Survey on Security Management of Multiple Spoofing Attackers in Wireless Networks

Mr. Rajpure Amol Subhash
M.E IT (II)
Department of Computer Engineering, DGOI,FOE,Daund.
Pune University, Maharashtra India
amolrajpure9@gmail.com

Prof. Bere Sachin Sukhadeo
Assistant Professor
Department of Computer Engineering, DGOI,FOE,Daund.
Pune University Maharashtra India
sachinbere@gmail.com

Abstract - Wireless spoofing attacks are very easy to initiate and can highly impact the performance of networks. In this paper, we have plan to use spatial information a physical property related to each point or node ,complex to mispresent and that depend on cryptography, as the initializing for detecting spoofing attacks and find out the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple opponent. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to find out the spoofing attacks. For find out the number of attackers we are using cluster based mechanism. . To localize the positions of multiple attackers, we have developed an integrated detection and localization system. The generated localization results with a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries. As the wireless networks are easily susceptible for various types of spoofing attacks, basically this paper focuses on Identity-based spoofing attacks and the enhanced and efficient techniques to secure from such attacks

Keywords**:** *Denial of Service (DoS), G-MOAD, IDAL-M, Inter domain Packet filters (IDPF), PAM, and Received Signal Strength (RSS).*

*****

I. INTRODUCTION

In the current age of Computing and communication networks the more affection is laying towards the wireless networks. As the wireless networks are easily susceptible for various types of spoofing attacks, basically this paper focuses on Identity-based spoofing attacks and the enhanced and efficient techniques to secure from such attacks. The existing security technique involves the key computation cryptographic schemes, but such techniques are not always affordable due to its key computation and respective management. Hence to enhance efficient and such effective security management this paper gives the innovative and improved technique to use the physical property based on RSS (Received Signal Strength) [1]. Received Signal Strength is the physical property associated with each node. The security management scheme based on RSS, It doesn’t require any additional modifications to the existing code. Also it is totally independent from the key based cryptographic technique, and hard to falsify. Here the objective which is obtained through the RSS-based security techniques as like Detection of Identity based spoofing attack, Determining number of spoofing attackers, Positioning of actual location of the attackers in the victim targeted system, Detects the Denial-Of-Service attack with location of attackers [3].

II. LITERATURE SURVEY

A. Detecting Spoofing Attacks In Mobile Wireless Networks

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 [8]. 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. Our approach does not require any changes or cooperation from wireless devices other than packet transmissions. Through experiments from an office building environment, we show that DEMOTE achieves accurate attack detection both in signal space as well as in physical space using localization and is generic across different technologies including IEEE 802.11 b/g and IEEE 802.15.4 [2].

B. Spatial Signatures For Lightweight Security In 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 [5]. The protocol enables lightweight collusion-resistant methods for broadcast authentication unicast authentication, non-repudiation and integrity of communication. We have implemented our primitive and protocol, and quantified the high-level of accuracy of the protocol via test bed experiments with *CC1000* radio-enabled motes.

C. Wireless Localization Using Rf-Based Fingerprint Matching

Accurately obtaining the position of mobile devices is critical to high-level applications. In indoor environments, localization approaches employing RF-based fingerprint matching is an active research area because it can reuse the existing communication infrastructure, as well as reduce the signal uncertainty to achieve better location accuracy. Specifically, we derived an analytic expression for the cumulative distribution function (CDF) of the location error and investigated the mathematical relationship between the location error and the sampling points. Particularly, we studied the effects of the number of sampling points and the distance between adjacent sampling points. We further conducted experiments using an 802.11 network in a real office building environment.

D.A Localization-Based Anti-Sensor Network System

An anti-sensor network system is proposed, aiming to protect an important area from being under surveillance by an adversary's sensor nodes. The major components of the system are a set of observing points (monitors) deployed in the area of importance. The observers try to localize sensor positions using antenna arrays to measure direction of arrival (DOA) and received signal strength of the signals emitted by sensors. Once sensors are localized, additional measures are taken to physically remove or disable localized sensors. The proposed anti-sensor network system is designed to handle additional counter-measures that can be employed by sensors, including message encryption and non-uniform transmission power levels. The simulation results show the effectiveness of the proposed system and effects of counter measures on sensor localization performance.

E. Estimating The Number Of Clusters

The estimation of the number of clusters (NC) is one of crucial problems in the cluster analysis of gene expression data. Most approaches available give their answers without the intuitive information about separable degrees between clusters. However, this information is useful for understanding cluster structures. To provide this information, we propose system evolution (SE) method to estimate NC based on partitioning around medoids (PAM) clustering algorithm [6]. SE analyzes cluster structures of a dataset from the viewpoint of a pseudo thermodynamics system. The system will go to its stable equilibrium state, at which the optimal NC is found, via its partitioning process and merging process. The experimental results on simulated and real gene expression data demonstrate that the SE works well on the data with well-separated clusters and the one with slightly overlapping clusters.

III. CONCLUSION

In this survey paper multiple node are use for the communication. For detection of the attack node are divided into clusters. With the help of RSS algorithm the attacker node determined and by using graphical model representation of attacker node with respect to X and Y axis. By using this algorithm same node identity with multiple attacks are detected and localized. The results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries

REFERENCES

[1] Jie Yang, Yingying (Jennifer) Chen, Wade Trappe, Jerry Cheng,"Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", IEEE Transactions on Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.

[2] F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access point's 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 signal prints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.

[4] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.

[5] 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.

[6] 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.

[7] J. Yang, Y. Chen, and W. Trappe, “Detecting spoofing attacks in mobile wireless environments,” in Proc. IEEE SECON, 2009.

[8] Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wireless spoofing attacks,” in Proc. IEEE SECON, May 2007.