International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 3, Issue 10, October 2014

DETECTING THE ATTACKS AND CONFINING NUMEROUS ADVERSARIES IN WIRELESS SPOOFING ATTACK

Vengadapathiraj.M [1], Rajendhiran.V [2], sathish kumar.R[3],Vinoth kannan.A[4]
[1,2]P.G student Department of Applied Electronics, IFET College Eng. Tamilnadu, India
[3]P.G student Department of computer science and engineering, IFET College Eng. Tamilnadu, India
[4] Assistant Professor Department of electronics and communication Eng., IFET College Eng. Tamilnadu, India

***Abstract*:** Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Even though the uniqueness of a node can be proved through cryptographic authentication, conventional security methods are not always desirable because of their overhead requirements. In this work propose to use spatial statistics, a somatic property related with every node, hard to fiddle, and not reliant on cryptography, as the root for 1) identifying spoofing attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. Proposed to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. Then formulate the problem of determining the number of attackers as a multiclass revealing problem. Cluster-based mechanisms are developed to determine the number of attackers. When the training data are available, explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, developed an integrated detection and localization system that can localize the positions of multiple attackers.Evaluated the techniques through two test beds using in cooperation an 802.11 (Wi-Fi) network and an 802.15.4 (ZigBee) networks in two real office structures.Experimental results displays that proposed methods can achieve over 89 percent Hit Rate and Accuracy when determining the number of attackers. Localization results using a descriptive set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

Index terms-Spoofing attacks,crypyographic authentication

I.INTRODUCTION

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 ifconfig command to masquerade as another device. In spite of existing 802.11 security techniques including wired Equivalent Privacy (P), 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. Proposed a method for detecting spoofing attacks as well as localizing the adversaries in wireless and sensor networks. In contrast to traditional identity-oriented authentication methods, RSS based approach does not add additional overhead to the wireless devices and sensor nodes. Formulated the spoofing detection problem as a classical statistical significance testing problem.Then utilized the K-means cluster analysis to derive the test statistic. Further, built a real-time localization system and integrated K-means spoofing detector into the system to locate the positions of the attackers and as a result to eliminate the adversaries from the network. After analysing the requirements of the task to be performed, the next step is to analyse the problem and understand its context. The first activity in the phase is studying the existing system and other is to understand the requirements and domain of the new system. Both the activities are equally important, but the first activity servesas a basis of giving the functional specifications and then successful design of the proposed system.

ISSN: 2278 – 909X

II.WIDESPREAD ATTACK REVEALING FORM

Using methods like GADE (flow monitoring algorithm) show the process of detection of DOS attacks based on RSS value

- Current rss value of client will be checked
- Then it is compared with default rss value
- If the value exceeds the threshold then dos attack occurred
- The above mentioned details will be forwarded to prevention module

2.1 MAN-IN THE MIDDLE ATTACK:

Server will check all the requested client address and file path. Server will check file transfer details.ie verify whether the files are transferred based on client file path to corresponding IP address If the files are not transferred to correct path and IP address then man in the middle attack detected The above mentioned detail will be forwarded to prevention

2.2 SESSION HIJACKING:

Server will check all the client session details. Compare session details with the values stored in the Database, if session ID of two requested clients is same at the same time then session hijacking has occurred. The above mentioned detail will be forwarded to prevention sub-module.

2.3 FLOW MONITORING ALGORITHM:

First no of flows x1, x2…xn will be set to zero and parameters c, will be initialized.
Then the no of packets per flow is calculated by the formula/
The values will be saved and used by the server at the time of request from client
I/p: no of packets during a time interval.
O/p: packet (rss value) where rss=no of packets at a particular time.
Also in order to detect it uses the following formula to calculate the difference .If there is a difference then it usesTraceback algorithm to detect the attacker.

2.4 TRACEBACK ALGORITHM

Initialize a set A and obtain the local parameter of C.Let U={ui},I be a set of upstream routers, D ={di},I be a set of the destinations of the packets and V be the victim for i=1 to n Calculate H(F/ui) If (|H(F)-C|Based on the details ,the server will traceback to the both the victim and attacker using their IP and Mac address to find the real client who made request. Then the attacker will be blocked for a particular time interval and the corresponding detail will be stored in the database. The next time if the client uses same IP and Mac address the client will be blocked without any further analysis.

III.FUTURE WORK

A traditional security approach to cope with identity fraud is to use cryptographic authentication. An authentication framework for hierarchical, ad hoc sensor networks is proposed in and a hop-by-hop authentication protocol is presented in.Additional infrastructural overhead and computationalpower are needed to distribute, maintain, and refresh the key management functions needed for authentication. Has introduced a secure and efficient key management framework (SEKM).SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group. Implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. In addition, binding approaches are employed by Cryptographically Generated Addresses (CGA) to defend against the network identity spoofing. Due to the limited resources in wireless and sensor nodes, and the infrastructural overhead needed to maintain the authentication mechanisms, it is not always desirable to use authentication. Recently new approaches have been proposed to detect the spoofing attacks in wireless networks. Have introduced a security layer that is separate from conventional network authentication methods.

They developed forge-resistant relationships based on packet traffic by using packet sequence numbers, traffic interarrival, one-way chain of temporary identifiers, and signal strength consistency checks to detect spoofing attacks. Proposed a lower layer approach that utilizes properties of the wireless channel at the physical layer to support high-level security objectives such as authentication and confidentiality. The most closely related work to this paper is which proposed the use of matching rules of signal prints for spoofing detection.

ISSN: 2278 – 909X

IV.SYSTEM ARCHITECTURE

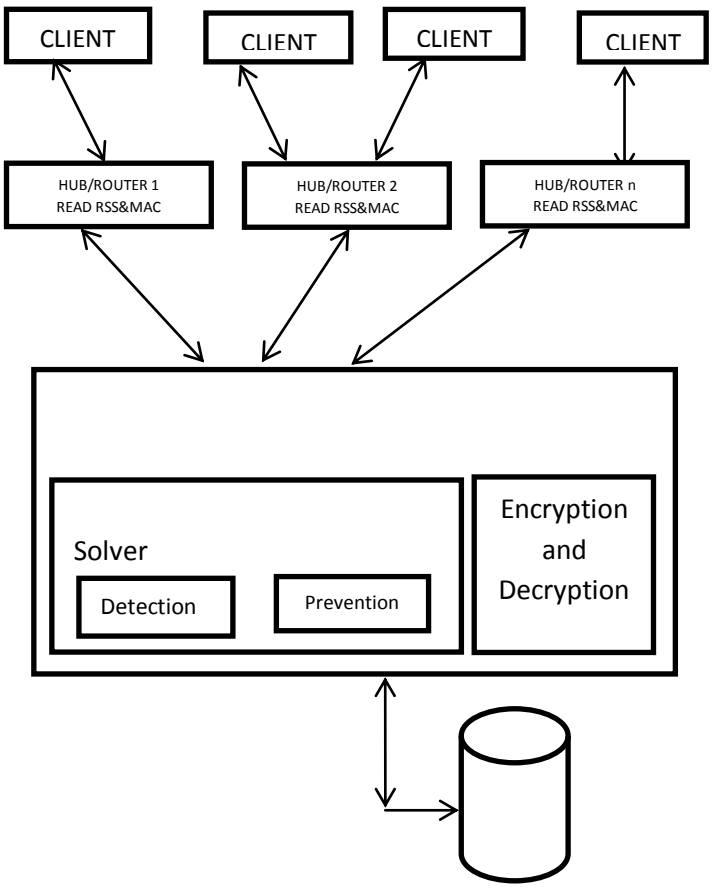

Fig.Architecture of Grid Environment

Technical Feasibility centres on the existing computer system hardware, software, etc. and to some extent how it can support the proposed addition. This involves financial considerations to accommodate technical enhancements. Technical support is also a reason for the success of the project. The techniques needed for the system should be available and it must be reasonable to use. Technical Feasibility is mainly concerned with the study of function, performance, and constraints that may affect the ability to achieve the system. By conducting an efficient technical feasibility need to ensure that the project works To solve the existing problem area. Since the project is designed with ASP.NET with C# as Front end and SQL Server 2000 as Back end, it is easy to install in all the systems wherever needed. It is more efficient, easy and user-friendly to understand by almost everyone. Huge amount of data can be handled efficiently using SQL Server as back end. Hence this project has good technical feasibility.

V.OPERATIONAL FEASIBILITY

People are inherently instant to change and computers have been known to facilitate change. An estimate should be made to how strong a reaction the user staff is likely to have towards the development of the computerized system. The staffs are accustomed to computerized systems. These kinds of systems are becoming more common day by day for evaluation of the software engineers. Hence, this system is operationally feasible. As this system is technically, economically and operationally feasible, this system is judged feasible.

VI.ECONOMICAL FEASIBILITY

The role of interface design is to reconcile the differences that prevail among the software engineer's design model, the designed system meet the end user requirement with economical way at minimal cost within the affordable price by encouraging more of proposed system. Economic feasibility is concerned with comparing the development cost with the income/benefit derived from the developed system. In this need to derive how this project will help the management to take effective decisions. The system once developed must be used efficiently. Otherwise there is no meaning for developing the system. For this a careful study of the existing system and its drawbacks are needed. The user should be able to distinguish the existing one and proposed one, so that one must be able to appreciate the characteristics of the proposed system, the manual one is not highly reliable and also is considerably fast. The proposed system is efficient, reliable and also quickly responding.

VII.DISCUSSION AND CONCLUSION

In this proposed work to use received signal strength based spatial correspondence, a somatic propertyconcomitant with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. This work providedtheoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. This approach can detect the presence of attacks as well as determine the number of adversaries, deceiving the same node identity, so that can restrict any number of attackers and eradicate them. Formative the number of adversaries is a particularly challenging problem.To validate this approach, conducted experiments on two testbeds through both an 802.11network (Wi-Fi) and

ISSN: 2278 – 909X

an 802.15.4 (ZigBee) network in two real office building environments. found that detection mechanisms are highly effective in both detecting the presence of attacks with detection rates over 95 percent and determining the number of adversaries, achieving over 92percent hit rates andprecision simultaneously when using SILENCE and SVM-based mechanism. Further, based on the number of attackers determined by these mechanisms, integrated detection and localization system can localize any number of adversaries even when attackers using different transmission controllevels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing solidindication of the effectiveness of this approach in detecting wireless deceiving attacks, defining the number of attackers and localizing adversaries.

REFERENCE

[1] NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems Chun-Jen Chung, Student Member, IEEE, PankajKhatkar, Student Member, IEEE, Tianyi Xing, Jeongkeun Lee, Member, IEEE, and Dijiang Huang Senior Member, IEEE.

[2.] y. xiang, w. zhou, and m. guo ," flexible deterministic packet marking: an iptraceback system to find the real source of attacks" apr. 2009.

[3.]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.

[4.] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," Proc. Ann. IEEE Comm. Soc. Conf.Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[5.] Jie yang ,yingying(Jennifer)chen wade trapped ,Detection and Localization Multiple Spoofing Attackers in Wireless networks "IEEE transactions on parallel and distributed systems, vol. 24, no. 1, January 2013.

[6.]Krontiris, I.; Giannetsos, T.; Dimitriou, T. LIDeA: A Distributed Lightweight Intrusion Detection Architecture for Sensor Networks. Proceedings of the 4th International Conference on Security and Privacy for Communication Networks (SECURECOMM 2008), Istanbul, Turkey, 22–25 September 2008.

[7.]Hai, T.H.; Khan, F.I.; Huh, E. Hybrid Intrusion Detection System for Wireless Sensor Networks. Proceedings of International Conference on Computer Science and Applications, San Francisco, CA, USA, October 2007.

[8.]Onat, I.; Miri, A. A Real-Time Node-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks. Proceedings of Systems Communications 2005 (ICW/ICHSN/ICMCS/ SENET 2005), Montreal, QC, Canada, 14–17 August 2005.

[9.]Wallenta, C.; Kim, J.; Bentley, P.J.; Hailes, S. Detecting interest cache poisoning in sensor networks using an artificial immune algorithm. *Appl. Intell* 2008, *32*, 1–26.

[10]Kaplantzis, S.; Shilton, A.; Mani, N.; Sekercioglu, Y.A. Detecting Selective Forwarding Attacks in WSNs using Support Vector Machines. Proceedings of 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, Melbourne, Australia, 3–6 December 2007; pp. 335–340.

[11] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks, "in Proc. IEEE IPDPS, 2005.

[12] 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.

[13] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell,"Detecting 802.11 MAC layer spoofing using received signalstrength," in Proc. IEEE INFOCOM, April 2008.

[14] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[15] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[16] 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.

BIOGRAPHY

Vengadapatjiraj.M received the B.E degree in Electronics and communication engineering from Government College of engineering Salem, Tamilnadu.Currently he is pursuing his ME in applied electronics from IFET College of engineeringVillupuram,Tamilnadu. His current research interes tincludes digital electronics, high performance networking and Microprocessor.

Rajendhiran.V received the B.E degree in electronics and communication engineering from E.S College of engineering Villupuram,Tamilnadu. Currently he is pursuing his ME IN applied electronics from IFET College of engineering Villupuram,Tamilnadu.his current research interest include digital image processing.

Sathishkumar.Rreceived the B.E degree in computer science engineering from arunai Engineering College thiruvannamalai, Tamilnadu.currently he is pursuing his M.E in computer science engineering from IFET College of engineering Villupuram tamilnadu his current research interest include computer networking and cloud computing

Vinoth Kannan.Aworkingas anAssistant Professor inthe DepartmentofElectronicsand Communication Engineeringat IFETCollegeof Engineering Villupuram, tamilnadu. Obtained B.E., fromannai mathammal sheela engineering college namakkal, Tamilnadu, M.E., inVLSI DESIGN from muthayammal engineering college Rasipuram,Tamilnadu. Having 2years ofteachingexperience.Hisareaof interestisCMOS VLSI design and digital image processing.

ISSN: 2278 – 909X