Indian J.Sci.Res. 17(2): 521 - 524, 2018

ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

MULTIPLE SPOOFING ATTACKERS USING CLUSTER ANALYSIS FOR IDENTIFYING AND LOCATING IN WIRELESS NETWORKS

[1] Imthiazunnisa Begum , [2] Swetha Sirasanagandla
[1,2]Electronics and Communication Engineering,,Aurora's Scientific, Technological Research Academy,
Bandlaguda, Hyderabad, Telangana.

Abstract – Attacks can occur on Wireless networks, since they are vulnerable to spoofing. Authentication is almost impossible because it requires key management and other infrastructural facilities, even though the identity of a node can be verified by it . This paper proposes a method for both locating adversary positions as well as detecting spoofing attacks, we propose firstly an attack detector for spoofing that utilizes K-means cluster analysis. Secondly, we describe how to integrate this attack detector in a real time indoor localization system. Finally, we show that the position of attackers can be localized using either area based or point based localization algorithms with the same relative errors as in the normal case.

Keywords – Cryptographic authentication, Spoofing attacks, K-means cluster analysis, Wireless networks, localization algorithms

I INTRODUCTION

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to 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 facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing attackers and eliminate them from the networks.

Spoofing attacks can further facilitate a variety of traffic injection attacks [1], [2] such as attacks on access control lists, rogue access point attacks, and eventually DoS attacks.

Reference [3] shows that a transmitting device can be robustly identified by its signal prints, a tuple of signal strength values reported by access points acting as a sensor. By tagging a suspicious packet with their corresponding signal print, the network is able to robustly identify each transmitter independently of packet contents, which allows detection of a large class of identity based attacks with high probability. [4] Introduced a security layer that used forge-resistant relationships based on the packet traffic, including MAC sequence number and traffic pattern to detect spoofing attacks.

Paper [5] which uses Received Signal Strength (RSS) & K-means cluster analysis to detect spoofing attacks. Also studied the localization of adversaries. However it does not give a scheme to determine the number of attackers when multiple adversaries use a same node identity to launch attacks if the adversary uses different transmission power levels.

In paper [6] an authentication framework for hierarchical, adhoc sensor network is proposed. However cryptographic authentication is not always applicable, since wireless device has limited resources and lack of fixed key infrastructure in the network. [7] Proposed to use the node's "spatial signature", including Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) to authenticate messages in wireless networks. It experimentally investigates the feasibility of crypto free communication resources constrained in wireless sensor networks and exploits the spatial signatures induced by the radio communication of a node of its neighboring nodes.

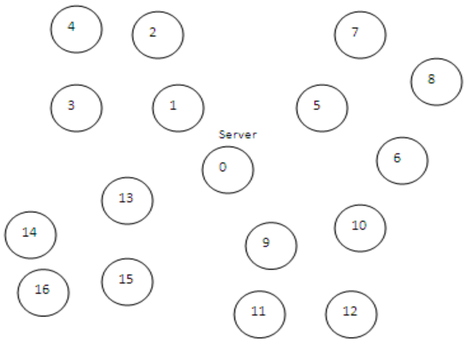
Reference [8] proposed to perform detection of attacks on wireless localization.

I. Experimental Design

A. Node Deployment

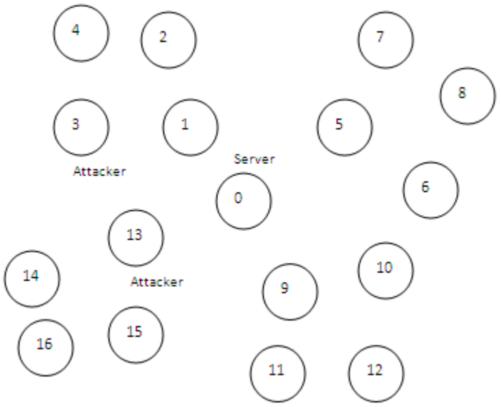
We consider a wireless network with N nodes. Let N denote the set of all nodes in the network. The communication among all N nodes is based on a tree topology with the destination as the root. The tree is formed in the initial phase as follows. The nodes receiving the message will set the message sender as the parent node, increase the hop counter by one, and broadcast it to their neighbors. If a node receives multiple messages, it will select the one with the minimum hop counter to broadcast and set the sender of the message as its parent.

[1]Corresponding Author



B. Node Characterization

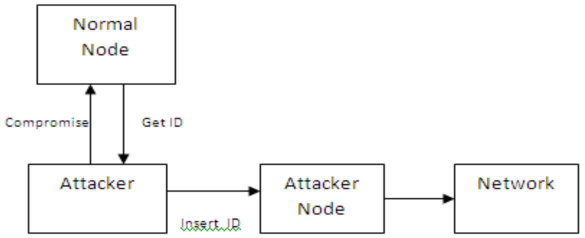
We characterize the nodes deployed as two types, one is Normal node and the other is Attacker. Also we consider the wireless nodes composed of several clusters of Normal nodes. Every cluster is responsible for specific geographical region. Normal node carries out the monitoring for a specific geographical region. Normal node carries out the monitoring of a particular spatial area it is responsible for and then transmits data with a secure approach. Each and every node acquires a unique key value, with which the data will be forwarded to the destination.



Node Characterization

C. Spoofing Attack Detection

Spoofing attack detection is performed using cluster analysis. As the wireless network is deployed as clusters, the attackers are identified in each and every cluster separately. Under the spoofing attack, the victim and attacker are using the same id to transmit data packets. Since under a spoofing attack, the data packets from the victim nodes and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top spatial correlation to find out the presence of spoofing attackers in physical space.

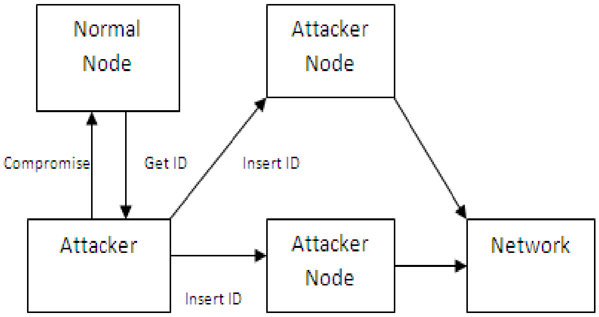


D. Detection of Multi-Spoofing Attack

The Partitioning Around Medoids (PAM) Method is used to perform clustering analysis. The PAM method is a popular iterative descent clustering algorithm.

Spoofing detection is identified as statistical significance testing problem, where the null hypothesis is : H0 which denotes no spoofing attack. In attack detection phase, the same node identity is partitioned into 2 clusters (i.e. K=2)no matter how many attackers are using this identity.

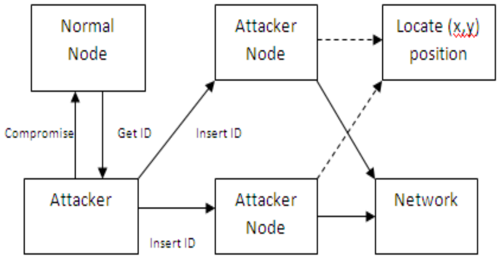
Distance between two mediods Dm is taken, significance test for spoofing detection **Dm = || Mi-Mj||**, where Mi and Mj are the medoids of two clusters. Under normal conditions, the test static Dm should be small, under a spoofing attack Dm will be large, there is more than one node at different physical locations claiming the same node identity. Initially the value of ‘A’ given as 0. Whenever the attackers are identified the value of A is incremented.



Detection of Multi-Spoofing Attack

E. Localization of Attackers

The simulation is performed under Linux environment on NS2. Let us consider the number of nodes deployed in 2D platform. Each and every position of nodes are defined, thus from the initialized value, the attacker's location in the 2D area can be determined accurately.



Localization of Attackers

II. Implementation

A. Input Data

Simulation models are generated from a set of data taken from a stochastic system. It is necessary to check that the data is statistically valid by fitting a statistical distribution and then testing the significance of such a fit.

Further, as with any modeling process the input data's accuracy must be checked and any outliers must be removed.

B. Output Data

When a simulation has been completed, the data need to be analyzed. The simulation output data will only produce a likely estimate of real world events. Methods to increase the accuracy of the output data include repeatedly performing simulations and comparing results, dividing events into batches and processing them individually, and checking the results of simulations conducted in adjacent time periods "connect" to produce a coherent holistic view of the system.

C. Path Selection

Path selection involves applying a route metric to multiple routes, in order to select the best route.

In the case of computer networking, the metric is computed by a routing algorithm, and can cover such information as bandwidth, network delay, hop count, path cost, load, MTU, reliability, and communication cost.

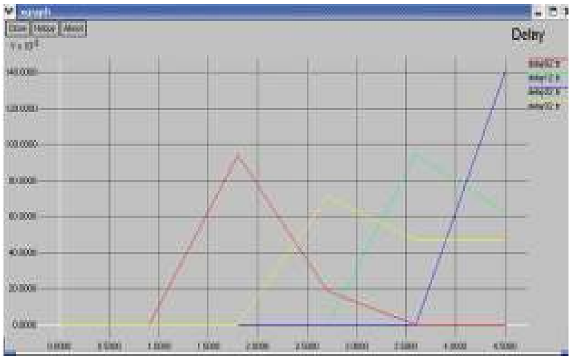
Because a routing metric is specific to a given routing protocol, multi-protocol routers must use some external heuristic in order to select between routes learned from different routing protocols. A local network administrator, in special cases, can setup host specific routes to a particular machine which provides more control over network usage, permits testing and better overall security.

This can come in handy when required to debug network connections or routing tables.

III. Performance Analysis

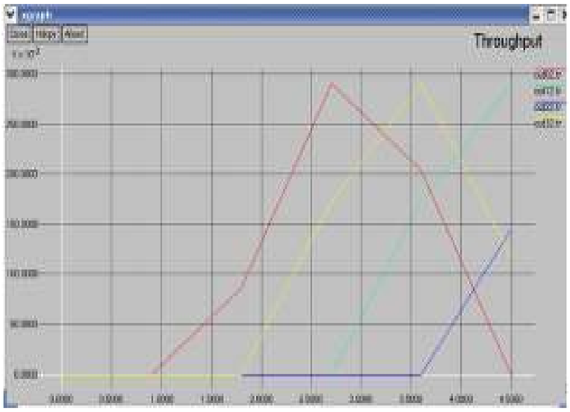
The NS2 simulation is done and we analyzed Delay for the flow taken.

Delay



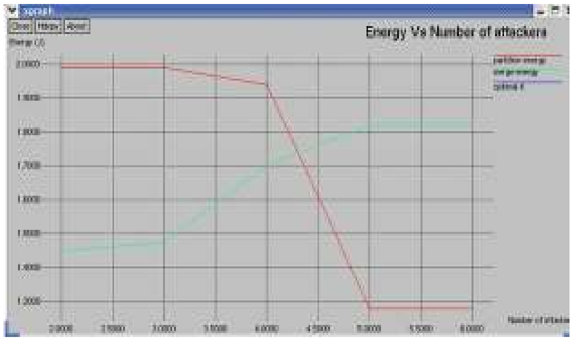
The delay graph defines the delay in the simulation phase. The experiment was running for about 4.5 seconds of a time. End to end delay refers to the time taken for a packet to be transmitted across a network from source to destination during the simulation time.

Throughput



The graph defines the throughput for the proposed protocol. Throughput is the rate at which a network sends the receives data. It is a good channel capacity of net connections and rated in terms of bits per second (bps).

Energy Vs Number of Attackers



V. Conclusion

This paper presents an approach that can both detects the presence of spoofing 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 particularly a challenging problem. The mechanism that employs the minimum distance testing to achieve better accuracy of determining the number of attackers which uses cluster analysis alone.

Further, based on the number of attackers determined by the mechanisms, our integration detection and localization system can localize any number of adversaries even when attackers using different transmission power levels.

The performance of localizing adversaries provides strong evidence of 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 Proceedings of the USENIX Security Symposium 2003, pp. 15-28.

[2] F. Ferreri, M. Benaschi, and L. Valcamonici, “Access points vulnerabilities to DOS attacks in 802.11 networks”, in Proceedings of the IEEE Wireless Communication 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] Q. Li and W. Trappe, “Relationship- based detection of spoofing-related anomalous traffic in ad hoc networks”, in Proc. IEEE SECON, 2006.

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

[6] M. Bohge and W. Trappe, “An Authentication framework for hierarchial ad hoc sensor networks”, in Proceedings of the ACM Workshop on Wireless Security (Wise), 2003, pp.79-87.

[7] L. Sang and A. Arora, “Spatial signatures for lightweight security in wireless sensor networks”, in The 27th Conference on Computer Communications, INFOCOM 2008., 2008, pp 2137-2145.

[8] Y. Chen, W. Trappe, and R. Martin, “Attack detection in wireless localization”, in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), April 2007.