IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-04, Issue-02 E-ISSN: 2347-2693

A Study on Identity Based Attack Detection and Localization by the Clustering in Wireless Sensor Network

Tuhin Das

Department of Computer Science Engineering, SBITM College, RGPV University, India

www.ijcseonline.org

Received: Jan /21/2016 Revised: Feb/04/2016 Accepted: Feb/15/2016 Accepted: Feb/29/2016

***Abstract*—**Wireless sensor networks are most vulnerable to identity based attacks in which malicious device is used to create forged MAC addresses of specified authorized client. The identity of a node can be easily verified through cryptographic authentication techniques which are not always possible because it requires key management and other additional infrastructural overhead. In this paper we propose a system for detecting identity based attacks and also searching the actual positions of adversaries which are responsible for the attacks. Firstly we propose OADL (Attack Detection & Localization) model for identity based attack that utilizes correlation of nodes signal's spatial property (i.e spatial information, a physical property of each node) and the average received signal gain of received signal strength (RSS) collected from each wireless sensor nodes. Then we describe the integration of our attack detection model into our real time localization system, which has the ability to locate the actual positions of the attackers through Partitioning AroundMedoids clustering analysis for localization. We are able to show that the actual positions of the attackers that can be located using localization algorithms. Then we make evaluation based on our model through experimentation using both 802.11 network and 802.15.4 network model. Our results will indicate that identity based attack detection can be achieved with high precision in attack detection rate and localization of multiple adversaries.

***Keywords*—** Identity based attack, localization, OADL model, Received signal strength

I. Introduction

Wireless sensors networks consists of sensor nodes which are made up of small electronic devices and are capable of sensing, analyzing and transmitting information from physical environments. These small sensing devices namely nodes consists of processing units for data processing, memory for data storage, battery for energy and transceiver for transmitting and receiving data from one node to another and the size of each sensor node varies with applications. Wireless sensor networks uses radio waves to connect devices like laptops, mobile phones, the business network and applications to the Internet or other private networks. The popularity of wireless network is gained due to many causes for example easiness of installation, flexibility, mobility, low maintenance cost and scalability. The use of wireless sensor networks is gradually progressing day by day and at the same time it is facing the problems regarding security aspect of the wireless network. Due to the broadcast nature of wireless sensor networks, an adversary can hinder the signal and interrupt the operation of wireless network. Adversaries are malicious unit whose target is to prevent authorized user from accessing the network. Openness of wireless sensor network allows adversaries to easily monitor any data transmission and can easily use low cost wireless devices commonly available platforms to perform variety of attacks with minimal effort. It is quite easy for an attacker to gather precise media access control (MAC) address information by the help of passive monitoring and then modifying its MAC address using an ifconfig command. In IT world, Identity based attacks like spoofing refers tricking or deceiving computer users to retrieve private confidential information from their system. When any person masquerades as another by falsifying data and gaining the advantage in network can create multiple fake identities and cause stealing of confidential information and also network failure. The attacker forwards data packets to a computer with a source address specifying that the packet is coming from an authorized system. So these type of attacks facilitates development of various attacks such as data modification, Denial of Service (DoS) attacks, session hijacking and man-in-the-middle attacks [1], [2], [3] are massive threat to the integrity of wireless sensor networks.

In 802.11 networks, if control frames are not secured properly, then identity based attacks are feasible. The conventional cryptographic system will fail to provide security if the key is broken then identity-based spoofing attacks are still possible [4], [5], [6]. Under the above circumstances, it has become necessary to use the physical-layer information or characteristics to detect identity-based spoofing attacks in wireless networks [7]–[15]. In this paper we proposed to use OADL model which implements special algorithm that is well efficient in identity based attack detection and localizing spoofing attacks in mobile wireless network. Numerous methods of conventional approaches are used to authenticate application to address the problem of identity based attack but fails eventually.

II. RELATED WORK

In 2000, P. Bahl et al. [1] presented RADAR (Radio Detection And Ranging) system for localizing and tracking user in a building which is based on RF (radio frequency) system .The system is developed for finding the exact physical location of the authorized and unauthorized users. In 2001, Maurizio A. Spiritoet et al.[17] make analysis of the multilateration techniques accuracy on possible application based on mobile communications networks. This method helps to find the positioning, measurement accuracy & geometric conditioning of the problem. The result proved that this technique provides better location precision on mobile communication network. In 2002, C. Hsu et al. [18] proposed the logic of 'Support Vector Machine' which is designed for binary classification & to solve multiclass problems. In 2002, Daniel B. Faria et al. [19] proposed the architecture that consists of SIAP (Secure Internet Access Protocol) and SLAP (Secure Link Access Protocol) which implements public keys together with the RSA and AES encryption algorithms to serve reliable service. The combination of authentication and IP assignment, SIAP nullify the effect of DoS attacks on DHCP (Dynamic Host Configuration Protocol) servers. The results displayed that the proposed protocols are secure enough to protect 802.11b network model. In 2002, T.Roos et al. [20] suggested the three machine learning approaches Non-Probabilistic Nearest Neighbor method and two probabilistic approaches in Kernel, Histogram methods as a solution of the estimating location problem.

In 2003, Mathias Bohgeetal. [21] proposed TESLA certificate (framework) for solving scalability problems in ad hoc networks. They explore the job of providing entity & data authentication for wireless ad hoc sensor networks. There wireless sensor network consists of three tiers architecture in which devices with different level of computational and communication abilities. The suggested framework approves and authenticates incoming sensor nodes and thus maintains trusted relationship during topological changes and yields data origin authenticity over wireless ad hoc network. In 2003, Bellardo et al. [22] performed several experimental analysis for identification of the attackers by the help of efficacy and potential low-overhead implementation and then to weaken the underlying vulnerabilities. The authors demonstrate some steps for identification of the attacker and discard the same. It firstly, implies a description of vulnerabilities and threats present on the 802.11 management and media access. Secondly, it proposed that all attacks can be practically implemented by evading the normal operation on the firmware of 802.11 devices. Thirdly, they implemented two classes of DoS attacks and finally description to implement and evaluate conventional non-cryptographic countermeasures which can be implemented in the existing MAC hardware's firmware. The result displayed this mechanism is highly effective in identifying the attacks.

F. Ferreri et al. [23] illustrate the possible Denial-of-Service attacks on the wireless networks. To implement such attacks software & commodity hardware components are essential. The results displays that serious vulnerable threats exist in different node access points & single station can easily targeted by any attacker for taking illegitimate advantage over communication within secured network. For securing this communication, the Finite State Machine (FSM) concept is used. In 2006 Yingying Chen et al. [15] analyzed the reliability and robustness of Radio Frequency based fingerprinting localization procedure and algorithms to attacks that target RSS measurements. The metrics composed of localization error, holder metrics and precision of area based algorithms. This result proposes the average susceptibility of the results to an attack is essentially identical across area based and point based algorithms, although it is desirable to deploy point based methods or area based methods that operate average in order to reduce the worst-case affect of potential attack. In 2006, D. Faria et al . [8] displayed that client identifiers, called as signal prints, can be created using RSS(received signal strength) measurements of access points acting as node sensors. The strength of every received signal is calculated and analyzed when the communication is established between client & server in wireless sensor network. The value of each received signal is nearer to the specific range can be termed as 'signal print value' .The signal print value actually depends on the exact physical location of the client in wireless sensor network. In the year 2007, Qing Li et al. [24] tender an alternative to conventional identity based oriented authentication methodology for detecting device spoofing on wireless sensor network. The scheme was to use relationships within stream of data packets arriving from an individual network node identity.

In 2009, J.Yang et al., [25] present efficient technique of detecting Mobile Spoofing attacks in wireless Environments (DEMOTE). The developed DEMOTE system uses received signal strength traces collected over time from sensor nodes and achieve an optimal threshold to classify the received signal strength traces into significant classes for attack detection. In 2010 Yingying Chen et al. [26] proposed a model in wireless sensor networks of detecting spoofing, an identity-based attacks and Sybil attacks and also localizing the adversaries. Further there is scope of utilization of the K-means cluster analysis to derive the test statistic. In 2013, Jie Yang et al. [15] first proposed to use RSS(received signal strength) based spatial correlation, a physical property associated with each wireless sensor node it is difficult to falsify and not depending upon traditional cryptographic system for detecting identity based spoofing attacks in wireless sensor networks.

III. PROPOSED WORK

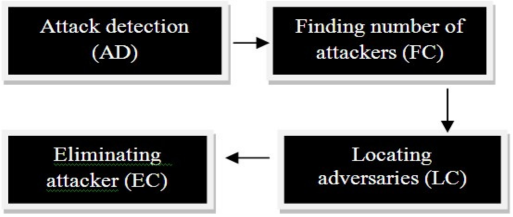
Among different types of attacks, identity-based attacks are especially difficult to handle and can cause adverse effect on network performance and also cause instability.

For example, in wifi network, it is very easy for an attacker to gather useful MAC address information and misuse it for during passive monitoring and then modify its MAC address by the help of an ifconfig command. The problematic issues in existing systems are as follows:-

- It requires large infrastructure overhead.
- Works only when implemented by large number of network.
- Used only on static wireless network
- System Deployment is expensive

There are other problems present in the existing systems for example the systems have no self defense mechanism they are unable to secure data confidentiality and integrity they can only able to identify the attacker. Some systems are reliable to work well in large network. In this paper we present a concept of using OADL modelin which spatial correlation of the RSS (Received Signal Strength) information, a physical property related with every wireless device or node is used for detecting and locating the identity based attacks.

OADL model working steps


Attack detection (AD)
Finding number of attackers (FC)
Locating adversaries (LC)
Eliminating attacker (EC)

However, techniques of using RSS across a set of access points to perform spoofing detection and localization will work for static and dynamic wireless sensor networks. The localization system that has the capability to localize the exact positions of the attackers through Partitioning AroundMedoids(PAM) clustering analysis.

Objectives

- identity based attack detection in both 802.11 network and 802.15.4 network model
- determination of access pattern of illegitimate adversaries network
- finding out the number of attackers when multiple attackers are masquerading as the same node identity
- locating exact position of multiple adversaries in the network and eliminating the same

For increasing the precision and accuracy we will use multi vector SVM (support vector machine) so that our experimental results could attain over 90 percent Hit Rate in the course of determining the number of adversaries.

IV. CONCLUSION

In this paper, we proposed methodology for detecting identity-based attacks like spoofing attacks and hence localizing multiple adversaries in wireless sensor networks with high accuracy and precision. In contrast to conventional authentication methods, our RSS based scheme does not require any additional overhead to the wireless sensor nodes. Our technique is use the concept of exploiting spatial correlation of RSS gained from wireless sensor nodes for attack detection and using PAM for clustering analysis for localizing multiple adversaries. Our model has capability to attained high detection rates like more than 90%, with low false-positive rates. We will look forward to study the effectiveness of our OADL modelin both the 802.11 & 802.15.4.

REFERENCES

[1] John Bellardo and Stefan Savage, “802.11 Denial-ofservice attacks: real vulnerabilities and practical solutions”, Proceedings of the 12th conference on USENIX Security Symposium, Vol. 12, pp. 15-28, 2003.

[2] F. Ferreri, M. Bernaschi and L. Valcamonici, “Access Points Vulnerabilities to Dos Attacks in 802.11 Networks”, IEEE Wireless Communications and Networking Conference, Vol. 1, pp. 634-638, 2004.

[3] Martin Eian, “Fragility of the robust security network: 802.11 denial of service”, Applied Cryptography and Network Security: Lecture Notes in Computer Science, Vol. 5536, pp. 400–416, 2009.

[4] Bing Wu, Jie Wu, E.B. Fernandez and S. Magliveras, “Secure and Efficient Key Management in Mobile Ad Hoc Networks”, Proceedings of IEEE International Symposium on Parallel and Distributed Processing, 2005.

[5] Avishai Wool, “Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation”, Wireless Networks, Vol. 11, No. 6, pp. 677-686, 2005.

[6] Mathias Bohge and Wade Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks”, Proceedings of the 2nd ACM workshop on Wireless security, pp. 79-87, 2003.

[7] M. Demirbas and Youngwhan Song, “An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks”, International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp. 564–570, 2006.

[8] Daniel B. Faria and David R. Cheriton, “Detecting identitybased attacks in wireless networks using signalprints”, Proceedings of WiSe’06: ACM Workshop on Wireless Security, pp. 43–52, 2006.

[9] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Fingerprints in the Ether: Using the physical layer for wireless authentication”, IEEE International Conference on Communications, pp. 4646–4651, 2007.

[10] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “A Physical Layer Technique to Enhance Authentication for Mobile Terminals”, IEEE International Conference on Communications, pp. 1520–1524, 2008.

[11] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “MIMO assisted channel-based authentication in wireless networks” 42nd Annual Conference on Information Sciences and Systems, pp. 642–646, 2008.

[12] Yong Sheng, K. Tan Guanling Chen, D. Kotz and A. Campbell, A, “Detecting 802.11 MAC Layer Spoofing R Maivizhi AND S Matilda: detection and localization of multiple spoofing attackers for mobile wireless networks 1118 Using Received Signal Strength”, IEEE 27th Conference on Computer Communications, pp. 1768–1776, 2008.

[13] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Using the physical layer for wireless authentication in time-variant channels”, IEEE Transactions on Wireless Communications, Vol. 7, No. 7, pp. 2571–2579, 2008.

[14] Vladimir Brik, Suman Banerjee, Marco Gruteser and Sangho Oh, "Wireless device identification with radiometric signatures", Proceedings of the 14th ACM international conference on Mobile computing and networking, pp. 116–127, 2008.

[15] Jie Yang, Yingying Chen, W. Trappe and J. Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 1, pp. 44-58, 2013.

[16] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF- Based User Location and Tracking System," Proc. IEEE INFOCOM, vol. 2, Page(s): 775 – 784, 2000

[17] Maurizio A. Spirito, "On the Accuracy of Cellular Mobile Station Location Estimation," IEEE Transactions On Vehicular Technology,Vol. 50, No. 3, May 2001.

[18] C. Hsu and C. Lin, "A Comparison of Methods for Multiclass Support Vector Machines," IEEE Trans. Neural Networks, vol. 13, no. 2, pp. 415-425, Mar. 2002

[19] Daniel B. Faria and David R. Cheriton, "DoS and Authentication in Wireless Public Access Networks," In Proceedings of the First ACM Workshop on Wireless Security (WiSe'02), September 2002

[20] T. Roos, P. Myllymaki, H.Tirri, P. Misikangas, and J.Sievanen, "A probabilistic approach to WLAN user location estimation," +International Journal of Wireless Information Networks, vol. 9, no. 3, pp.155–164, July 2002.

[21] Mathias Bohge and Wade Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," IEEE Trans. Ad Hoc Sensor Networks, WiSE'03, September 19, 2003

[22] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. USENIX Security Symp.,pp. 15-28,2003.

[23] F.Ferreri, M.Bernaschi, and L.Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," Proc. IEEE Wireless Comm. And Networking Conf., 2004.

[24] Qing Li and Wade Trappe, "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationship,"IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4,December 2007

[25] J. Yang, Y. Chen, and W. Trappe, "Detecting Spoofing Attacks in Mobile Wireless Environments," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.

[26] Yingying Chen, Jie Yang, Wade Trappe and Richard P. Martin, "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks "IEEE transactions on vehicular technology, vol. 59, no. 5, June 2010

AUTHORS PROFILE

TuhinDas,is a student of M.techin CSE Final year fromShriBalaji institute of Technology and Management college, under RGPV, Bhopal. His areas of interest are Wireless Sensor Network, Java, Network Security, and Data Mining.