Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 9, September 2014, pg.212 – 218

RESEARCH ARTICLE

AN INTEGRATED METHOD TO DISCOVER AND CONFINE OF VARIOUS MALICIOUS BLUFFING ATTACKERS IN MOBILE ADHOC NETWORK

K. Sumithra, Research Scholar, G.Narayanamma Institute of Technology & Science
M. Sridevi, Assistant Professor, G.Narayanamma Institute of Technology & Science

Abstract: A wireless network which is a self governing network which do not depend on other nodes. The mobile in ad hoc networks usually depends on the neighbor nodes to forward the data packets from one node to another node. Mobile nodes in ad hoc network are vulnerable to bluff attacks, which allows for many other forms of attacks on the networks. Every node can be identified by a cryptographic authentication, but every time an authentication process is not always possible because of its key management like public and private key and additional infrastructure overhead. In this paper, we propose a method to discover bluffing node attackers and locate the positions of the nodes performing the attack. We propose an attack detector for wireless bluffing that utilizes k-means cluster analysis. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the bluffing attacks. We then formulate the problem of determining the number of attackers as a multiclass detection problem. Cluster-based mechanisms are developed to determine the number of attackers. When the training data are available, we explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers.

Introduction:

An ad hoc network is a wireless network which is a self configured and self governing network which has multiple mobile nodes. The mobile nodes which are connected each other will act as a self configuring system which transfer's data packets from one node to another node.

As more wireless and sensor networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless ad hoc networks, they are especially vulnerable to bluff attacks where an attacker forges its identity to masquerade as another device, or even creates multiple

illegitimate identities. Bluffing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of bluffing nodes and eliminate them from the network.

The traditional approach to address bluffing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network. In this paper, we take a different approach by using the physical properties associated with wireless transmissions to detect spoofing. Specifically, we propose a scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices and sensor nodes.

By analyzing the RSS from each MAC address using K-means cluster algorithm, we have found that the distance between the centroids in signal space is a good test statistic for effective attack detection. We then describe how we integrated our K-means spoofing detector into a real-time indoor localization system. Our K-means approach is general in that it can be applied to almost all RSS-based localization algorithms. For two sample algorithms, we show that using the centroids of the clusters in signal space as the input to the localization system, the positions of the attackers can be localized with the same relative estimation errors as under normal conditions.

Related Work:

The traditional approach to prevent bluffing node attacks is to use cryptographic based authentication. Maliveras[1] has introduced a secure and efficient key management framework. This framework builds a public key infrastructure by applying a secret sharing scheme and an underlying multi server group. Wool [2] implemented a key management mechanism with a time period key and a host revocation to prevent the compromise of authentication keys. Based on the fact that wireless channel response decorrelates quietly rapidly in a space, a channel based authentication scheme was proposed to discriminate between transmitters at different locations and thus to identify bluff attacks in wireless network.[3]Gruteser modeled the RSS reading using a Gaussian mixture model. Arora [4] proposed to use the node's spatial Signature including Received signal strength Indicator and Link Quality Indicator. Turning to studying localization techniques, in spite of its several meter level accuracy, using RSS[5] [6] [7], is an alternate approach because it can reuse the existing wireless infrastructure and is highly co-related with physical locations.

Generalized Attack Detection Model: This method consists of two phases: attack detection, which detects the presence of an attack and a number determinator which determines the number of adversaries.

Handling Different Transmission

The spoofing attacker used transmission power of 10 dB to send packets, whereas the original node used 15 dB transmission power level. We observed that the curve of Dm under the different transmission power level shifts to the right indicating larger Dm values. Thus, spoofing attacks launched by using different transmission power levels will be detected effectively in GADE.

Performance of Detection

The cluster analysis for attack detection, Fig. 6 presents the Receiver Operating Characteristic curves of using Dm as a test statistic to perform attack detection for both the 802.11 and the 802.15.4 networks. Table 1 presents the detection rate and false positive rate for both networks under different threshold settings. The results are encouraging, showing that for false positive rates less than 10 percent, the detection rate are above 98 percent when the threshold is around 8 dB. Even when the false positive rate goes to zero, the detection rate is still more than 95 percent for both networks.

The Number Of Attackers

The 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 multiclass detection problem and is similar to determining how many clusters exist in the RSS readings.

Attacker Number Determination

The System Evolution is a new method to analyze cluster structures and estimate the number of clusters. The System Evolution method uses the twin-cluster model, which are the two closest clusters among K potential clusters of a data set. The twin-cluster model is used for energy calculation. The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energy is calculated as the average distance between elements in the border region of the twin clusters.

The Silence Mechanism

The advantage of Silhouette Plot is that it is suitable for estimating the best partition. Whereas the System Evolution method performs well under difficult cases such as when there exists slightly overlapping between clusters and there are smaller clusters near larger clusters. However, we observed

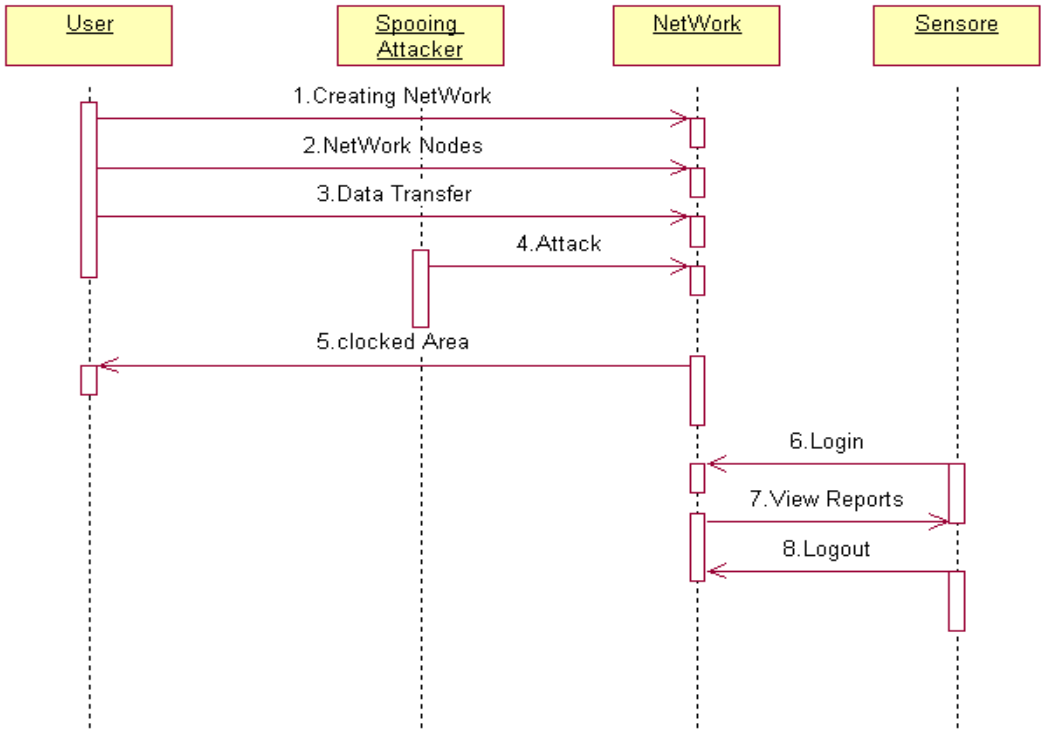
that for both Silhouette Plot and System Evolution methods, the Hit Rate decreases as the number of attackers increases, although the Precision increases.

Support Vector Machines-Based Mechanism

The training data collected during the offline training phase, we can further improve the performance of determining the number of spoofing attackers. In addition, given several statistic methods available to detect the number of attackers, such as System Evolution and SILENCE, we can combine the characteristics of these methods to achieve a higher detection rate. In this section, we explore using Support Vector Machines to classify the number of the bluffing attackers.

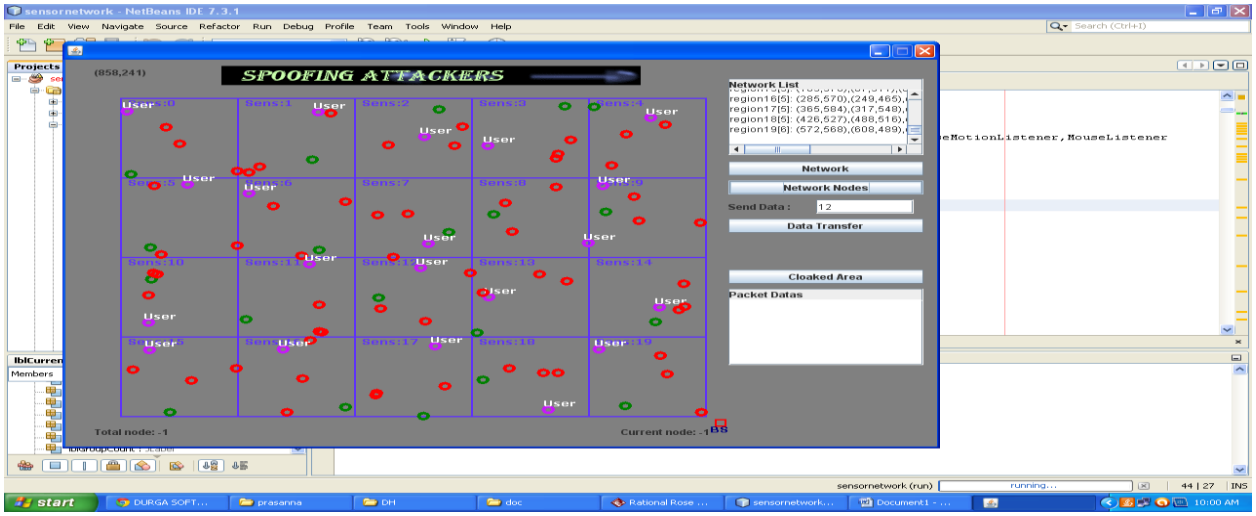
Method to Determine the Number of Attackers:

In general a user is connected directly to bluff node and inturn it is connect to a network and proceeded by sensor. At first a user requested for an attacker, then we create a network and specify the nodes of the network. Then after getting an acknowledgment from the consine node, we transfer the data packets. Then a confine node is used to make an attack by the network and at last the sensors are used to collect a valid report that contains to find the number of nodes in the network and to find the number of nodes that can be processed.

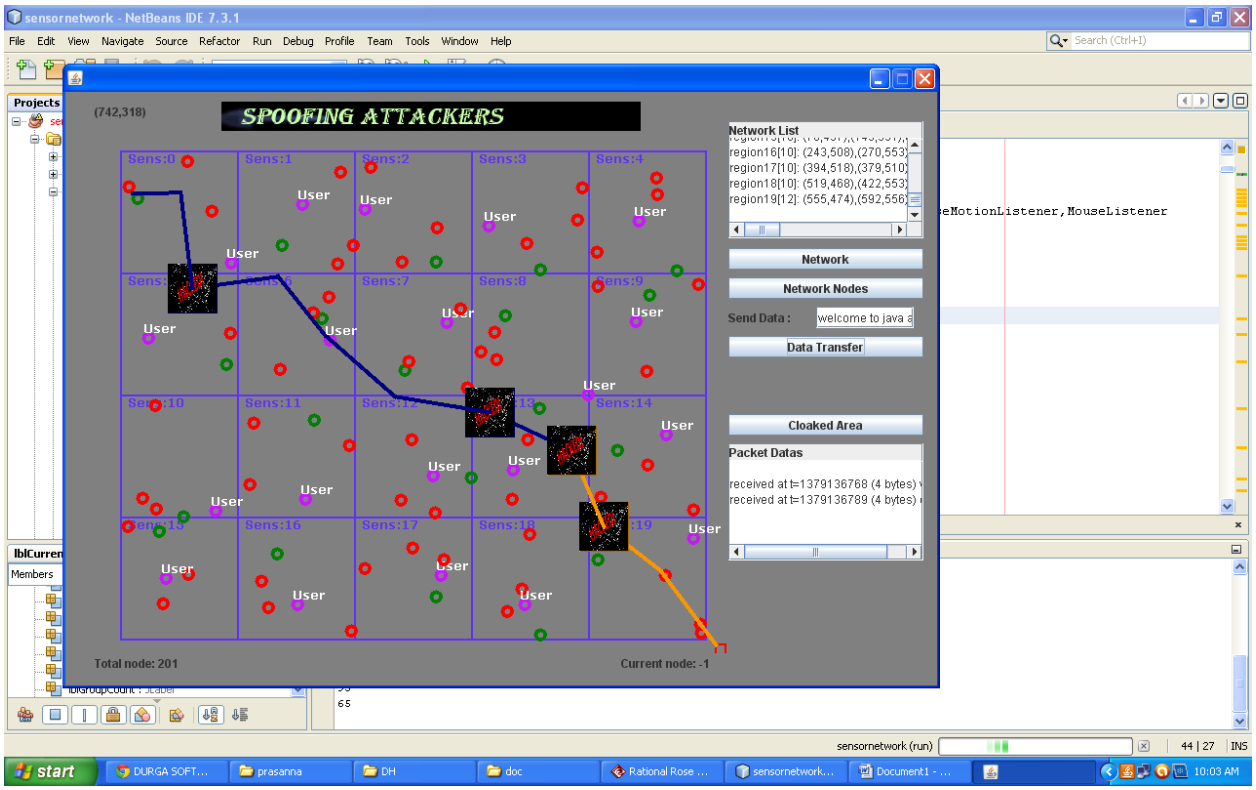


Simulation:

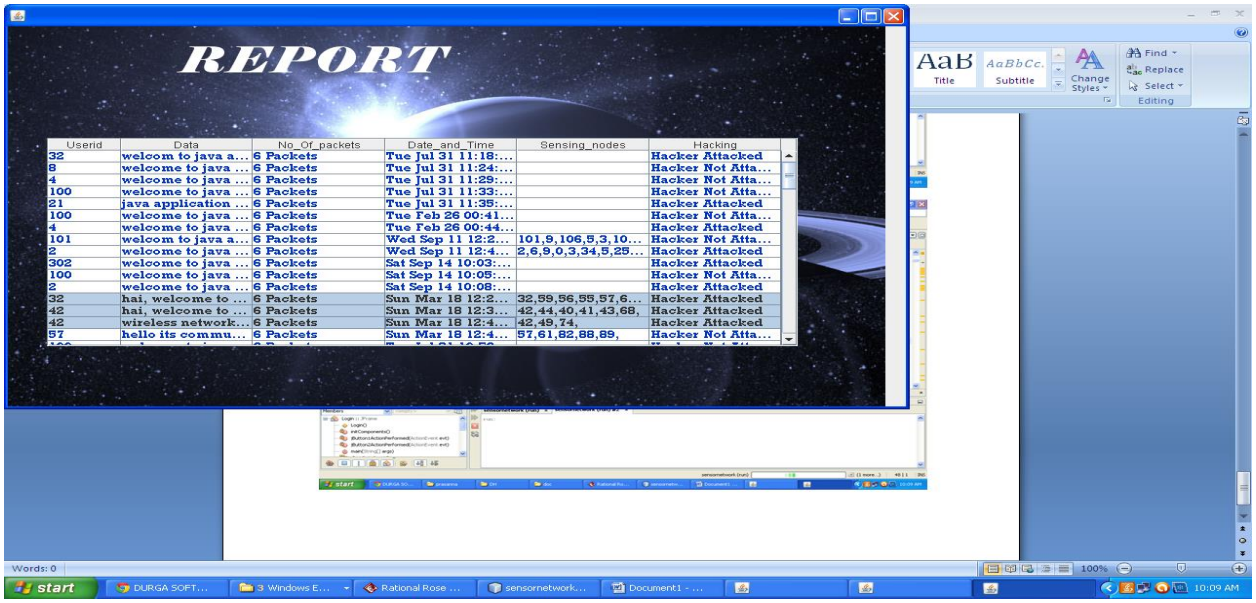
We plan to simulate using the Java Technology to find the malicious that bluff by discovering the attacker nodes and by localizing the nodes. At first, we define the bluff attack and create a group of homogenous nodes in multiple networks.



Then by using localized nodes within the range , it then discovers the path and confine the particular way.



By using that it generally confine multiple nodes in an area and discovers the path in order to transfer the data packets. At last we make a report to discover and confine the malicious nodes in the network.



Conclusion:

In this work, we proposed a method for detecting bluff attacks as well as localizing the adversaries 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 formulated the bluff detection problem as a classical statistical significance testing problem. 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 bluff detector into the system to locate the positions of the attackers and as a result to eliminate the adversaries from the network. Therefore, our experimental results provide strong evidence of the effectiveness of our approach in detecting the bluff attacks and localizing the positions of the adversaries.

References:

1. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.
2. M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

3. L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4646-4651, June 2007.
4. 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.
5. F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.
6. L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137- 2145, 2008. P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE

