spoofing node orvictim node).

Since under a spoofing attack, the RSS readingsfrom the victim node and the spoofing attackers are mixedtogether, this observation suggests that may conductcluster analysis on top of RSS-based spatial correlation tofind out the distance in signal space and further detect thepresence of spoofing attackers in physical space.This work, utilize the Partitioning Around MedoidsMethod to perform clustering analysis in RSS. The PAMMethod [26] is a popular iterative descent clusteringalgorithm. Compared to the popular K-means method [9],the PAM method is more robust in the presence of noise andoutliers.

ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

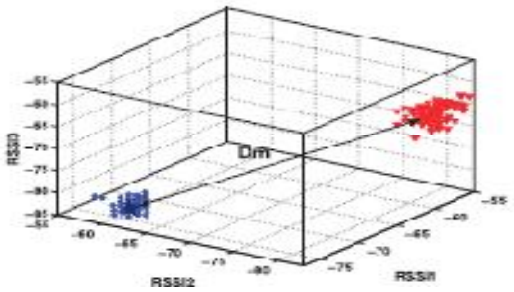


Fig.1. Illustration of RSS readings from two physical locations.

Thus, the PAM method is more suitable indetermining clusters from RSS streams, which can be unreliable and fluctuating over time due to random noise and environmental bias. Then formulate spoofing detection as a statisticalsignificance testing problem, where the null hypothesis is

H0 : normal (no spoofing attack)

In significance testing, a test statistic T is used to evaluatewhether observed data belong to the null-hypothesis or not.In this attack detection phase, partition theRSS vectors from the same node identity into two clusters(i.e., K ¼ 2) no matter how many attackers are using this identity, since the objective in this phase is to detect the presence of attacks. Then choose the distance betweentwo medoidsDm as the test statistic T in our significancetesting for spoofing detection, Dm ¼ kMi _Mjk, where Miand Mj are the medoids of two clusters. Under normalconditions, the test statistic Dm should be small since thereis basically only one cluster from a single physical location.However, under a spoofing attack, there is more than onenode at different physical locations claiming the same nodeidentity. As a result, more than one clusters will be formedin the signal space and Dm will be large as the medoids arederived from the different RSS clusters associated withdifferent locations in physical space.

IV. SUPPORT VECTOR MACHINES-BASED MECHANISM

Provided the training data collected during the offline training phase, it can further improve the performance ofdetermining the number of spoofing attackers. In addition,given several statistic methods available to detect thenumber of attackers, such as System Evolution and SILENCE,can combine the characteristics of these methods toachieve a higher detection rate. Then this exploreusing Support Vector Machines to classify the number ofthe spoofing attackers. The advantage of using SVM is thatit can combine the intermediate results (i.e., features) fromdifferent 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 learningmethods for data classification, which involves a training phase and a testing phase. Each data instance in thetraining set consists of a target value (i.e., class label) andseveral attributes (i.e., features).

V. UNMASK

Wireless networks enable a wide range of applications in both military and civilian domains. The deployment scenarios, the functionality requirements, and the limited capabilities of these networks reveal them to a wide-range of attacks against control traffic and data traffic (such as selective forwarding). This paper proposes a framework called UNMASK that mitigates such attacks by detecting, diagnosing, and isolating the malicious nodes. UNMASK uses as a fundamental building block the ability of a node to oversee its neighboring nodes' communication. On top of UNMASK, build a secure routing protocol, LSR, that provides additional protection against malicious nodes by supporting multiple node-disjoint paths. Then analyze the security guarantees of UNMASK and use ns-2 simulations to show its effectiveness

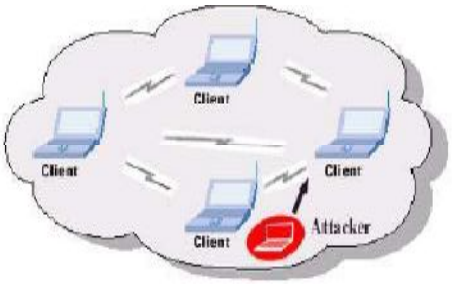
ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Special Issue 3, July 2014

against representative control and data attacks. The overhead analysis shows that UNMASK is a lightweight protocol appropriate for securing resource constrained sensor networks.



A distributed protocol, called UNMASK, for detection, diagnosis, and isolation of nodeslaunching control attacks, such as, wormhole, Sybil, rushing, spoofing, and replay attacks. UNMASK uses localmonitoring to detect control and data traffic, and local response to diagnose and isolate the Thesaurusnodes.

VI. CONCLUSION

As wireless network threats are becoming more dangerous day by day, security in wireless is most essential. The design ofUNMASK fundamentally relies on the ability of some guard nodes to overhear the behavior of neighboring nodes. Any technique that relies on this has the drawback that it can be bypassed by a powerful adversary that can accurately place malicious nodes capable of colluding with compromised nodes to create collision or delegates its identity to some other compromised node Then analyze the security guarantees of UNMASK and show its ability to handle attacks through arepresentative set of these attacks.

And present a coverage analysis and find the probability of false alarm and misseddetection. But it is less susceptible to this drawback than prior techniques since it increases the number of nodes that are performing verification.Note that incremental deployment of nodes is equivalent to a node moving to the new position and the situation can be handled similarly. As future work we are investigating secure neighbor discovery protocols appropriate for resource-constrained mobile networks.

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 Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.
[4] Q. Li and W. Trappe, "Relationship-Based Detection of Spoofing-Related Anomalous Traffic in Ad Hoc Networks," Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.
[5] 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.
[6] A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless LansWith Key Refresh and Host Revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.
[7] 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.
[8] 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.
[9] 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.
[10] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM WorkshopWireless Security (WiSe), pp. 79-87, 2003.