Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.13 – 17

SURVEY ARTICLE

Survey of Detection and Localization of Multiple Spoofing Attacks in Wireless Networks

[1]K.Suresh Babu, [2]Swetha Gurram

[1]Assistant Professor M.Tech (CS), School Of Information Technology JNTUH, India

[2]M.Tech in Department of CNIS at School Of Information Technology, JNTUH, India

[1] kare_suresh@yahoo.com

[2] swethag58@gmail.com

Abstract: Wireless systems are defenseless to spoofing attacks, which takes into consideration numerous different types of attacks on the systems. Despite the fact that the personality of a hub might be confirmed through cryptographic verification, confirmation is not dependably conceivable in light of the fact that it requires key administration and extra infrastructural overhead. A method for both detecting spoofing attacks and spotting the positions of foes performing the attacks is introduced. An attack detector for wireless spoofing that uses K-implies cluster analysis is used. Next, how we integrated our attack detector into a real time indoor confinement framework is portrayed, which is additionally equipped for limiting the positions of the attackers. It is shown that the positions of the attackers might be confined utilizing either zone based or focus based confinement calculations with the same relative slips as in the ordinary case. We have assessed our routines through experimentation utilizing both a 802.11 (Wifi) organize and additionally an 802.15.4 (Zigbee) system. Our effects show that it is conceivable to identify wireless spoofing with both a high recognition rate and a low false positive rate, along these lines furnishing solid proof of the viability of the K-methods spoofing detector and also the attack localizer.

Keywords: Wireless network security, spoofing attack, attack detection, localization, wireless spoofing

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. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or 802.11i (WPA2), such methodology can only protect data frames - an attacker can still spoof management or control frames to cause significant impact on networks. Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. In a large-scale wireless 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. Therefore, the problem can be divided into three folds such as (1) detect the presence of spoofing attacks, (2) determine the number of attackers, and (3) localize multiple adversaries. To determine the number of attackers when multiple adversaries use a same identity to launch attacks, this is the basis to further localize multiple adversaries after attack detection. The identification and localization can be done in the following ways.1) GADE: a generalized attack detection model that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods.2) IDOL: an integrated detection and localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels.In GADE, the Partioning around Medoids (PAM) cluster analysis method is used to perform attack detection. We formulate the problem of multi-class detection problem. We then applied cluster based methods to determine the no of attackers. Moreover, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. Recently new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed. As we demonstrated through our experiments using both an 802.11 network as well as an 802.15.4 network in two real office buildings.GADE is highly effective in spoofing detection with over 90% hit rate and precision. One key observation is that IDOL can handle attackers using different transmission power levels, thereby providing strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network.Additionally ,when the training data is available, We propose to use Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers in the network.

II. Related Work

1. Detecting Identity Based Attacks in Wireless Networks Using Signalprints

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. In this paper we show that a transmitting device can be robustly identified by its signalprint, a tuple of signal strength values reported by access points acting as sensors. We show that, different from MAC addresses or other packet contents, attackers do not have as much control regarding the signalprints they produce. Moreover, using measurements in a testbed network, we demonstrate that signalprints are strongly correlated with the physical location of clients, with similar values found mostly in close proximity. By tagging suspicious packets with their corresponding signalprints, the network is able to robustly identify each transmitter independently of packet contents, allowing detection of a large class of identity-based attacks with high probability.

2. 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 certificate authority (CA) and provides certificate update service for all nodes, including the servers themselves. A ticket scheme is introduced for efficient certificate service. In addition, an efficient server group updating scheme is proposed. The performance of SEKM is evaluated through simulation.

3. Lightweight Key Management for IEEE 802.11 Wireless LANs With Key Refresh and Host Revocation

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. This paper propose 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.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, or built using free, open-source tools.

4. An Authentication Framework for Hierarchical Ad Hoc Sensor Networks

Recent results indicate scalability problems for flat ad hoc networks. To address the issue of scalability, self-organizing hierarchical adhoc architectures are being investigated. In this paper, we explore the task of providing data and entity authentication for hierarchical ad hoc sensor networks. Our sensor network consists of three tiers of devices with varying levels of computational and communication capabilities. Our lowest tier consists of compute-constrained sensors that are unable to perform public key cryptography. To address this resource constraint, we present a new type of certificate, called a TESLA certificate, that can be used by low powered nodes to perform entity authentication. Our framework authenticates incoming nodes, maintains trust relationships during topology changes through an efficient handoff scheme, and provides data origin authentication for sensor data. Further, our framework assigns authentication tasks to nodes according to their computational resources, with resource-abundant access points performing digital signatures and maintaining most of the security parameters. We conclude by providing an initial performance evaluation and security analysis for our framework.

5. Sequence Number-Based MAC Address Spoof Detection

The exponential growth in the deployment of IEEE 802.11- based wireless LAN (WLAN) in enterprises and homes takes 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 different set of intrusion detection mechanism. Most link-layer attacks in WLANs are denial of service at- tacks 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 held 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.

6. Spatial Signatures for Lightweight Security in Wireless Sensor Networks

This paper experimentally investigates the feasibility of cryptofree communications in resource-constrained wireless sensor networks. We exploit the spatial signature induced by the radio communications of a node on its neighboring nodes. We design a primitive that robustly and efficiently realizes this concept, even at the level of individual packets and when the network is relatively sparse. Using this primitive, we design a protocol that robustly and efficiently validates the authenticity of the source of messages: authentic messages incur no communication overhead whereas masqueraded communications are detected cooperatively by the neighboring nodes. The protocol enables lightweight collusion-resistant methods for broadcast authentication, unicast authentication, non-repudiation and integrity of ommunication. We have implemented our primitive and protocol, and quantified the high-level of accuracy of the protocol via testbed experiments with CC1000 radio-enabled motes.

III. Proposed Method and Its Advantages

Spoofing detection system which can both detect the spoofing attacks, as well as localize the adversaries in wireless and sensor networks.A different approach is handled by using the physical properties associated with wireless transmissions to detect spoofing. A scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks is proposed. This method utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. By analyzing the RSS from each MAC address using K means cluster algorithm, we have found that the distance between the centroids in signal space is a good test statistic for effective attack detection. We then describe how we 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, we 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.Main advantages are to Detect the presence of spoofing attacks, Determine the number of attackers, Localize multiple adversaries and eliminate them,Will not require any additional cost or modification to the wireless devices themselves.

IV. CONCLUSION

The proposed approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that it can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. This 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.Further, based on the number of attackers determined by the mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power 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,” in Proceedingsof the USENIX Security Symposium, 2003, pp. 15 – 28.

[2] F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access points vulnerabilities to dos attacks in 802.11 networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference, 2004.

[3] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.
[4] Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proc. IEEE SECON, 2006.
[5] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.
[6] 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.
[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell,"Detecting 802.11 MAC layer spoofing using received signal strength," in Proc. IEEE INFOCOM, April 2008.

Author Profiles:

Swetha Muthuluri, Pursuing M.Tech in Department of CNIS at School Of Information Technology JNTUH, Kukatpally, Hyderabad Rangareddy dist., A.P., India. Her research interest includes in Wireless Security, Networks.

K.Suresh Babu, Assistant Professor M.Tech(CS), School Of Information Technology JNTUH, Kukatpally, Hyderabad, Rangareddy dist., A.P., India.