Prashant.R.R *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 5, May- 2014, pg. 1-6 **ISSN: 2321-8363**

Detecting and Identifying the Location of Multiple Spoofing Adversaries in Wireless Network

Prashant.R.R
IV Semester, M-Tech, Dept. of E&C
BTLIT College, Bangalore
Email: prr.sangu@gmail.com

Mohammed Fayaz
Assistant Professor, Dept. of E&C
BTLIT College, Bangalore
Email: mfaiyazz1@gmail.com

Abstract— Wireless networks are vulnerable to identity-based attacks, including spoofing attacks, significantly impact the performance of networks. Conventionally, ensuring the identity of the communicator and detecting an adversarial presence is performed via cryptographic authentication. Unfortunately, full-scale authentication is not always desirable as it requires key management, coupled with additional infrastructural overhead and more extensive computations. The proposed non cryptographic mechanism which are complementary to authenticate and can detect device spoofing with little or no dependency on cryptographic keys. This generalized Spoofing attack-detection model utilizes MD5 (Message Digest 5) algorithm to generate unique identifier for each wireless nodes and a physical property associated with each node, as the basis for (1) detecting spoofing attacks; (2) finding the number of attackers when multiple adversaries masquerading as a same node identity; and localizing multiple adversaries. Nodes Counter technique is developed to determine the number of attackers. Cluster Euclidean distance method is developed for localization of spoofing attackers.

Keywords— Wireless Network, Spoofing Attack, Identity-Based Attack, Message Digest 5, Cluster Euclidean distance method

INTRODUCTION

A spoofing attack [1] is the most common online attack in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage, it become more sophisticated defence mechanisms. 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. 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 [2] quickly.

Therefore, it is important to

- detect the presence of spoofing attacks,
- determine the number of attackers, and
- Localize multiple adversaries and eliminate them.

Clustering is the process of examining a collection of "points," and grouping the points into "clusters" according to some distance measure. The goal is that points in the same cluster have a small distance from one another, while points in different

clusters are at a large distance from one another. A dataset suitable for clustering is a collection of points, which are objects belonging to some space. In its most general sense, a space is just a universal set of points, from which the points in the dataset are drawn.

MAC spoofing is a technique for changing a factory-assigned MAC address of a network interface on a networked device. The MAC address is hard-coded on a network interface controller (NIC) and cannot be changed. The process of masking a MAC address is known as MAC spoofing. Due to the open-nature of the wireless medium, it is easy for adversaries to monitor communications to find the layer-2 MAC addresses of the other entities. For most commodity wireless devices, attackers can easily forge their MAC address in order to masquerade as another transmitter.

AODV Routing [3][4] is a routing protocol for mobile ad hoc networks (MANETS) and other wireless ad hoc networks. It is jointly developed in nokia research center, university of California. The AODV routing protocol uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path. However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow of data packet transmission.

The main contributions of our work are: 1) SADe: a Spoofing attacker detection model (SADe) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods and 2) IDLM: an integrated detection and localization model system that can both detect attacks as well as find the positions of multiple adversaries. In SADe, the Message Digest 5(MD5) cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multiclass detection problem. We then applied cluster-based methods to determine the number of attacker. Moreover, we developed an integrated system, IDLM, which utilizes the results of the number of attackers returned by SADe to further localize multiple adversaries.

Literature Survey

1. Sequence Number-Based MAC Address Spoof Detection

Fanglu Guo and Tzi-cker Chiueh, Computer Science Department, Stony Brook University, NY 11794

The exponential growth in the deployment of IEEE 802.11- based wireless LAN (WLAN) in enterprises and homes makes 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 attacks 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 equipment's, 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.

2. Lightweight Key Management For IEEE 802.11 Wireless LANs

With Key Refresh and Host Revocation AvishaiWool, Dept. Electrical Engineering - Systems, Tel Aviv University, Ramat Aviv 69978, ISRAEL

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 proposes 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.

3. Implementation of the AODV Routing Protocol in ns2 for Multi-hop Wireless Networks

Zehua Wang, Yuanzhu Peter Chen, Cheng Li *Memorial University fzw1640, yzchen, lichengg@mun.ca*

Multi-hop wireless network is a wireless communication network without centralized control mechanism. Network nodes organize themselves automatically, and help other nodes relay data packets if they are not within the communication range. Perfect study of protocol designed for such networks has been very challenging. Hence, simulations are always utilized to obtain the desired perfect results. OPNET and *ns*2 are the two most popular simulators used in network simulation, and *ns*2 as a open source software has attracted more attention in recent years. However, the implementations of routing protocol in *ns*2 are non-trivial. In this paper, we conduct a case study of implementing a routing protocol is *ns*2. The widely used routing protocol AODV [3][4] is selected to demonstrate the implementation procedures. The methods of collecting and analysing simulation results are also reviewed and discussed.

4. Detecting Spoofing Attacks in Mobile Wireless Environments

Jie Yang∗, Yingying Chen∗ and Wade Trappe† ∗Dept. of ECE, Stevens Institute of Technology † WINLAB, Rutgers University Castle Point on Hudson, Hoboken, NJ 07030 North Brunswick, NJ 08854

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. 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.

EXISTING SYSTEM

The traditional approach to address spoofing attacks is to apply cryptographic authentication.

Disadvantages

- 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.
- Key management often incurs significant human management costs on the network.

PROPOSED SYSTEM

- Use spatial information to identify the attackers it not only identify the attackers but also localize adversaries.
- It also detects attackers when multiple users use the same node identity.
- It does not require additional cost.
- The Cluster Based wireless Sensor Network Message Digest 5(MD5) based spatial correlation of network Strategy.
- The training data is available; we explore using Cluster Counter technique (CCT) method to further improve the accuracy of determining the number of attackers.
- In localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

- 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 wireless networks.

IV PROCEDURE FOR IMPLEMENTATION

Step 1: Generate Unique ID for all nodes in the
Network using MD5 algorithm
Step 2: Define the cluster and the nodes in clusters
Step 3: Let Clusters in Network be "Cn"
Step 4: for (i=0; i<=Cn) {Attacker Node A=0;
Perform spoofing attack detection by checking the node key value in every cluster A=A++; //Node, which has replicated key value is identified as attacker node}
Step 5: Perform the detection in every cluster, if
Unique ID of any two nodes is same then the presence of spoofing attackers.
Step 6: Identify the number of attackers "A" by
Nodes counter technique
Step 7: Localize the Attacker, by finding distance
Between reference node and attacker node

RESULTS

The following result shows the total numbers of nodes are deployed in the network. There are total 17 nodes used in a network.

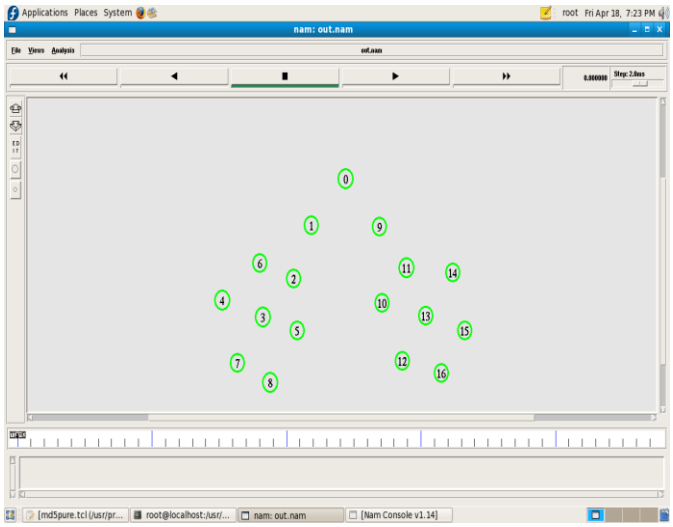

Fig 1: Node Deployment

The following result shows the detection of spoofing attackers. Here node 5 is a attacker node and the location of the Node 8. Because it get a id from the Node 13. In this situation Node 5 act as Node 13. Node 5 is a spoofing attacker in the network. Now Node 13 is a compromised node in the network.
The compromised node is also act as attacker, so the number of attackers in network is 2.

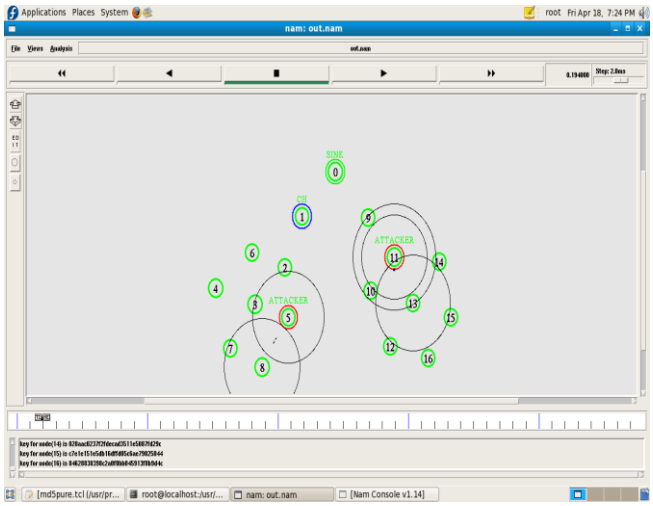

Fig 2: Detection and the number of attackers

In the above result node 5 and compromised node 13 acts as spoofing attacker node in the network. Here node 0 is used as base station or common node. For localization, the distance between common node and attacker node can be found.

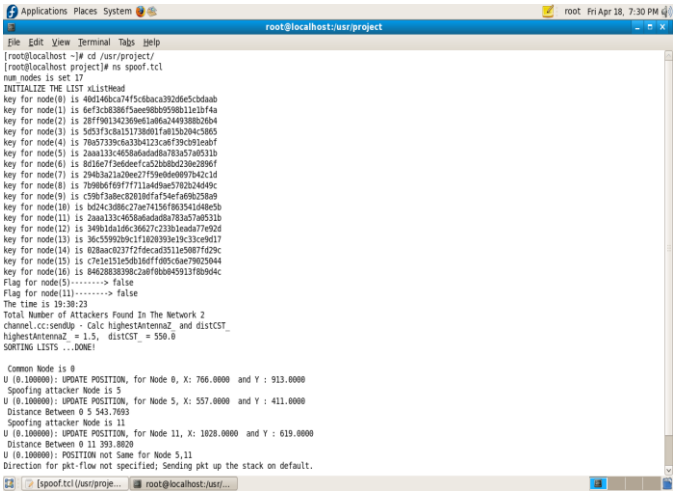

Fig 3: Multiple Attackers and its Location

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 Nodes Counter Techniques, 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. By using Cluster Euclidean distance method, we can localize where the attackers are

present. 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]. *Q. Li and W. Trappe, "Light-weight detection of spoofing attacks in wireless networks," in Proceedings of the 2nd International Workshop on Wireless and Sensor Network Security (WSNS), October 2006.*
[2]. *J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proceedings of the USENIX Security Symposium, 2003, pp. 15 – 28.*
[3]. *Ian D. Chakeres and Elizabeth M. Belding-Royer. AODV Routing Protocol Implementation Design*
[4]. *Magnus Frodigh, Per Johansson and Peter Larsson. Wireless ad hoc networking—The art of networking without a network.*
[5]. *T. Aura, "Cryptographically generated addresses (cga)," RFC 3972, IETF, 2005.*
[6]. *L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. Wiley Series in Probability and Statistics, 1990*
[7]. *Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007*
[8]. *M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.*
[9]. *B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.*
[10]. *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.*
[11]. *S. Yi, P. Naldurg and R. Kravets Security-Aware Ad-hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290 , UIUC, 2002.*
[12]. *C.E.Perkins and E.M.Royer, "Ad-Hoc on Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb, 1999.*

