ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 2 Issue Special 1 Jan-March 2014
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014)

Detection and Prevention of Impersonation Attack in Wireless networks

[I]Ms.B.Lakshmi, [II]Ms.B.Sanmuga Lakshmi, [III]Mr.R.Karthikeyan
[I,III]Dept of CSE ,Mohamed Sathak Engg College, Kilakarai, India
[II]Dept of IT, VSB Engg College, Karur, India

Abstract
Wireless impersonation attack is easy to launch and cause impact on network performance. Cryptographic method is not enough to avoid impersonation attack. During this paper we have tendency to propose to use special data, a property related to every node these data's are complex to falsify and not dependent on cryptographic because the basis for 1.police investigation of spoofing attacks. 2. Crucial the amount of attackers once multiple adversaries masquerading as a same node identity and 3.localizing multiple adversaries. We have to propose to use the spacial correlation of received signal strength (RSS) transmitted from wireless nodes to sight the impersonation attacks and using EPPM (efficient probabilistic packet marking) to detect the adversaries. Cluster-based mechanisms square measure developed to work out the amount of attackers. Once the coaching knowledge is accessible, we have a tendency to explore exploitation Support Vector Machines (SVM) methodology to improve the accuracy of crucial the amount of attackers. Additionally, we have a tendency to develop an integrated detection and localization system which will localize the positions of multiple attackers. We have a tendency to evaluate our techniques through 2 test beds exploitation each an 802.11 (Wi-Fi) network and an 802.15.4 (ZigBee) network in 2 real workplace buildings. Our experimental results show that our planned strategies can do over ninetieth Hit Rate and exactitude once crucial the amount of attackers. Our localization results employing a representative set of algorithms offer robust proof of high accuracy of localizing multiple adversaries.

Keywords
Wireless network security, attack detection, impersonation attack, localization

I. Introduction

Impersonation attacks will additional facilitate a range of traffic injection attacks [1], [2], like attacks on access management lists, varlet access purpose attacks, and eventually Denial-of- Service (DoS) attacks. A broad survey of doable impersonation attacks is found in [3], [4]. Moreover, in an exceedingly large-scale network, multiple adversaries might masquerade because the same identity and collaborate to launch malicious attacks like network resource utilization attack and denial-of-service attack quickly. Therefore, it's vital to

- detect the presence of spoofing attacks,
- determine the amount of attackers, and
- find the location of the attackers and eliminate them.

Most existing approaches to handle potential impersonation attacks use science schemes [6].However the appliance of science schemes needs reliable key distribution mechanisms. it's not perpetually fascinating to use these science ways as a result of its infrastructural, process, and management overhead. Further, science ways square measure prone to node compromise that may be a serious concern as most wireless nodes square measure simply accessible, permitting their memory to be simply scanned. During this work, we have a tendency to propose to use RSS-based spacial correlation, a property related to every wireless node that's exhausting to falsify and not dependent on cryptographic and using EPPM mechanism because the basis for detective work impersonation attacks. Since we have a tendency to square measure involved with attackers World Health Organization have totally different locations than legitimate wireless nodes, utilizing spacial data to handle impersonation attacks has the distinctive power to not solely determine the presence of those attacks however conjointly localize adversaries. another new an extra advantage of using spacial correlation to discover spoofing attacks is that it'll not need any additional price or modification to the wireless devices themselves.We concentrate on static nodes during this work, that square measure common for spoofing eventualities .we have a tendency to addressed impersonation detection in mobile environments in our different work [9]. The works that square measure closely associated with United States of America square measure projected the utilization of matching rules of signal prints for impersonation detection, sculptural the RSS readings employing a Gaussian mixture model and [8] used RSS and K-means cluster analysis to discover impersonation attacks. However, none of those approaches have the ability to see the amount of attackers once multiple adversaries use a same identity to launch attacks, that is that the basis to additional localize multiple adversaries when attack detection. Though [10] studied the way to localize adversaries, it will solely handle the case of one impersonation assailant and can't localize the assailant if the soul uses totally different transmission power levels.
The main contributions of our work are:

GADE

A generalized attack discover model that may each detect spoofing attacks in addition as verify the amount of adversaries victimization cluster analysis ways grounded on RSS-based spacial correlations among traditional devices and adversaries also use EPPM; and

IDOL

Associate degree integrated discover and localization system that may each detect attacks in addition as notice the positions of multiple adversaries even once the adversaries vary their transmission power levels.
In GADE, the Partitioning around Medoids (PAM) cluster analysis technique is employed to perform attack detection [15]. We have a tendency to formulate drawback the matter of decisive the amount of attackers as a multi-class detection problem. We have a tendency to then applied cluster based mostly ways to see the amount of assailant. Once the coaching knowledge is out there, we have a tendency to propose to use Support Vector Machines (SVM) technique to additional improve the accuracy of decisive

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

the amount of attackers [12].

Moreover, we have a tendency to developed associate degree integrated system, IDOL, that utilizes the results of the amount of attackers came by GADE to additional localize multiple adversaries. As we have a tendency to incontestable through our experiments victimization each associate degree 802.11 network in addition as associate degree 802.15.4 network in 2 real office block environments, GADE is very effective in impersonation detection with over ninetieth hit rate and exactitude. Moreover, employing a set of representative localization algorithms, we have a tendency to show that IDOL is able to do similar localization accuracy once localizing adversaries thereto of beneath traditional conditions. One key observation is that IDOL will handle attackers victimization totally different transmission power levels, thereby providing robust proof of the effectiveness of localizing adversaries once there square measure multiple attackers within the network.

II. Related Work

The traditional approach to prevent impersonation attack is to use cryptographic based authentication. Introduced a key management framework to apply secret sharing scheme and multicast server group. Due to limited resource on wireless devices cryptographic authentication may not be applicable. New approaches utilizing physical properties associated with wireless transmission to detect impersonation attack. Use RSS (Received Signal Strength) and EPPM (Efficient Probabilistic Packet Marking) to find out attack. This method didn't capable of determining number of attackers. Our work differs from the previous study, in that we use spatial information (RSS) and EPPM.

III. Overview of Techniques

A. Generalized Attack Detection Model

Here, we describe our Generalized Attack Detection ModEl (GADE), which consists of attack detection, which detects the presence of an attack.

B. Determining the Number of Attackers

Inaccurate estimation of the number of attackers will cause failure in localizing the multiple adversaries. As we do not know how many adversaries will use the same node identity to launch attacks, determining the number of attackers becomes a multi-class detection problem and is similar to determining how many clusters exist in the RSS readings.

C. Integrated Detection and Localization Framework (IDOL)

In this section we present our integrated system that can detect impersonation attacks, determine the number of attackers, and localize multiple adversaries. The experimental results are presented to evaluate the effectiveness of our approach, especially when attackers using different transmission power levels.

D. Data Flow Diagram

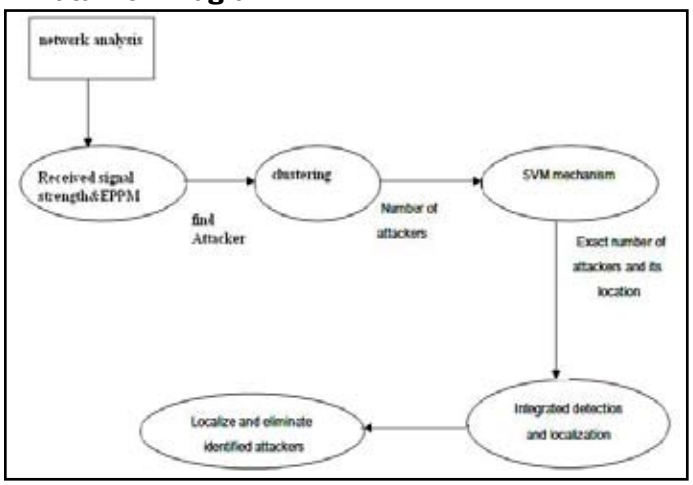

Fig.1: Data Flow Diagram

IV. Proposed System

- In the proposed system we used Inter domain packet filter (IDPFs) architecture, a system that can be constructed solely based on the locally exchanged BGP updates.
- Every node only selects and propagates to neighbors based on two set of routing policies, namely Import and Export Routing policies.
- The IDPF uses a feasible path from source node to the destination node, and the packet can reach to the destination through one of its upstream neighbors.
- The training data is available we investigate using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers [13].
- In localization results by means of a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.
- The Cluster Based wireless Sensor Network information received signal strength (RSS) based spatial correlation of network Strategy.
- Use EPPM mechanism to find owner of spoofed IP.
- 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.

V. Network Analysis

We initiate a fixed-length walk on the node. This walk should be long enough to make sure that the visited peers represent a close sample from the underlying stationary distribution. We then retrieve certain information about the system details and process details. It acting as source for the network .In sender used to create sends the request and received the response and destination used to received the request and send the response for the source.

A. Impersonation Attack

Impersonation attacks are particularly easy to launch and can cause significant damage to network performance. For example, in an 802.11 network, it is easy for an attacker to collect useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an If config command to masquerade as another device. In spite of existing 802.11 security techniques including Wired Equivalent Privacy (WEP), Wi-Fi 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.

B. Attack Detection

In the attack detection instead of relying on cryptographic-based approaches. Furthermore, our work is novel because none of the exiting work can determine the number of attackers when there are multiple adversaries masquerading as the same identity. Additionally, our approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

C. Localization

Localization estimate errors using RSS which are about 15 feet. When the nodes are smaller than 15 feet apart, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90 percent, but still greater than 70 percent. However, when Spoof moves closer to the attacker also increases the probability to expose itself. The detection rate goes to 100 percent when the impersonation node is about 45-50 feet away from the original node.

VI. Algorithms

In order to estimate the generality of IDOL for localizing adversaries, we have chosen a set of representative localization algorithms ranging from nearest neighbor matching in signal space (RADAR), to probability-based (Area-Based Probability),and to multilateration (Bayesian Networks) .

A. RADAR-Gridded

The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known (x, y) locations [11]. Given an observed RSS reading with an unknown location, RADAR returns the x, y of the nearest neighbor in the signal map to the one to localize, where "nearest" is defined as the Euclidean distance of RSS points in an N-dimensional signal space, where N is the number of landmarks.

B. Area Based Probability (ABP)

ABP also utilizes an interpolated signal map [16]. Further, the experimental area is divided into a regular grid of equal sized tiles. ABP assumes the distribution of RSS for each landmark follows a Gaussian distribution with mean as the expected value of RSS reading vector s. ABP then computes the probability of the wireless device being at each tile Li, with i = 1...L, on the floor using

Bayes' rule:

Given that the wireless node must be at exactly one tile satisfying $\sum^{L}_{i=1} P(Li|s) = 1$, ABP normalizes the probability and returns the most likely tiles/grids up to its confidence α.

C. Bayesian Networks (BN)

BN localization is a multilateration algorithm that encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization [14]. Figure 13 shows the basic Bayesian Network used for our study. The vertices X and Y represent location; the vertex si is the RSS reading from the ith landmark; and the vertex Di represents the Euclidean distance between the location specified by X and Y and the ith milestone. The value of si follows a signal propagation model $si = b_{0i}+b_{1i}$ logDi, where b_{0i}, b_{1i} are the parameters specific to the i^{th} landmark.

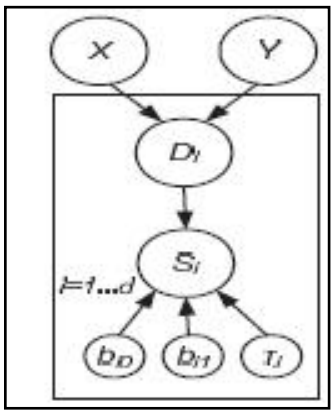

Fig. 2: Bayesian Model

Bayesian graphical model in our study

The distance $Di = \sqrt{(X - x_i)^2 + (Y - y_i)^2}$ in turn depends on the location (X, Y) of the measured signal and the coordinates (x_i, y_i) of the ith landmark. The network models noise and outliers by modeling the si as a Gaussian distribution around the above propagation model, with variance τi: $si \sim N(b_{0i} + b_{1i}\ \text{logDi}, \tau_i)$. Through Markov Chain Monte Carlo (MCMC) simulation, BN proceeds the sampling distribution of the possible location of X and Y as the localization result.

VII. CONCLUSION

In this work, we tend to planned to use received signal strength (RSS) based mostly special correlation, a property related to every wireless device that's a difficult to falsify and not dependent on cryptographic furthermore EPPM mechanism because of these basis can detect impersonation attacks in wireless networks. We tend to provided theoretical analysis of exploitation the special correlation of RSS genetic from wireless nodes for attack detection. We tend to derived the take a look at data point supported the cluster analysis of RSS readings. Our approach will each find the presence of attacks furthermore as verify the quantity of adversaries, impersonation constant node identity, in order that we are able to localize any variety of attackers and eliminate them. Determinant the quantity of adversaries may be a significantly difficult drawback. Cluster analysis wont to attain higher accuracy of determinant the quantity of attackers than alternative strategies underneath study, like Silhouette Plot and System Evolution that use cluster analysis alone. in addition, once the coaching information is offered, we tend to explored exploitation Support Vector Machines (SVM) based mostly mechanism to any improve the accuracy of determinant the quantity of attackers gift within the system. To validate our approach, we tend to conducted experiments on 2 test-beds through each Associate in Nursing 802.11network (Wi-Fi) Associate in Nursing an 802.15.4 (Zig-Bee) network in 2 real edifice environments. we tend to found that our detection mechanisms an extremely effective in each detective work the presence of attacks with detection rates over ninety eight and determinant the quantity of adversaries, achieving over ninetieth hit rates and exactitude at the same time once exploitation SVM-based mechanism. Further, supported the quantity of attackers determined by our mechanisms, our integrated detection and localization system will localize any variety of adversaries even once attackers exploitation completely different transmission

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

level of power. The action of localizing adversaries achieves similar results as those underneath traditional conditions, thereby, providing sturdy proof of the effectiveness of our approach in detective work wireless impersonation attacks, determinant the quantity of attackers and localizing adversaries.

References

[1] *Jie Yang, Yingying Chen, and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" in IEEE 2012.*
[2] *J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proceedings of the USENIX Security Symposium, 2003, pp. 15 – 28.*
[3] *F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access point's vulnerabilities to dos attacks in 802.11 networks," in Proceedings of the IEEE Wireless Communications and Networking Conference, 2004.*
[4] *D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proceedings of the ACM Workshop on Wireless Security (WiSe), September 2006.*
[5] *Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proc. IEEE SECON, 2006.*
[6] *B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.*
[7] *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.*
[8] *Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in Proc. IEEE INFOCOM, April 2008.*
[9] *J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in Proc. IEEE SECON, 2009.*
[10] *Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wirelss spoofing attacks," in Proc. IEEE SECON, May 2007.*
[11] *P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBasedUser Location and Tracking System," Proc. IEEEINFOCOM, 2000.*
[12] *N. Cristianini and J. Shawe-Taylor, An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods. CambridgeUniv. Press, 2000.*
[13] *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.*
[14] *D. Madigan, E. Elnahrawy, R. Martin, W. Ju, P. Krishnan, and A.S.Krishnakumar, "Bayesian Indoor Positioning Systems," Proc. IEEE INFOCOM, pp. 324-331, Mar. 2005.*
[15] *Lamia Fattouh Ibrahim, " Using of Clustering and Ant-Colony Algorithms CWSP-PAM-ANT in Network Planning", International Conference on Digital Telecommunications (ICDT 2006), Cap Esterel, French Riviera, France, 26-31 August 2006.*

About The Authors

Ms.B.Lakshmi pursuing M.E (CSE) in Mohamed Sathak .Engineering College, Kilakarai.She has received B.E (CSE) from Mohamed Sathak Engineering College. Her area of interest includes Network Security, Cloud Computing.

Ms.B.Sanmuga Lakshmi pursuing M.Tech (IT) in V.S.B.Engineering College,karur. She has received B.Tech (IT) from Mohamed Sathak Engineering College. Her area of interest includes Network Security, Database management System and MANET.

Mr.R.Karthikeyan has received the M.E(CSE) degree from Mohamed Sathak Engineering College and pursuing Ph.D in could computing.He is currently working as an associate professor in Mohamed Sathak Engineering College,kilakarai.