ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Detection of Tricking Attack and Localization Of Deceivers In Multiple Wireless Networks

Srividhya.A[1], Ms.M. Anitha[2]

M.E CSE, Department of computer science, P.S.V. College of engineering & technology, Krishnagiri, Tamilnadu, India[1]

Assistant Professor, Department of computer science, P.S.V. College of engineering & technology, Krishnagiri, Tamilnadu, India[2]

Abstract: Wireless Tricking attack means it is the situation in which one person or program masquerading another for illegitimate advantage. Here person is not authorized but pretend to be authorized for gaining illegal access. Because of this attack network performance is reduced and openness of wireless transmission medium, adversaries can monitor any transmission. In existing system cryptographic mechanisms are used for detecting this tricking attack but it is not always desirable because of the overhead of requirements and maintance mechanisms. In this paper spatial correlation of received signal strength (RSS) inherited from wireless nodes is used to detect the tricking attacks. And also an integrated detection and localization system is developed that can localize the positions of multiple attackers. This paper is to address the problem in wireless networks that happens by tricking attack. In existing system only detection of tricking attack is occurred. But in our scheme localization and prevention of tricking attacks is occurred.

Keywords: Wireless network security, Tricking attack, attack detection, localization.

I. INTRODUCTION

The openness of the wireless transmission medium, adversaries can monitor any transmission. Further, adversaries can easily purchase low-cost wireless devices and use these commonly available platforms to launch a variety of attacks with little effort. Among various types of attacks, identity-based tricking attacks are especially easy to launch and can cause significant damage to network performance. For instance, in an 802.11 network, it is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an ifconfig command to masquerade as another device. The existing 802.11 security techniques including Wired Equivalent Privacy, Wi-Fi Protected Access such methodology can only protect data frames an attacker can still spoof management or control frames to cause significant impact on networks.

1.1 ABOUT THE TRICKING ATTACK

Tricking attacks can further facilitate a variety of traffic injection attacks such as attacks on access control lists, rogue access point attacks, and eventually Denial of Service attacks. A broad survey of possible Tricking attacks can be found in. Moreover, in a large scale 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 (DOS) attack quickly. Therefore, it is important to detect the presence of Tricking attacks, determine the number of attackers and localize multiple adversaries the spatial correlation is used here for detecting multiple adversaries and eliminates them. An added advantage of employing spatial correlation to detect Tricking attacks is that it will not require any additional cost or modification to the wireless devices themselves. The theoretical analysis and generalized attack is also occurred for detecting the attackers. Intrusion detection and localize for the system is used for detection and also finding the position of multiple adversaries.

One key observation in intrusion detection is that can handle attackers using different transmission power levels, thereby providing strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network

1.2 OVERVIEW

Here received signal strength-based spatial correlation used, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting Tricking attacks in wireless networks. The theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. The test statistic based on the cluster analysis of RSS readings. Our approach can detect the presence of attacks as well as determine the number of adversaries, tricking the same node identity, so that we can localize any number of attackers and eliminate them

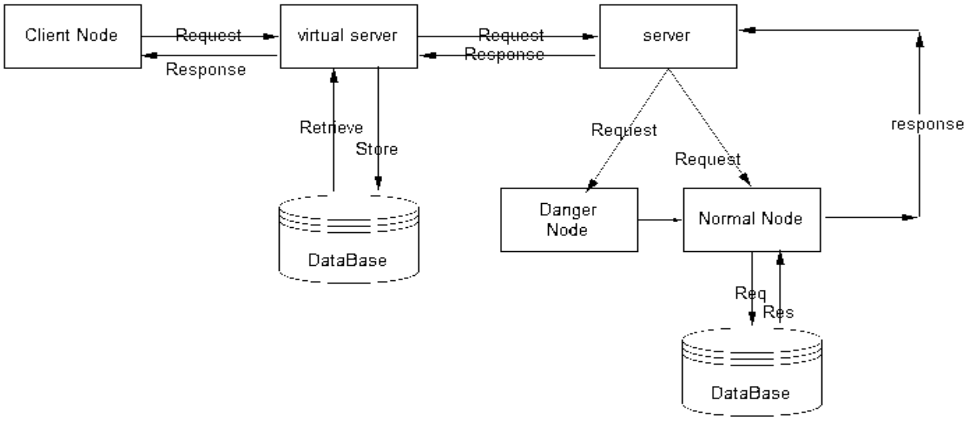

FIG 1 ARCHITECTURE DESIGN

SILENCE, a 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. Additionally when the training data are available explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system. Further, based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission.

1.3 SYSTEM ANALYSIS

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 Tricking attacks determining the number of attackers and localizing adversaries. The path loss exponent is set to 2.5 and the standard deviation of shadowing is 2 dB.From the ROC curves shift to the upper left when increasing the distance between two devices.

It shows that the two nodes are separated thus the better detection performance can be achieved. By means of a Tricking attack, the RSS readings from the victim node and the attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of tricking attackers in physical space. The new method to evolutes the System evolution used to analyses the data structure and also estimates the number of clusters. The System Evolution method uses the twin-cluster model, which are the two closest clusters among K potential clusters of a data set.

This model is used for the energy calculation. The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energies calculated as the average distance between elements in the border region of the twin clusters

II. LITERATURE SURVEY

In cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned. In this work, the received signal strength (RSS)-based spatial correlation is used, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting tricking attacks. The attackers are in different locations than the legitimate wireless nodes we are concerned with the utilizing spatial information to address tricking attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. To detect tricking attacks it will not require any additional cost or modification to the wireless devices themselves it is also an advantage. The large-scale 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. The accuracy of determining the number of attackers. Additionally, when the training data are available, we propose to use the Support Vector Machines method to further improve the accuracy of determining the number of attackers. Here 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.[1].The several attack detection schemes for wireless localization systems. The first formulate a theoretical foundation for the attack detection problem using statistical significance testing. Next, define test metrics for two broad localization approaches: multilateration and signal strength. Here the attack detection is get occurred by using many theoretical analysis and by means of the tests and also by using the signal strength. Here the process derived both mathematical models and analytic solutions for attack detection for any system that utilizes those approaches. The studied additional test statistics that are specific to a diverse set of algorithms.[3].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. 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. [7]

III. ALGORITHM AND TECHNIQUES

3.1 BAC GENEREATION

The stream packets are clustered to blocks, denoted as block[i], with b Packets in each block, where 0 <i< |total packet number/b|. Padding is used when necessary to generate the last block. The length (in terms of bits) of the BAC for each data block is n. A hash function, denoted as H(X), is a one-way hash, using an algorithm Such as MD5 or SHA.X, Y represents the concatenation of X with Y.A secret key k is only known to the communicating parties. The origin of the data stream can be identified by a flag, which is f bits, Where 0≤f≤ n.

3.2 ATTACK DETECTION USING CLUSTER ANALYSIS

The analysis provides the theoretical support of using the RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection. It also showed that the RSS readings from a wireless node may fluctuate and should cluster together. In particular, the RSS readings over time from the same physical location will belong to the same cluster points in the dimensional signal space, while the RSS readings from different locations over time should form different clusters in signal space. Under the tricking attack, the victim and the attacker are using the same ID to transmit data packets, and the RSS readings of that ID is the mixture readings measured from each individual node (i.e., spoofing node or victim node). Since under tricking attack, the RSS readings. from the victim node and the attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space. In this work, we utilize the Partitioning around Medoids Method to perform clustering analysis in RSS. The PAM Method is a popular iterative descent clustering algorithm. Compared to the popular K-means method the PAM method is more robust in the presence of noise and outliers. Thus PAM method is more suitable in determining clusters from RSS streams, which can be unreliable and fluctuating over time due to random noise and environmental bias. Thus the detection is formulate as a statistical significance testing problem, where the null hypothesis is whether observed data belong to the null-hypothesis or not. In particular, in attack detection phase, partition of the RSS vectors from the same node identity into two clusters (i.e., K ¼ 2) no matter how many attackers are using this identity, since our objective in this phase is to detect the presence of attacks. Thus the distance between two Medoids as the test statistic in our significance testing for tricking detection and are the Medoids of two clusters. Under normal conditions, the test statistic should be small since there is basically only one cluster from a single physical location. However, under attack, there is more than one node at different physical locations claiming the same node identity. As a result, more than one cluster will be formed in the signal space and will be large as the Medoids are derived from the different RSS clusters associated with different locations in physical space.

3.3THE SILENCE MECHANISM

The advantage of Silhouette Plot is that it is suitable for estimating the best partition. Whereas the System Evolution method performs well under difficult cases such as when there exists slightly overlapping between clusters and there are smaller clusters near larger clusters. However, we observed that for both Silhouette Plot and System Evolution Methods, the Hit Rate decreases as the number of attackers increases, although the Precision increases. This is because the clustering algorithms cannot tell the difference between real RSS clusters formed by attackers at different position and fake RSS clusters caused by outliers and variations of the signal strength.

IV. MODELS AND DEFINITION

4.1LOGIN PROCESS DENIAL OF SERVICES

The continuous login-requests will lead to overwhelm the login process that require the presentation tier to access the authentication mechanism, rendering it unavailable or unreasonably slow to respond. Generic error message will display while the user enters an incorrect username and/or password. If the application explicitly states which component of the username/password pair was incorrect then an attacker can automate the process of trying common usernames from a dictionary file in an attempt to enumerate the users of the application. While applications may handle authentication failure messages correctly, many still allow attackers to enumerate users through the forgotten password feature.

4.2 KEY DISTRIBUTION

In private key cryptography the parties involved all need to be in possession of the same secret key in order to be able to successfully communicate. But how they distribute such a secret key? We cannot just send it over an insecure channel and encrypting it also does not work, since then the receiving party will not be able to decrypt it. There are quite a few variations of this problem. We will start out assuming that there is no previously shared information between the participating parties. The solution to that setting and also gave rise to public key cryptography in their truly revolutionary

4.3 GROUP ATTACKER MODULES

The attacks includes the depletion of the application service resource at the server side it will produce maximum destruction, the unavailability of service access to legitimate user, and possible fatal system errors which require rebooting the server for recovery. For that any malicious behaviors can be discovered by monitoring the service resource usage, based on dynamic value thresholds over the monitored objects. Data manipulation and system intrusion are out of this scope. That application interface presented by the servers can be readily discovered and clients communicate with the servers using HTTP/1.1 sessions on TCP connections.

V. CONCLUSION AND FUTURE ENHANCEMENT

5.1 CONCLUSION

A novel technique for detecting application DOS attack by means of a new constraint-based group testing model. Motivated by classic GT methods, three detection algorithms were proposed and a system based on these algorithms was introduced Theoretical analysis and preliminary simulation results demonstrated the outstanding performance of this system in terms of low detection latency and false positive/negative rate. Our focus of this paper is to apply group testing principles to application DOS attacks, and provide an underlying framework for the detection against a general case of network assaults, where malicious requests are indistinguishable from normal more efficient d-disjunction matrix could dramatically decrease the detection latency, as we showed in the theoretical analysis.

5.2 FUTURE ENHANCEMENT

We will continue to investigate the potentials of this scheme and improve this proposed system to enhance the detection efficiency. The sequential algorithm can be adjusted to avoid the requirement of isolating attackers. More efficient d-disjunction matrix could dramatically decrease the detection latency, as we showed in the theoretical analysis. A new construction method for this is to be proposed and can be a major theoretical work for another paper. The overhead of maintaining the state transfer among virtual servers can be further decreased by more sophisticated techniques.

VI. ACKNOWLEDGEMENT

First and Foremost, I would like to thank my graduate advisor, Asst.prof. Anitha .M, for his guidance and encouragement throughout my graduate studies. His vast knowledge and working experience in computer science and engineering have proven invaluable in my quest to learn and grow. I would also like to thank my other professors and advisors, Prof. Sakthivel .B, for their constructive support, camaraderie, and teamwork. My studies would not have been the same without their contributions. Finally, but definitely not least, I want to thank my parents for their loving encouragement and grounding support at home which allowed me to concentrate and complete my work.

REFERENCES

[1]. J. Bellardo and S. Savage, "Detecting Spoofing Attacks in Mobile Wireless environments" Proc. USENIX Security Symp. pp. 15-28,2003.
[2]. F. Ferreri, M. Bernaschi, and L. Valcamonici, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength" Proc. IEEE Wireless Comm. and Networking.2004
[3]. D. Faria and D. Cheriton, "Attack Detection in Wireless Localization" Proc. ACM Workshop Wireless Security (Wise), Sept. 2006
[4]. Q. Li and W. Trappe, "Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data," Proc. Ann. IEEE Comm. Soc. On IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006
[5]. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Detecting and Localizing Wireless Spoofing Attacks," Proc IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005
[6]. A. Wool, "secure and efficient key management," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005
[7]. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "sequence number based spoof detection" Proc. IEEE INFOCOM, Apr. 2008
[8]. J. Yang, Y. Chen, and W. Trappe, "Lightweight Key Management for IEEE 802.11 Wirelesses Lans with Key Refresh and Host Revocation"Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.
[9]. Y. Chen, W. Trappe, and R.P. Martin, "comparison methods for support vector machines"Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007
[10] M. Bohge and W. Trappe, "Bayesian indoor postioning systms" Proc. ACM Workshop Wireless Security (Wise), pp. 79-87, 2003.