International Journal of Advance Foundation and Research in Computer (IJAFRC)
Volume 1, Issue 12, December 2014. ISSN 2348 – 4853

Spoofing Attackers Detection and Localization in Wireless Networks.

Parvez Ahmed Sheikh
PG -Information Technology, PRMIT&R-Badnera, SGB Amravati University
Email: parvezsheikh63@gmail.com

A B S T R A C T

In world of advanced technology wireless is being considered as significant way of communication. As a result wireless networks growing importance they are susceptible to various attacks- spoofing, phishing which works as path for so many other forms of attacks on the wireless networks. Cryptographic authentication methods provide verification of nodes identity, but since much effort is required in authentication key management and additional infrastructural load it's not always possible. So a method/way for detecting spoofing attacks, and locating the positions of adversaries performing the attacks is proposed. Use of spatial information, a physical property associated with each and every node, which is difficult to falsify, and independent of cryptographic functions, as the basis for detecting the spoofing attacks, determining the number of attackers when multiple adversaries are masquerading as the same node identity and locating multiple adversaries. To be more precise K-means cluster analysis model that utilizes spatial information of received signal strength (RSS) inherited from wireless nodes is used to find the spoofing attacks and cluster-based mechanisms can be developed to determine the number of attackers. Ultimately the positions of the attackers can be identified using either area/ point-based localization algorithms with the same relative errors as in the normal case. We researched using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. Also used techniques for evaluation through two wireless adhoc networks.

Index Terms: Wireless network security, spoofing, attack detection, localization, AP-Access Point.

I. INTRODUCTION

Openness and flexibility of wireless networks helps to masquerade easily as other devices and enables an adversary. Due to vary nature of wireless and sensor networks, they are vulnerable to spoofing attacks where an attacker forge its identity to masquerade as another device, or creates multiple illegitimate identities Among various types of attacks, Identity based attacks- spoofing, are serious network threats as they can help a variety of advanced attacks to erode the normal operation of networks. A cluster analysis model that utilizes spatial information of received signal strength (RSS) inherited from wireless nodes is used to detect the spoofing attacks and cluster-based mechanisms are developed to determine the number of attackers. We researched using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. We evaluated techniques through two wireless adhoc networks and some other wireless network standard. Our experimental results show that our proposed methods can achieve over 88% Hit Rate and Precision when determining the number of attackers. Our localization results after using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

II. RELATED WORK

Cryptography is the traditional approach to detect and prevent spoofing attack. It requires secure key management and framework respective to that. The Public Key Interface (PKI) can be used further to reduce the overhead of key management [1][2]. In addition to avoid compromise with key, wool implemented key management mechanism which include periodic key refresh and host revocation. However because of the limited resources on wireless devices and lacking of a fixed key management infrastructure in the wireless network, such cryptographic authentication may not be always applicable. E.g. The Wired Equivalent Privacy protocol is used in networks to protect link-level data during wireless transmission. It represents following properties:-

WEP relies on a secret key shared between the communicating parties to protect the body of a transmitted frame of data.

A. Encryption of a frame proceeds as follows:

Encryption: In the 2nd stage, plaintext derived above is encrypted using RC4. We choose an Initialization vector (IV). The RC4 algorithm generates a key stream i.e., a sequence of long pseudorandom bytes—as a function of IV and the key. Then, exclusive-or (XOR, denoted by) the plaintext with the keystream is used to obtain the ciphertext.

B. Transmission

Transmit the IV & the ciphertext over the wireless link. As of now the current approaches use physical properties like RSS (Received Signal Strength) associated with wireless nodes so as to address spoofing attacks in the wireless network. The channel-based authentication scheme is proposed to discriminate between transmitters at different locations, and thus used to detect spoofing attacks in wireless networks [3]. Security layer introduced by Li and Trappe [5] that uses forge-resistant relationships based on the packet traffic, including MAC sequence number and traffic pattern, to detect spoofing attacks. Also The MAC sequence number has been used in [4] to perform spoofing detection. Both i.e. the sequence number and the traffic pattern can be manipulated by an adversary as long as the adversary learns the traffic pattern under normal conditions. The basic RSS work was also proposed in [6], [7] & [10]. However, none of these approaches were capable of determining the number of attackers when there are multiple adversaries collaborating to use the same identity to launch malicious attacks. Also they did not have the ability to localize the positions of the adversaries after attack detection. So here is the main point that our work uses the spatial information which helps to detect the attacks instead of any cryptographic scheme, and hence it differs from the techniques used previously. In Addition approach followed by us is innovative and more creative as it helps in finding number of spoofing attackers and also provides the accuracy in localizing such multiple adversaries masquerading with the same identity.

III. SYSTEM MODEL

Figure .2 Below gives the representation of the new security technique.

GADE (Generalized attack Detection Model):-

Has been used to propose RSS, a physical property co-related with location in physical space and even it is readily available in the existing wireless networks. As RSS can be affected due to random noise,

environmental bias, and multipath effects even then the RSS measured at a set of landmarks is closely related to the transmitter's physical location [9].According to RSS readings present strong spatial correlation characteristics. The RSS vector is defined with value vector as- S= {s1, s2, s3… sn} where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes which know their locations. In case of spoofing attack, the two important elements are-

- Victim
- Attacker

Using same ID and the RSS readings of that ID which is measured from each individual node (i.e., spoofing node or victim node) both can transmit data packets .Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, observations suggests that we may need to conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and there by further detect the presence of spoofing attackers in physical space. Here, we propose and opt to use Partitioning around Medoids (PAM) Method so as to perform clustering analysis in RSS. PAM is a popular iterative descent clustering algorithm [10]. In addition the evaluation results showed that PAM method is more robust than any popular K-means clustering algorithm [11].Particularly our objective in this method is to detect the presence of attacks. Null hypothesis here indicates that no spoofing attack. T is the Test spec i.e. (Test specification) that is used to indicate whether observed data belongs to the null hypothesis or not. Then consider the distance between two medoids as Dm.

Dm=¦Mi-Mj¦

Where Mi and Mj are the medoids of two clusters.

Under normal condition (i.e. No spoofing attack) there should be only one cluster from a single physical location. In such case Dm should be small. However, under a spoofing attack, as there are more than one node at different physical locations and hence Dm will be large. Model suggests that if the value of Dm distance is small then it means that there is no spoofing attack present in the system. But if Dm distance is large then it means that spoofing attack is detected.

IV. DETECTION PROBLEM IN MULTICLASS.

As the problem is in determining number of attackers and similar in determining how many clusters existing in the RSS readings. We have to check

Pi=Ci ; Ni= . cj € C

Here C is the set of all classes.ci is the specific number of attackers under particular class.Ni is the all other class as negative class. The related precision and F-measure are in [12].This gives the number of attackers in the system.

A. SILENCE Mechanism.

Figure 3. Shows Cluster Representation view.

SILENCE mechanism's basic Silhouette Plot for cluster is in [13][14].Based on the observation we used SILENCE, Silhouette Plot and System Evolution with minimum distance of cluster. Which helps in

evaluating the minimum distance between clusters so as to improve the accuracy of determining the number of attackers? It gives the K as number of attackers in the system. It also depends on Dm-that's the distance between medoids.

B. **Support Vector Machine**

(SVM) based mechanism. SVM is a set of kernel-based learning methods for data classification that involves training phase and a testing phase [15]. Each data instance in the training set consists of a target value (i.e., class label) and several attributes (i.e., features). The performance of determining number of

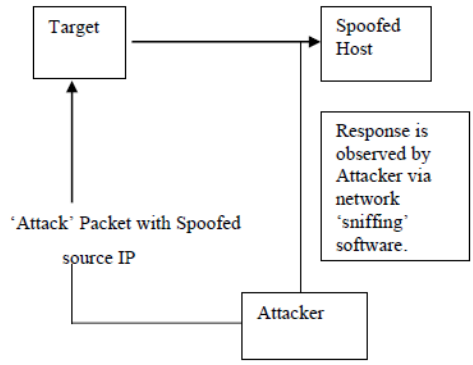

Figure 1. Spoofing of IP

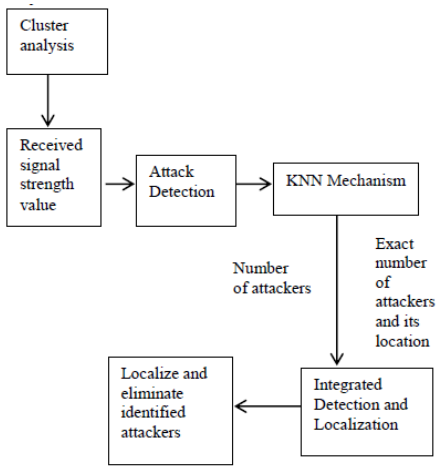

Figure 2 –Representation of security Technique

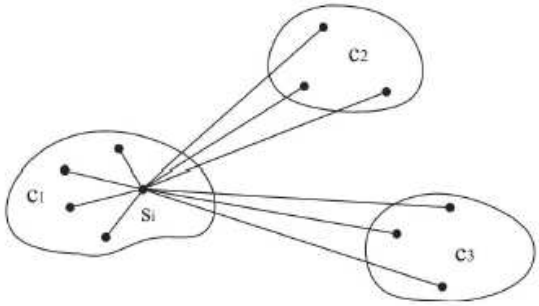

Figure 3. Cluster Representation View

spoofing attackers can be improved further by using SVM based mechanism. Here, SVM is used to classify the number of spoofing attackers and thereby to improve the detection rate. It accurately predicts the number of attackers using model based on training data. Comparison between the results of SVM to those of Silhouette Plot, System Evolution and SILENCE methods leads to the ultimate decision that SVM is the best one as it gives significant increase in Hit rate, Precision etc.

C. IDOL (Integrated Detection and Localization Model)

Our integrated detection and localization system makes use of localization algorithm to detect and estimate the positions of adversaries or attackers. This model utilizes RSS medoids returned from SILENCE as an inputs to localization algorithms. The resulted returned positions include the location

estimate of the original node along with the attacker in the physical space. When an adversary residing at a physical location

Varies its transmission power to perform a spoofing attack, the difference of the RSS readings from the adversary between two different landmarks is a constant since the RSS readings are obtained from a single physical location. We can then utilize the differences of the medoids vectors in signal space obtained from SILENCE to localize adversaries. In such a way on improving [14] the advanced enhancement is obtained as IDOL.

The proposed model makes use of localization algorithms such as given below

- Multi lateration algorithm
- RADAR Grid algorithm
- Area Based Probabilistic algorithm

V. CONCLUSION

While working with wireless devices used for communication. Have identified that extracting and throwing out the attackers is getting huge interest in any Client and Server based communication. This is due to the fact that a considerable amount of secure communication and data security is required. Since the existing systems have number of flaws with the methods used and algorithm followed. In order to increase the data security new functions, methods and paths are used so that the attackers are identified and thrown out which is lacking in existing system.

VI. REFERENCES

[1] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, .Secure and Efficient Key Management in Mobile Ad Hoc Networks,. Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.

[2] 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

[3] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, .Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication, Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4646-4651, June 2007.

[4] F. Guo and T. Chiueh, .Sequence Number-Based MAC Address Spoof Detection,. Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.

[5] Q. Li and W. Trappe, .Relationship-Based Detection of Spoofing- Related Anomalous Traffic in Ad Hoc Networks, Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[6] D. Faria and D. Cheriton, .Detecting Identity-Based Attacks in Wireless Networks Using Signalprints,. Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, .Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proc. IEEE INFOCOM, Apr. 2008.

[8] L. Sang and A. Arora, .Spatial Signatures for Lightweight Security in Wireless Sensor Networks, Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.

[9] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, .A Practical Approach to Landmark Deployment for Indoor Localization,.Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks.(SECON), Sept. 2006.

[10] L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. Wiley Series in Probability and Statistics, 1990.

[11] G. Zhou, T. He, S. Krishnamurthy, and J.A. Stankovic, .Models and Solutions for Radio Irregularity in Wireless Sensor Networks,.ACM Trans. Sensor Networks, vol. 2, pp. 221-262, 2006.

[12] C. van Rijsbergen, Information Retrieval, second ed. Butterworths,1979.

[13] P. Rousseeuw, .Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis,. J. Computational and Applied Math., vol. 20, no. 1, pp. 53-65, Nov. 1987.

[14] K. Wang, .Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data,. Technical Report NO. 2007-258, Computer Science Dept., Xidian Univ., P.R. China, 2007.

[15] D. Madigan, E. Elnahrawy, R. Martin, W. Ju, P. Krishnan, and A.S. Krishnakumar, .Bayesian Indoor theorem..

