International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 1 (2016) pp 286-289
© Research India Publications. http://www.ripublication.com

Spoofing Assault Identification and Limiting Several Adversaries in Wireless Networks

Jayanthi .R
Assistant Professor (SITE) Vellore Institute of Technology, Vellore, India.
E-mail: profjai14@gmail.com

Siva Rama Krishnan S
Assistant Professor(Sr), (SITE) Vellore Institute of Technology, Vellore, India.
E-mail: siva.s@vit.ac.in

Rama Prabha K.P
Assistant Professor (SITE) Vellore Institute of Technology, Vellore, India.
E-mail: mail2ramaprabha@gmail.com

Abstract
Wireless based spoofing assaults are light to hit and can effectively impact the functionality of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. 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 spoofing attacks are especially easy to launch and can cause significant damage to network performance. We proposed to use received signal strength-based spatial correlation, 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.We provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. Our approach can detect both the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them.

Keywords: wireless, safety, transmission, spoofing, network

Introduction

The openness of the wireless transmission medium, adversaries can look at 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 spoofing assaults are especially easy to launch and can cause significant damage to network functionality. For instance, in an 802.11 network, it is easy for an hit to gather useful MAC (Media Access Control) address information during passive monitoring and then modify its MAC address by simply issuing an if configuration 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. Spoofing assaults 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 spoofing 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 spoofing assaults, 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 spoofing 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

Existing System

The existing approaches to address potential spoofing attacks employ cryptographic schemes. Cryptographic schemes application requires reliable key distribution, management, and maintenance mechanisms. Because of its infrastructural, computational, and management overhead the Cryptographic method is not desirable to apply. However 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 spoofing attacks. The attackers are in different locations than the legitimate wireless nodes we are concerned with the utilizing spatial information to address spoofing attacks has the unique power to not only identify

the presence of these attacks but also localize adversaries. To detect spoofing attacks it will not require any additional cost or modification to the wireless devices themselves it is also an advantage.

A. Deficiency Of The Existing System

- 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.

Proposed System

The path loss exponent is set to 2.5 and the standard deviation of shadowing is 2 databases. From the figure, we observed that 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. This is because the detection performance is proportional to the no centrality parameter which is represented by the distance between two wireless nodes together with the landmarks. By means of a spoofing attack, the RSS readings from the victim node and the spoofing 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. 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.

A. Proposed Algorithm (Bac Genereation)

To present our scheme, we use the following notations:

1. 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
2. The length (in terms of bits) of the BAC for each data block is n.
3. A hash function, denoted as H(X), is a one-way hash, using an algorithm such as MD5 or SHA.
4. X, Y represents the concatenation of X with Y.
5. A secret key k is only known to the communicating parties.
6. The origin of the data stream can be identified by a flag, which is f bits, where 0≤f≤ n

B. Advantages Of Proposed System

- The basic idea behind using the System Evolution method to determine the number of attackers is that all the rest of clusters are separated if the twin clusters are separable.
- The Hit Rate is lower when treating four attackers as errors than treating two attackers as errors.
- errors.

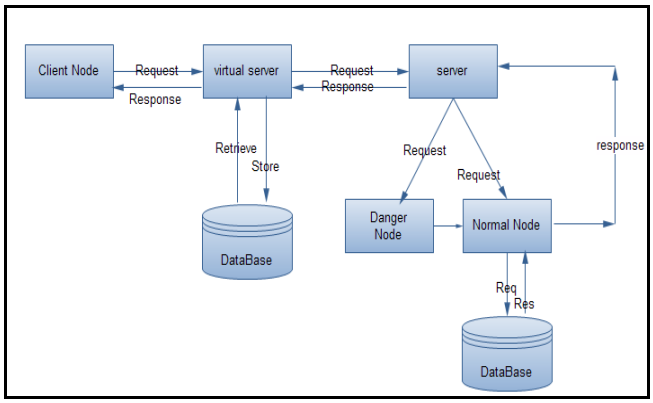

Figure 1: System Architecture

Implementation And Results

A. Login 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.

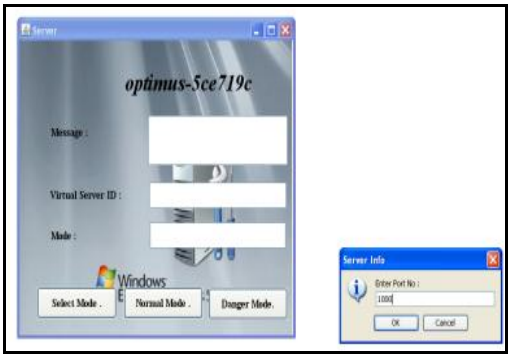

Figure 2: Login password denial of service

B. 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 revolution.

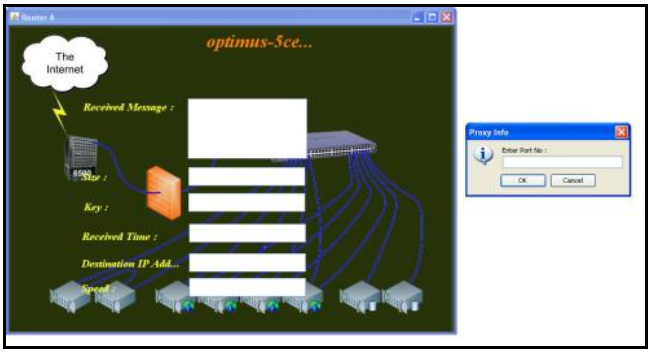

Figure 3: Key Distribution

C. 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. The each client provides a not assaulted ID, which is utilized to identify the client during our detection period. Despite that the application Hit is difficult to be traced by identifying the IDs of attackers the firewall can block the subsequent malicious requests. The attackers are assumed to launch application service requests either at high inter arrival rate or high workload, or even both. he term "request" refers to either main request or embedded request for HTTP page. Since the detection scheme proposed will be orthogonal to the session affinity, we do not consider the repeated one shot attack mentioned in. We further assume that the number of attackers d << n where n is the total client amount. It will produce from the characteristics of this attack. The constraint can be relaxed by benefits of virtual servers, but we keep it for the theoretical analysis in the current paper.

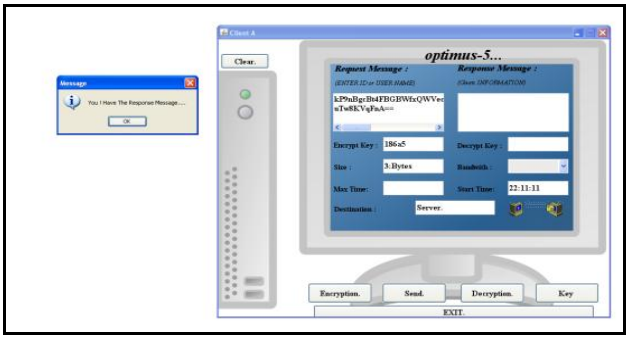

Figure 4: Group Attack Modules

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. 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.
- Even that process is already have quite low false positive/ negative rate from the algorithms,

That can still improve it via false-tolerant group testing methods.

Future Work

We will continue to investigate the potentials of this scheme and improve this proposed system to enhance the detection efficiency.

1. The sequential algorithm can be adjusted to avoid the requirement of isolating attackers.
2. 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.
3. The overhead of maintaining the state transfer among virtual servers can be further decreased by more sophisticated techniques.

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] 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] 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 postioningsystms" Proc. ACM Workshop Wireless Security (Wise), pp. 79-87, 2003.

[11] 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

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008

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

[14] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security''2145, 2008.

[15] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE. INFOCOM, 2000

[16] M. Youssef, A. Agrawal, and A. U. Shankar, "WLAN location determination via clustering and probability distributions," in Proceedings of IEEE PerCom'03, Fort Worth, TX, Mar. 2003.

[17] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in Proceedings of the 2003 ACM workshop on wireless security, 2003, pp. 1–10.

[18] Jiang .W and Clifton .C, "A secure distributed framework for achieving anonymity," vol. 15, no.4,pp 316-333,2006.