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. 3, Issue 4, April 2015

Detection and Localization Multiple spoofing Attackers in wireless in Networks

Dr.D.Parameswari[1], Kannan Subramanian[*2]

[1] Assistant Professor, Dept. of Master of Computer Application, Jerusalem College of Engineering, Chennai, Tamil Nadu, India

[2] Associate Professor, Dept. of Master of Computer Application, Bharath University, Chennai, Tamil Nadu, India

[*] Corresponding Author

ABSTRACT: Wireless spoofing attacks are easy to launch and can significantly impact the performance 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. This paper, propose to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting spoofing attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. This project propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. The project formulate the problem of determining the number of attackers as a multiclass detection problem. In addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers. Our localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

I. INTRODUCTION

The project has named" Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" for detecting multiple attackers in wireless networks.Due to 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. 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 ifconfigcommand to masquerade as another device. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA), or 802.11i (WPA2),such methodology can only protect data frames.An attacker can still spoof management or control frames to cause significant impact on networks.

The project is about how the data can be transferred from one node to another.The project also detect the attackers who tries to masquerades the data. The project use normalized entropy which calculates the over all probability distribution in the captured flow in our algorithm to get more accurate result. The aim of attack detection and recovery is to detect DDoS attack before it affects the end user . Intrusion detection systems are widely used for DdoS detection. An Intrusion detection system (IDS) is software and/or hardware which will monitor the network or a computer system for suspicious activity and alerts the system manager or network administrator.

II. MODULE DESCRIPTION

Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and effective [1]. Implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system.

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. 3, Issue 4, April 2015

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. A simple operating procedure is included so that the user can understand the different functions clearly and quickly [2-3].

III. MODULE DISCRIPTION

- Registration form
- Login Form
- Server Monitoring
- Man In The Middle Attack
- Denial of service Attack
- Session Hijacking
- Eaves Dropping

A. *REGISTRATION FORM*

This module contains the Registration Details.The Registration details contains username ,password,emailid,contact no etc,.To login to the page for transferring the file we should register with this form [4].

B.*LOGIN FORM*

To transfer a file, user should login to the page .The Login Form contains the Username and the password details.Once we enter a valid username and the password it redirects to the transfer page [5].

C.*SERVER MONITORING*

This module continuously monitoring the all request from the Client. When the request is coming, it identifies the IP address and stored in cache and starts counting the request from the same IP address and also maintains the timer [6].

D.*MAN IN THE MIDDLE ATTACK*

The **man-in-the-middle attack** is a kind of attack in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones.The below Fig 1.shows how the attack will take place [7].

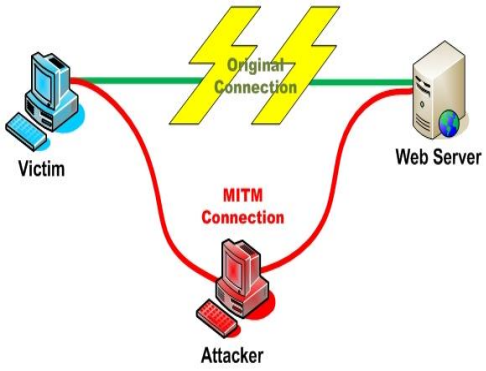

Fig 1.Man In The Middle Attack

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. 3, Issue 4, April 2015

E.*DENIAL OF SERVICE ATTACK(DOS):*

In this project, A DOS attack involves sending large number of packets to a destination to prevent legitimate users from accessing information or services. Zombies are gathered to send useless service requests continuously , packets at the same time. DOS attacks are targeted at stealing, modifying or destroying information.Fig.2. shows the DOS attack [8].

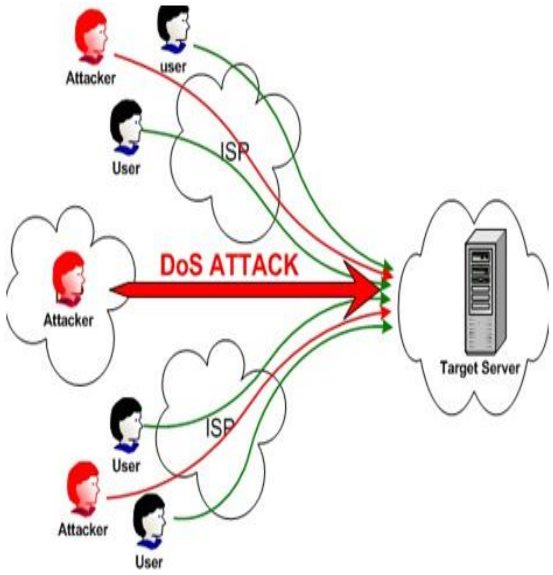

Fig 2.DOS Attack

F.*SESSSION HIJACKING*

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer, to gain unauthorized access to information or services in a computer system.The below Fig 3. shows how session hijacking is taken place [9].

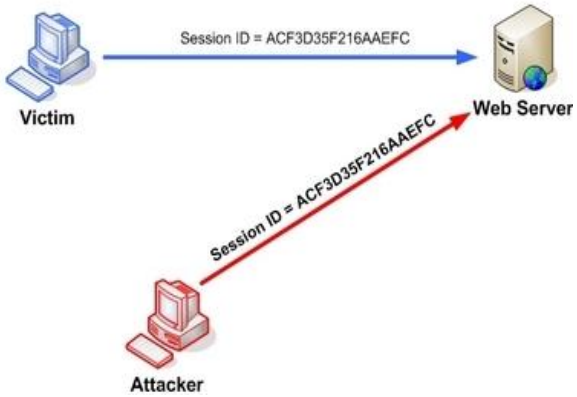

Fig 3.Session Hijacking

5.2.7.*EAVES DROPPING*

Eavesdropping is the act of secretly listening to the private conversation of others without their consent. This is commonly thought to be unethical and there is an old adage that "eavesdroppers seldom hear anything

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. 3, Issue 4, April 2015

good of themselveseavesdroppers always try to listen to matters that concern them.Fig4.Shows how the eavesdropping is done [10].

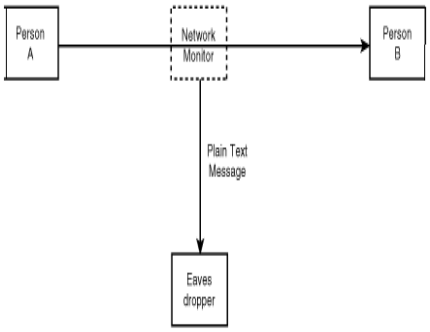

Fig 4.Eaves Dropping

IV. EXPERIMENTAL RESULT

HACKER FORM:

To use hacking mode we have to click to the ON radio button to activate hacker mode.Fig.5.shows the hacking mode on form [11].

Fig.5.Hacker Form.

After clicking the on mode ,we will see a hacker form with five attacks namely Man in the middle attack,sessionhijacking,DDOSattack,eaves dropping.Fig.6.shows the attacker form [12].

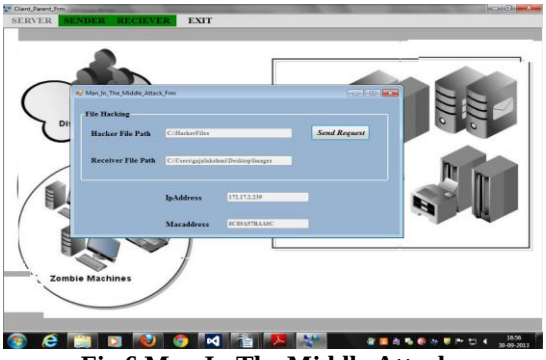

Fig 6.Man In The Middle Attack.

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. 3, Issue 4, April 2015

V. FUTURE ENHANCEMENTS

After implementing and testing the database we found that it almost fulfilled all of the requirements of our abstract and system designing considerations. The application is working smoothly for all its users, such as transferring the file and detecting the attackers. In further we will try to solve our limitation and we are hopeful next time it will be a complete localizing and detecting attackers.

VI. CONCLUSION

In this work, we proposed to use received signal strengthbased 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. We derived the test statistic based on the cluster analysis of RSS readings. Our approach can both detect 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. Determining the number of adversaries is a particularly challenging problem. Additionally, when the training data are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system. We found that our detection mechanisms are highly effective in both detecting the presence of attacks . Further, based on the number of attackers determined by our mechanisms, our integrateddetection and localization system can localize any number of adversaries even when attackers using different transmission power levels.

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.
2. Niranjan U., Subramanyam R.B.V., Khanaa V., "Developing a Web Recommendation System Based on Closed Sequential Patterns", Communications in Computer and Information Science, ISSN : 1865-0929, 101() (2010) PP.171-179.
3. F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access points vulnerabilities to dos attacks in 802.11 networks,” in Proceedings of the IEEE Wireless Communications and Networking Conference, 2004.
4. Das S., Das M.P., Das J., "Fabrication of porous chitosan/silver nanocomposite film and its bactericidal efficacy against multi-drug resistant (MDR) clinical isolates", Journal of Pharmacy Research, ISSN : 0974-6943, 6(1) (2013) PP. 11-15.
5. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and efficient key management in mobile ad hoc networks,” in Proc. IEEE IPDPS, 2005.
6. A. Wool, “Lightweight key management for ieee 802.11 wireless lans with key refresh and host revocation,” ACM/Springer Wireless Networks, vol. 11, 2005.
7. Anbuselvi S., Jeyanthi Rebecca L., Sathish Kumar M., Senthilvelan T., "GC-MS study of phytochemicals in black gram using two different organic manures", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(2) (2012) PP. 1246-1250.
8. M. bohge and W. Trappe, “An authentication framework for hierarchical ad hoc sensor networks,” in Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003.
9. Beula Devamalar P.M., Thulasi Bai V., Srivatsa S.K., "Design and architecture of real time web-centric tele health diabetes diagnosis expert system", International Journal of Medical Engineering and Informatics, ISSN : 1755-0661, 1(3) (2009) PP.307-317.
10. Herbert Schildt,”The Complete Reference C#”,TataMcGRAW- Hill edition.
11. Sharmila S., Jeyanthi Rebecca L., Saduzzaman M., "Biodegradation of domestic effluent using different solvent extracts of Murraya koenigii", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 5(2) (2013) PP.279-282.
12. James R.Groff, Paul N.Wcinberg, and Andrew J.Oppel,”The Complete Reference SQL”,TataMcGRAW-Hill Third Edition.
13. B Karthik, TVU Kirankumar, MS Raj, E BharathKumaran,Simulation and Implementation of Speech Compression Algorithm in VLSI, Middle-East Journal of Scientific Research 20 (9), PP 1091-1092, 2013
14. M.Sundararajan & R.Pugazhanthi,” Human finger print recognition based biometric security using wavelet analysis”, Publication of International Journal of Artificial Intelligent and Computational Research, Vol.2. No.2. pp.97-100(July-Dec 2010).
15. .M.Sundararajan & E.Kanniga,” Modeling and Characterization of DCO using Pass Transistor”, proceeding of Springer – Lecturer Notes in Electrical Engineering-2011 Vol. 86, pp. 451-457(2011). ISSN 1876-1100.(Ref. Jor- Anne-II)
16. .M.Sundararajan & C.Lakshmi, “Wavelet based finger print identification for effective biometric security”, Publication of Elixir Advanced Engineering Informatics-35(2011)-pp.2830-2832.
17. .M.Sundararajan, ”Optical Instrument for correlative analysis of human ECG and Breathing Signal” Publications of International Journal of Biomedical Engineering and Technology- Vol. 6, No.4, pp. 350-362 (2011). ISSN 1752-6418.(Ref. Jor-Anne-I
18. M.Sundararajan, C.Lakshmi & D.Malathi, “Performance Analysis Restoration filter for satellite Images” Publications of Research Journal of Computer Systems