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 7, July 2015

Detecting Malicious Attacker in Mobile Adhoc Sensor Networks

P.Tharanya [1], L.Gomathi .,[2]

Research Scholar, Department of Computer Science, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[1]

Associate Professor, Department of Computer Science, Muthayammal College of Arts & Science, Rasipuram, Namakkal, India[2]

ABSTRACT: Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client or to create multiple illegitimate identities. 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. To address the issue of scalability, self-organizing hierarchical ad hoc architectures are being investigated. Design, implement, and evaluate a technique to identify the source network interface card (NIC) of an IEEE 802.11 frame through passive radio-frequency analysis. Although the identity of a node can be verified through cryptographic security, conventional security approaches these are not always desirable. we propose to use spatial information, a physical property of each node, so hard to forge or alter fraudulently and not depend on cryptographic security, on the basis for detecting spoofing attacks; (2) determining the number of attackers when multiple node pretend as a same node identity, and (3) localizing multiple adversaries. We propose to use the correlation between a signal's spatial direction and the average received signal gain of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. In this paper enlist the various methods of spoofing attack detection using spatial correlation between wireless nodes. And cluster based mechanisms to determine the number of attackers in network. , we explore using Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. We evaluated techniques through two wireless adhoc networks using both an 802.11 (WiFi) network and some other wireless network standard.

KEYWORDS: ADHOC sensor network, spoofing attack, attack detection

I. Introduction

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 a command to masquerade as another device. Remote sensing applications are becoming an increasingly important area for research and development due to the critical need for applications that will perform environmental monitoring, provide security assurance, assist in healthcare services and facilitate factory automation. The limited computational and storage resources available to sensors necessitates alternatives to authentication based on public key certificates.

Another work on authentication for ad hoc networks that addressed the issue of scalability was presented in, which introduced the use of cluster heads to reduce the amount of control packets needed. In this work, the network is divided into cluster regions, and cluster heads are elected from the regular network nodes within each cluster. This is an assumption that does not hold in non-military applications, and therefore we consider a three tier hierarchical ad hoc network that is suitable for more general remote sensing applications running on the Internet. Device identity management is, perhaps, one of the most significant challenges in any network security solution. Since the source MAC

DOI: 10.15680/ijircce.2015. 0307152

address in a frame is easy to forge, admin-instructors need other mechanisms to identify the source of frames within their networks. In a wired network, switches provide the capability to distinguish track based on the in- coming port, each mapped to a single Ethernet jack in the wall. In contrast, the un tethered nature of wireless communication makes similar identification of a frame's source difficult. To overcome this hurdle, 802.11 WLAN administra- tors rely on various cryptographic mechanisms for wireless device identity management and access control. an approach and a prototype to accurately identify the source network interface card (NIC) of a wireless frame, and propose the use of this approach in various identity management and security applications. Our approach is based on the notion of radiometric identity: minor variations in analogy hardware of transmitters are manifested as idiosyncratic artifacts in their emitted signals and thus can be used to identify a signal's device-of-origin. Secure localization is important for distributed sensor systems because the position of sensor nodes is a critical input for many sensor network tasks, such as tracking, monitoring and geometric-based routing.

II. LITERATURE SURVEY

First wireless transmitter identification systems were developed as early as the 1960s for military aircrafts to differentiate between friendly and enemy radars. However, it is not clear whether such systems were effective and practical enough for the military to use for day-to-day operation. Nevertheless, similar transmitter identification systems have since been developed and used in the context of cellular networks. A large body of literature is dedicated to the general issues of design, implementation and operation that are relevant to many kinds of identification systems, whether they identify radars, cell phones, people, or 802.11 transmitters. A comprehensive overview of high-level issues in the context of transmitter identification is presented by Talbot et al. while a biometric perspective can be found. The range-based algorithms involve distance estimation to landmarks using the measurement of various physical properties like RSS, Time Of Arrival (TOA) and Time Difference Of Arrival (TDOA). Rather than use precise physical property measurements, range-free algorithms use coarser metrics like connectivity or hop-counts to landmarks to place bounds on candidate positions. In scene matching approaches, a radio map of the environment is constructed, either by measuring actual samples, using signal propagation models, or some combination of the two.

III. EXISTING SYSTEM

A node then measures a set of radio properties (often just the RSS of a set of landmarks), the fingerprint, and attempts to match these to known location(s) on the radio map. These approaches are almost always used in indoor environments because signal propagation is extensively affected by reflection, diffraction and scattering and thus ranging or simple distance bounds cannot be effectively employed. Matching fingerprints to locations can be cast in statistical terms, as a machine-learning classifier problem, or as a clustering problem.

Disadvantages of existing system:

Device identity management is, perhaps, one of the most significant challenges in any network security solution. Since the source MAC address in a frame is easy to forge, admin instructors need other mechanisms to identify the source of frames within their networks. In a wired network, switches provide the capability to distinguish track based on the in- coming port, each mapped to a single Ethernet jack in the wall. In contrast, the untethered nature of wireless communication makes similar identification of a frame's source difficult.

IV.PROPOSED SYSTEM

RF fingerprinting methods can be further broken down into two main categories: point-based methods, and area-based methods. Point-based methods return an estimated point as a localization result. A primary example of a point-based method is the RADAR scheme. Variations of RADAR, such as Averaged RADAR and Gridded RADAR have been proposed. On the other hand, area-based algorithms return a *most likely* area in which the true location resides. Two examples of area-based localization algorithms are the Area Based Probability (ABP) method and the Bayesian Networks method. One of the major advantages of area-based methods compared to point-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location. For this paper, we have selected a representative set of algorithms from each class of RF fingerprinting schemes for conducting our

DOI: 10.15680/ijircce.2015. 0307152

analysis. The algorithms we have selected are presented in Table 1. Although there are a variety of other fingerprinting localization algorithms that may be studied, our results are general and can be applied to other point-based and area-based methods.

ADVANTAGES OF PROPOSED SYSTEM:

One of the major advantages of area-based methods compared to point-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location.

V. ALGORITHMS AND SIGNAL STRENGTH ATTACKS

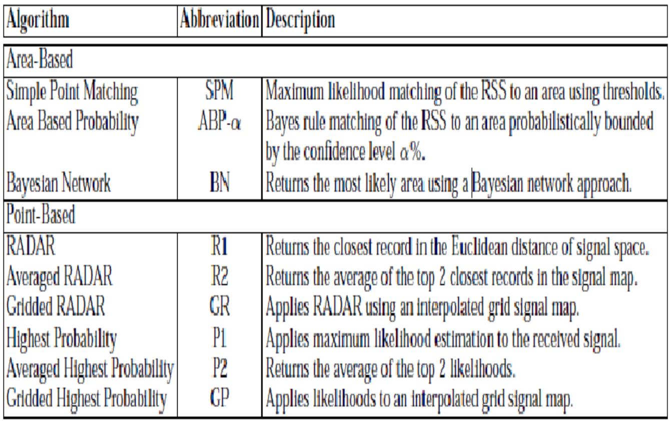
In this paper we are only concerned with localization algorithms that employ signal strength measurements. There are several ways to classify localization schemes that use signal strength: range-based schemes which explicitly involve the calculation of distances to landmarks; and RF fingerprinting schemes whereby a radio map is constructed using prior measurements, and a device is localized by referencing this radio map. For this study we focus on indoor localization schemes and therefore we restrict our attention to RF fingerprinting methods, which have had more success for indoor environments. RF fingerprinting methods can be further broken down into two main categories: point-based methods, and area-based methods. Point-based methods return an estimated point as a localization result. A primary example of a point-based method is the RADAR scheme. Variations of RADAR, such as Averaged RADAR and Gridded RADAR have been proposed.

On the other hand, area-based algorithms return a most likely area in which the true location resides. Two examples of area-based localization algorithms are the Area Based Probability (ABP) method and the Bayesian Networks method. One of the major advantages of area-based methods compared to point-based methods is that they return a region, which has an increased chance of capturing the transmitter's true location. For this paper, we have selected a representative set of algorithms from each class of RF fingerprinting schemes for conducting our analysis. The algorithms we have selected are presented in Table 1. Although there are a variety of other fingerprinting localization algorithms that may be studied, our results are general and can be applied to other point-based and area-based methods. More details for these algorithms can be found.

To attack signal-strength based localization systems, an adversary must attenuate or amplify the RSS readings.

This can be done by applying the attack at the transmitting device, e.g. simply placing foil around the 802.11 card; or by directing the attack at the landmarks. For example, we may steer the lobes and nulls of an antenna to target select landmarks. A broad variety of attenuation attacks can be performed by introducing materials between the landmarks and sensors. We measured the effect of different. materials on the RF propagation when inserted between the landmarks and the sensors. Figure shows the experimental results.

Table 1. Algorithms under study



Algorithm	Abbreviation	Description
Area-Based		
Simple Point Matching	SPM	Maximum likelihood matching of the RSS to an area using thresholds.
Area Based Probability	ABP-α	Bayes rule matching of the RSS to an area probabilistically bounded by the confidence level α%.
Bayesian Network	BN	Returns the most likely area using a Bayesian network approach.
Point-Based		
RADAR	R1	Returns the closest record in the Euclidean distance of signal space.
Averaged RADAR	R2	Returns the average of the top 2 closest records in the signal map.
Gridded RADAR	GR	Applies RADAR using an interpolated grid signal map.
Highest Probability	P1	Applies maximum likelihood estimation to the received signal.
Averaged Highest Probability	P2	Returns the average of the top 2 likelihoods.
Gridded Highest Probability	GP	Applies likelihoods to an interpolated grid signal map.

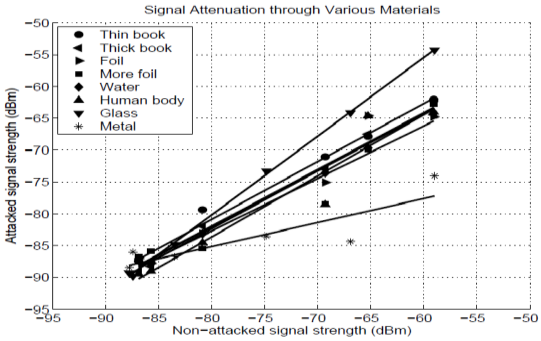


Fig.1. Signal attenuation when going through a barrier

These materials are easy to access and attacks utilizing these kind of materials can be simply performed with low cost. Based upon the results, we see that there is a linear relationship between the unattached signal strength and the attacked signal strength in dB for various materials. The linear relationship suggests that there is an easy way for an adversary to control the effect of his/her attack on the observed signal strength.

In the rest of this paper, we will use the linear attenuation model to describe the effect of an attack on the RSS readings at one or more landmarks. The resulting attacked readings are then used to study the consequent effects on localization for the algorithms surveyed above. In particular, in this study, we apply our attacks to individual landmarks, which might correspond to placing a barrier directly in front of a landmark, as well as to the entire set of landmarks, which corresponds to placing a barrier around the transmitting device. Similar arguments can be made for amplification attacks, whereby barriers are removed between the source and receivers. Although there are many different and more complex signal strength attack methods that can be used, we believe their effects will not vary much from the linear signal strength attack model we use in this paper, and note that such sophisticated attacks could involve much higher cost to perform.

VI. ATTACK SUSCEPTIBILITY METRICS

We wish to quantify the effect that an attack has on localization by relating the effect of a change in a signal strength reading s to the resulting change in the localization result p. We shall use p0 to denote the correct location of a transmitter, p to denote the estimated location (set) when there is no attack being performed, and ˜p to denote the position (set) returned by the estimator after an attack has affected the signal strength. There are several performance metrics can be used.

Estimator Distance Error:

An attack will cause the magnitude of p0 ˜p to increase. For a particular localization algorithm Galg we are interested in the statistical characterization of kp0 ˜pk over all possible locations in the building. The characterization of kp0 ˜pk depends on whether a point-based method or an area-based method is used, and can be described via its mean and distributional behaviour.

Estimator Precision:

An area-based localization algorithm returns a set p. For localization, precision refers to the size of the returned estimated area. This metric quantifies the average value of the area of the localized set p over different signal strength readings s. Generally speaking, the smaller the size of the returned area, the more precise the estimation is. When an attack is conducted, it is possible that the precision of the answer ˜p is affected.

Precision vs. Perturbation Distance:

The perturbation distance is the quantity kpmed ˜pmedk. The precision vs. perturbation distance metric depicts the functional dependency between precision and increased perturbation distance.

Holder Metrics:

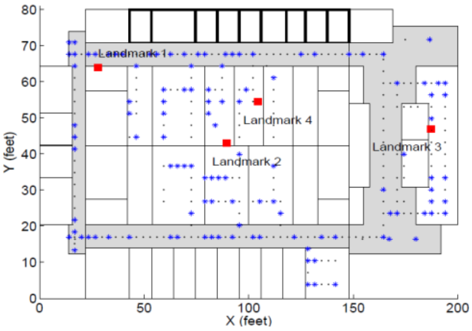
In addition to error performance, we are interested in how dramatically the returned results can be perturbed by an attack. Thus, we wish to relate the magnitude of the perturbation ks-˜sk to its effect on the localization result, which is measured by kGalg(s) − Galg(˜s)k. In order to quantify the effect that a change in the signal strength space has on the position space, we borrow a measure from functional analysis [21], called the Hölder parameter (also known as the Lipschitz parameter) for Galg.

VII. EXPERIMENTAL RESULTS

In this section we present our experimental results. We first describe our experimental method. Next, we examine the impact of attacks on the RSS to localization error when attacking all landmarks simultaneously as well as single-landmark attacks. We then quantify the algorithms' linear responses to RSS changes. Finally, we present a precision study that investigates the impact of attacks on the returned areas for area-based algorithms. In our evaluation we have chosen to focus on NICs of the same model. We believe that this is the most challenging classification scenario since all the NICs are likely to have been made of the same components at the same facility. Indeed, many of our NICs had consecutive serial numbers. Conversely, we expect that NICs of different brands, or even different models, will be easier to distinguish since their design, and perhaps component specifications are different. Although it is possible that transmitters by other manufacturers could be more resistant to classification, we note that all the data we used was compliant with 802.11 standard's accuracy requirements.

Data collection process

The data collection process was as follows. The data for this work was collected over about one week in the August of 2007 and another week in January of 2008. Exact collection set-up varied somewhat between the collection sessions. The variations were dictated by practical concerns, such as availability of hardware, and having to move our equipment. The available ORBIT nodes with Atheros NICs were conjured as 802.11b access points on channel 1.



We used Agilent 89641S vector signal analyzer (VSA) as the PARADIS sensor to capture the wireless frames sent out by the different nodes and to extract the modulation metrics of interest.

Over the collection period, the VSA used a 6 dBi omnidi- rectional antenna, 8 dBi patch antenna, and, for a few days, an 18 dB low-noise amplifier. Antenna orientation and location also changed by a few meters between sessions but maintaining line-of-sight with all the nodes. All the data was collected from nodes between 5 and 25 meters away from VSA's antenna. RF noise conditions actuated as well, de- pending on the level of activity of other wireless networks in the vicinity. Success of the identification process across such changes indicates robustness of PARADIS to variations in channel characteristics.

Experimental Setup

The floor map on the left, (a) is the 3rd floor of the CoRE building at Rutgers, which houses the computer science department and has an area of 200x80ft (16000 ft2). The other floor shown in (b) is an industrial research laboratory (we call the Industrial Lab), which has an area of 225x144ft (32400 ft2). The stars are the training points, the small dots are testing points, and the larger squares are the landmarks, which are 802.11 access points. Notice that the 4 CoRE landmarks are more co-linear than the 5 landmarks in the Industrial Lab. For both attenuation and amplification attacks, we ran the algorithms but modified the RSS of the testing points.

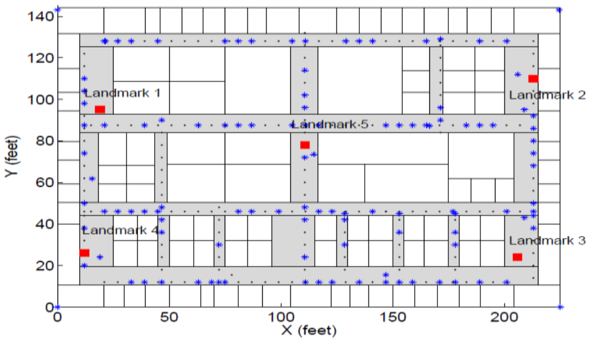


Fig.2. Deployment of landmarks and training locations on the experimental floors

VIII. Conclusion and Future Work

A method for detecting spoofing attacks as well as localizing the adversaries 9 in wireless and sensor networks. In contrast to traditional identity-oriented authentication methods, our RSS based approach does not add additional overhead to the wireless devices and sensor nodes. We then utilized the K-means cluster analysis to derive the test statistic. Further, we have built a real-time localization system and integrated our 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. We then provided theoretical analysis of exploiting the spatial correlation of RSS inherited from wireless nodes for attack detection. The *K*-means cluster analysis to derive the test statistic. Our attack detector is robust to detect attacks that are launched by adversaries that use different transmission power levels. In addition, we have built a real-time localization system and integrated our *K*-means attack detector into the system to locate the positions of the attackers and, as a result, to eliminate the adversaries from the network.

References

[1] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp.521–534, 2002.

[2] A. Weimerskirch and G. Thonet, "A distributed light-weight authentication model for ad-hoc networks," in The 4th International Conference on Information Security and Cryptology (ICISC 2001),pp. 341-354, 2001

[3] Agilent Technologies. RF Testing of WLAN products. Application note 1380-1.

[4] Agilent Technologies. Testing and Troubleshooting Digital RF Communications Transmitter Designs. Application note 1313.

[5] M. Barbeau, J. Hall, and E. Kranakis. Detecting Impersonation Attacks in Future Wireless and Mobile Networks. MANETS, 2006.

[6] Youssef, M., Agrawal, A., Shankar, A.U.: WLAN location determination via clustering and probability distributions. In: Proceedings of IEEE PerCom'03, Fort Worth, TX (2003)

[7] Roos, T., Myllymaki, P., H.Tirri: A Statistical Modeling Approach to Location Estimation. IEEE Transactions on Mobile Computing **1**(1) (2002)

[8] Battiti, R., Brunato, M., Villani, A.: Statistical Learning Theory for Location Fingerprinting in Wireless LANs. Technical Report DIT-02-086, University of Trento, Informaticate Telecomunicazioni (2002)

[9] Wu B., Wu J., Fernandez E. and Magliveras S. (2005) "Secure and Efficient Key Management in Mobile Ad Hoc Networks", Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS).

[10] Wang k. (2007) "Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data", Technical Report NO. 2007-258, Computer Science Dept., Xidian Univ., P.R. China.

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 7, July 2015

BIOGRAPHY

P.Tharanya,Received BCA degree from Muthayammal College of Arts & Science,Affiliated to Periyar University, Namakkal,2012. MCA degree from Muthayammal Engineering College, Affiliated to Anna University, Namakkal., 2014 & Pursuing my M.Phil(Full time) at Muthayammal College of Arts & Science , Affiliated to Periyar University, Namakkal, India.

L.Gomathi Currently doing Ph.D. She received her BCA degree from Bharathidasan University, Chitode 2002 and MCA degree from Bharathidasan University, Trichirapalli 2005. She has completed her M.Phil at Periyar University, Salem, 2007. She is having 9 years of experience in collegiate teaching and she is the Associate Professor, Department of BCA in Muthayammal College of Arts and Science, Rasipuram affiliated by Periyar University, Namakkal, India.

DOI: 10.15680/ijircce.2015. 0307152