Detection and Localization of Multiple Spoofing Attackers Using Cluster Analysis

P.Vijayalakshmi
PG Scholar
Kalasalingam Institute of Technology
Krishnankoil

R.Sankar
Assistant Professor
Kalasalingam Institute of Technology
Krishnankoil

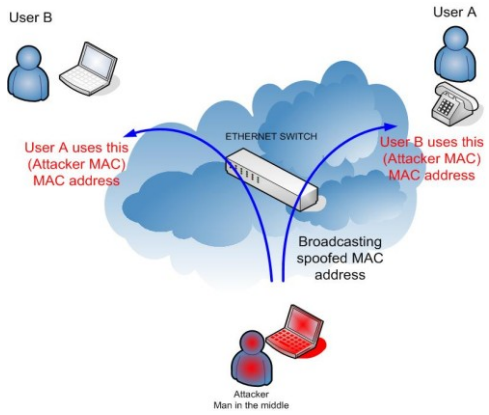
ABSTRACT- Wireless systems are defenseless to spoofing attacks, which takes into consideration numerous different types of attacks on the systems. Despite the fact that the personality of a hub might be confirmed through cryptographic verification, confirmation is not dependably conceivable in light of the fact that it requires key administration and extra infrastructural overhead. In this paper I propose a method for both detecting spoofing attacks, and spotting the positions of foes performing the attacks. I first propose an attack detector for wireless spoofing that uses K-implies cluster analysis. Next, we portray how we integrated our attack detector into a real time indoor confinement framework, which is additionally equipped for limiting the positions of the attackers. I show 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 (Wi-Fi) organize and additionally a 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.

Index Terms: Wireless network security, Spoofing attack, Attack detection, Localization.

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 refers tricking or deceiving computer systems or other computer users. Spoofing is when an attacker pretends to be someone else in order gain access to restricted resources or steal information. This type of attack can take a variety of different forms; for instance, an attacker can impersonate the Internet Protocol (IP) address of a legitimate user in order to get into their accounts. Also, an attacker may send fraudulent emails and set up fake websites in order to capture users' login names, passwords, and account information. Faking an email or website is sometimes called a phishing attack. Another type of spoofing involves setting up a fake wireless access point and tricking victims into connecting to them through the illegitimate connection.IP addresses are similar to postal addresses and route information to the correct location across networks. Data is broken up and sent in pieces called packets. IP address spoofing is possible because an attacker can forge the sender's address and make the packet appear to be coming from someone else. A common use of IP address spoofing is a denial of service attack where an attacker using spoofing to hide the source of their attack. Phishing attacks involve setting up fake websites or sending spam emails in an attempt to lure potential victim's to fake websites. The "sender" field in an email can be changed easily and as long as the email message protocols are acceptable, the message will be delivered. Programs that update automatically can also be another avenue for a wireless spoofing attack; therefore, be sure to enable the "ask me first" feature before allowing your computer to download updates. . 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.

ISSN: 2278 – 7798



Types of Network spoofing:

- Protocol Spoofing
- DNS spoofing
- MAC spoofing

Protocol Spoofing:

In every network, there is a protocol group called the Transmission Control Protocol(TCP). This protocol establishes, maintains and breaks down the connections. In the process of connecting the computer will send a check packet of data for verification. This adds up to the network traffic. This private network running over the public lines will incur extra charges as well. To avoid such a situation, the gateway can act as the remote computer and reply to the TCP messages. Here the network gateway is spoofing as the TCP connecting computer to reduce the traffic.

DNS spoofing:

When a web page is requested through a web browser, it does not connect to the real web address. Before connecting with the web page, it will check with the Domain Name System to get the original IP address. But companies maintain their own DNS server to save response time. So when you click on the web page, you are connected to the in-house server and not to the public DNS server. Here DNS server is spoofing as the public DNS server of the company.

MAC spoofing:

The entire device connected to a network will have a MAC (media access control) address. When you register for internet connection, the internet service provider will register the MAC address for a more secured connection. Only the device with that MAC address can be connected to the network. If the user wants dual access points for internet, it will not be accepted. So the new device will send the information through the registered MAC address to gain access to the network by spoofing the registered device MAC address.

II EXISTING SYSTEM

The identity of a node can be verified through conventional security approaches are not always desirable. Adversaries can easily purchase low-cost devices and use these commonly available platforms to launch a variety of attacks. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. It is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address. It can further facilitate a variety of traffic injection attacks, such as attacks on access control lists, rogue access point (AP) attacks, and eventually denial of service (DOS) attacks. The traditional approach to address spoofing attacks is to 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.

III PROPOSED SYSTEM

In the Proposed system, formulate the problem of determining the number of attackers as a multiclass detection. Preside over a secure and efficient key management framework that builds a public key infrastructure by applying a secret sharing scheme and an underlying multicast server group. Cluster-based mechanisms are developed to determine the number of attackers. Explore using the support vector machines method to further improve the accuracy of determining the number of attackers. By utilizing physical properties associated with transmission to combat attacks in networks. Determining the number of attackers when there are multiple adversaries collaborating to use the same identity to launch malicious attacks. This approach can accurately localize multiple adversaries. In this paper, I take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, I propose a scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks.

Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes.

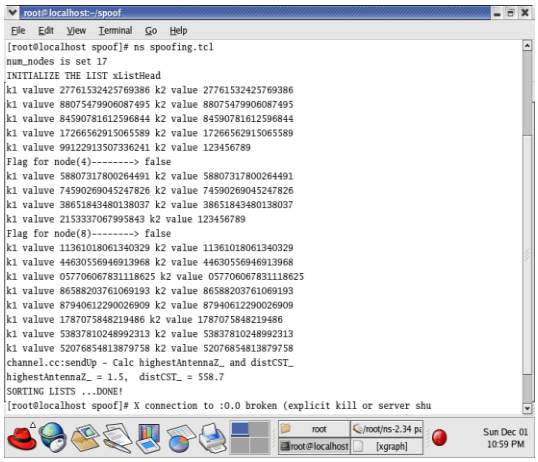
IV PROCEDURE FOR IMPLEMENTATION

Step 1: Generate Unique ID for all nodes in the network using MD5 algorithm

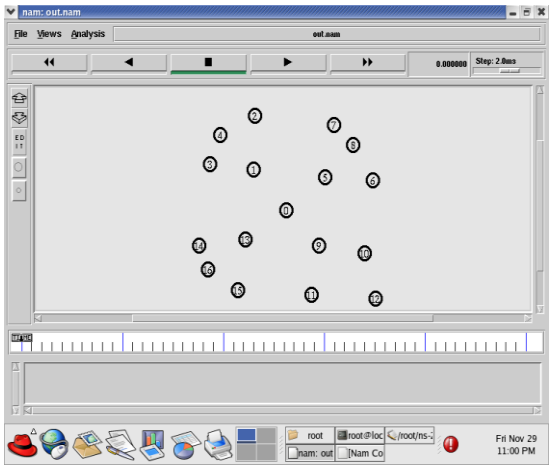
ISSN: 2278 – 7798

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)
{
AttackerNode 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
Step 6: Identify the number of attackers 'A'
Step 7: Localize the Attacker, by indentifying their (X,Y) coordinate values of
Position.

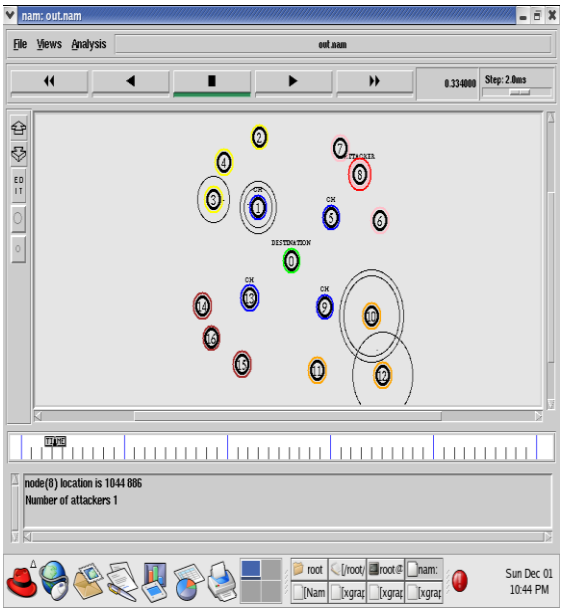
V RESULTS



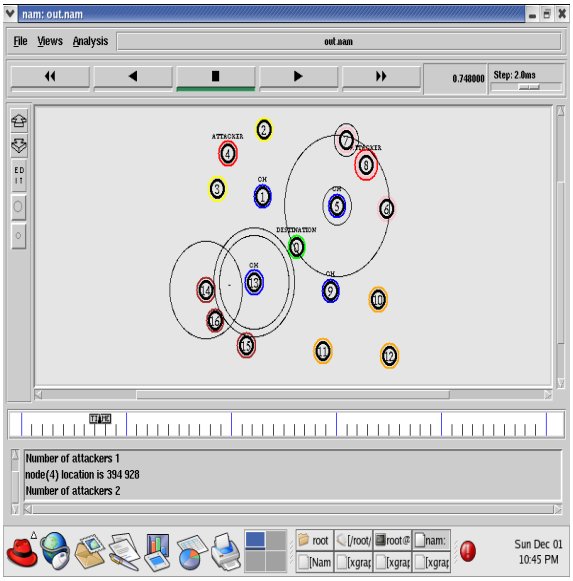
The above Fig shows the generation of random unique key value for all the nodes in the network. Here node 4 and node 8 are declared as false node. Because the key values are different.



The above shows that the total number of nodes deployed in the network. Here I deployed 17 nodes in the network.



The above Fig shows that the division of network into 4 different clusters and the packet flow in the clusters. Here I show that node 8 is a attacker node. I also show that location of node8.



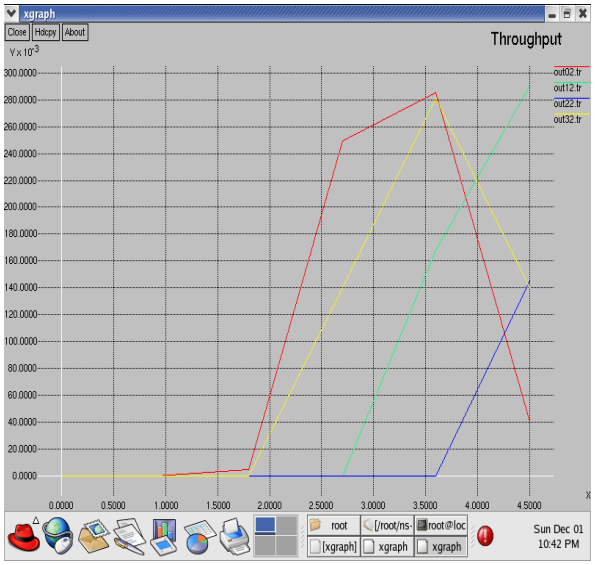
The above fig shows that node 4 is also a attacker node and location of node 4.The key value of node 4 is used

ISSN: 2278 – 7798

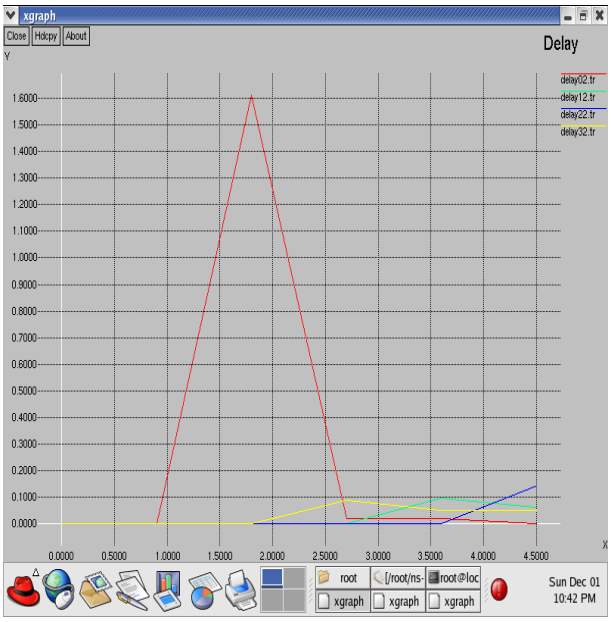
by node 8.now the compromised node 4 will also act as a attacker node. Now the total numbers of attackers are 2.

VI PERFORMANCE EVALUATION

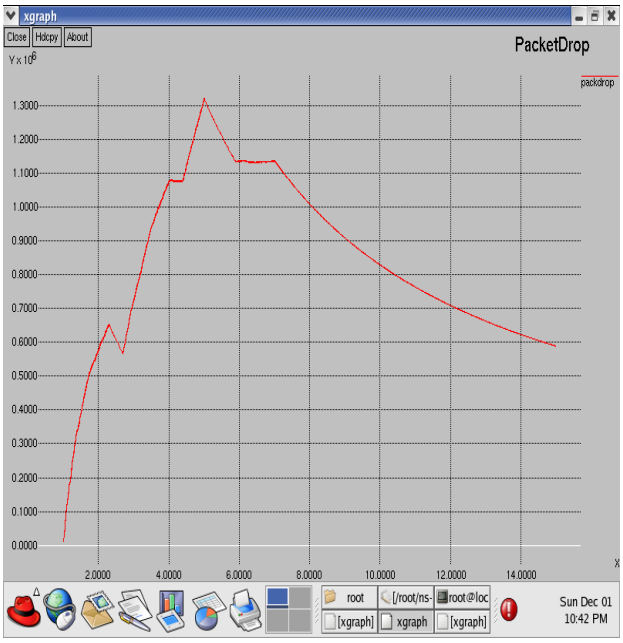
Throughput is the rate at which a network sends receives data. It is a good channel capacity of net connections and rated in terms bits per second (bit/s).



The above Fig shows that efficiency of the packets i.e how many packets are reached to its destination.



In the above Fig shows that delay of packets. End to End Delay refers to the time taken for a packet to be transmitted across a network from source to destination in each and every flow in all the clusters.



In the above Fig shows that Packet Loss. Packet Loss is where network traffic fails to reach its destination in a timely manner. Most commonly packets get dropped before the destination can be reached.

ISSN: 2278 – 7798

VII 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.

VIII REFERENCES

[1] Bellardo.J and Savage.S, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proceedings of the USENIX Security Symposium, 2003, pp. 15 – 28.

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

[3] Bohge.M and Trappe.W, "An authentication framework for hierarchical ad hoc sensor networks," in Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003, pp. 79–87.

[4] Campbell.A, Chen.G, Kotz.D,Sheng.Y and Tan.K "Detecting 802.11 MAC layer spoofing using received signal strength," in Proc. IEEE INFOCOM, April 2008.

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

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

[7] Cheriton.D and Faria.D, "Detecting identity-based attacks in wireless networks using signal prints," in Proceedings of

the ACM Workshop on Wireless Security (WiSe), September 2006.

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

[9] Li.Q and Trappe.W, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proc. IEEE SECON, 2006.

[10] Wool. A, "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.

Mrs. P.Vijayalakshmi

The author is currently a ME Student in Computer Science and Engineering Department at Kalasalingam Institute of Technology.She had completed BE from Arulmigu Kalasalingam College of Engineering.

Mr. R.Sankar

The author is an Assistant Professor in department of Computer Science and Engineering at Kalasalingam Institute of Technology. He received his B.E degree from PTR College of Engineering and Technology, affiliated to Anna University, Chennai and M.E from Thiagarajar College of Engineering. His research interest is networking.

ISSN: 2278 – 7798