Enhanced Security Management through Detecting and Localizing Spoofing Adversaries in Network System

Archana L. Shelar
PG Student
JSPM's JSCOE, Hadapsar

Madhav D. Ingle
Associate Professor
JSPM's JSCOE, Hadapsar

ABSTRACT
Currently the Wireless Networks are used worldwide across the Globe. Such Wireless Networks are easily susceptible for variety of attacks. The variety of Spoofing attacks can also be easily launched in the wireless environment. Here this paper presents the new enhanced technique which makes use of the physical property mainly -RSS (The Received Signal Strength) associated with each node. It mainly focuses on RSS means the physical property instead of existing cryptographic techniques, which is hard or difficult to falsify and also independent of cryptographic techniques. This paper mainly focuses on ---Detecting Identity based spoofing attack, Determining number of attackers in the cluster network, Localizing and determining the actual position of attackers. Also this can further be used for Detecting Denial of Service attacks and Man in the Middle Attack. The experimental results show that this enhanced form doesn't require any additional efforts and also doesn't require extra modifications to the existing. Hence such things depict that this technique gives the enhanced security management as compared to the existing security techniques.

Keywords
Spoofing Attack, Security, Cryptography, RSS, and Wireless Network

1. INTRODUCTION
In the current age of Computing and communication networks, the more affection is laying towards the wireless networks. As the wireless networks are easily susceptible for various types of spoofing attacks, basically this paper focuses on Identity-based spoofing attacks as well as the enhanced and efficient techniques to secure from such attacks. The existing security technique involves the key computation cryptographic schemes, but such techniques are not always affordable due to its key computation and respective management. Hence to enhance efficient and such effective security management this paper gives the innovative and improved technique to use the physical property based on RSS (Received Signal Strength).Received Signal Strength is the physical property associated with each node. The security management scheme based on RSS, It doesn't require any additional modifications to the existing code. Also it is totally independent from the key based cryptographic technique, and hard to falsify. Here the objective which is obtained through the RSS-based security techniques as like--------

- Detection of Identity based spoofing attack.
- Computing number of spoofing attackers.
- Positioning of actual location of the attackers in the victim targeted system.
- Also Detects the Denial-Of-Service attack with location of attackers.

2. EXISTING WORK
The traditional approach makes use of cryptographic technique of Symmetric algorithm like either AES or 3-DES, but this AES or other algorithm includes key distribution and management kind of overhead. Such cryptographic algorithms require a lot of efforts for reliable key management; further cryptography considers the PKI (Public Key Interface) which can reduce the overhead of key management to some extent. Further work gives the hash technique and key revocation n key distribution implemented by Wool. However due to limited resources on wireless devices and lacking of a fixed key management infrastructure in the wireless network, such cryptographic techniques are not affordable. This is what the reason that's why this paper makes use of newly advanced physical property associated with each node i.e. RSS (Received Signal Strength).Previously the RSS work was given by the Sheng et al. He modeled the RSS readings using a Gaussian mixture model [7] and the Chen et al. used K-means cluster analysis and RSS to detect Identity-based masquerading attacks, but unfortunately any of these approaches do not have the ability to determine the number of attackers when multiple adversaries use the same identity to attempt such attacks, This is the basis to further localize multiple adversaries after detection of attackers. Previously the Chen et al studied about how to localize adversaries [9]; but unfortunately it can only handle the case of a single spoofing attacker and cannot localize the attacker if the adversary uses different transmission power levels.

3. PROPOSED WORK
Here two advanced models are proposed mainly for detection and localization of Identity-based Spoofing Attacks accordingly as like

- G-MOAD
- IDAL-M

1. Generalized Model Of Attack Detection (G-MOAD).

2. Integrated Detection and Localization Model (IDAL-M).

1.**G-MOAD**:- Basically this particular model mainly focuses on Detection of Identity based spoofing Attack----for that purpose it consists of the new advanced technique that is---Partitioning around Medoids (PaM).As the spoofing attack detection could be performed by RSS-based spatial co-relation from wireless nodes, It also showed that the RSS readings from a wireless node may fluctuate and that could be clustered together. Basically, the RSS readings obtained over time from the same physical location will belong to the same

cluster points in the n-dimensional area called as n-signal space, whereas the different locations may have variety of RSS readings over time that should form different clusters in signal space. The observation suggests that cluster analysis could be conducted on top of RSS-based spatial correlation so as to find out the distance in signal space and further detect the presence of spoofing attackers in physical space. In this work, trick is to use Partitioning around Medoids Method to perform clustering analysis in RSS.

❖ Partitioning around Medoids:-

The according to PaM technique it consists of:-

Particularly in this attack detection phase following mathematical steps can be followed :-

1. Initially partition the RSS Vectors from the same node identity into 2 clusters.

2. Choose the distance between two medoids as Dm.

3. Calculate Dm= Di – Dj

4. If Dm is small

Then Spoofing Attack is not detected

5. Else if Dm is large

Then Spoofing Attack is detected.

For example: - The diagram is proposed to indicate Dm as distance between medoids.

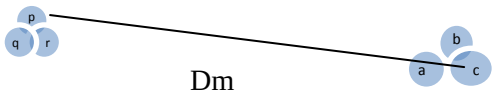

Fig 1: Distance Dm between medoids.

In this way finally the objective to detect the presence of attacks should be done. Here Mi and Mj are the medoids of two clusters. Basically under normal conditions only one cluster from a single and uniquely same physical location. In opposite whenever, there is probability of masquerading spoofing attack, there is more than one node at different physical locations claiming the same node identity. This result into the vulnerable portion, where more than one cluster will be formed in the signal space and Dm will be large as the medoids are derived from the different RSS clusters associated with different locations in physical space.

❖ System Evaluation:-

This technique is basically used for determining actual number of attackers in the network system. This technique makes use of Twin-Cluster Model from cluster analysis. It means this signifies that Twin-Cluster Model includes two closest clusters (e.g., clusters a and b) among K Potential clusters of a data set. Energy calculation is done by using twin cluster model. Mathematical model includes 2 types of energies—

1. Partition Energy (Ep (K))

2. Merging Energy (Em(K))

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. Here the border region includes a number of sample points chosen from clusters a and b that are closer to its twin cluster than any other points within its own cluster. Then further equations of partition energy and merging energy signify the conclusion as

1. Calculate Partition Energy Ep(K)

2. Calculate Merging Energy Em(K)

3. Then

   If

   Ep (K) > Em (K) &&
   Ep (K+1) < Em (K+1)

4. Then

   Koptimal = K

Where the value of K gives the actual number of spoofing attackers in the system.

Integrated Detection and Localization Model (IDAL-M)

This section presents the technique which can be used for localizing actual position of the spoofing attackers. Here RADAR algorithm is used.

❖ RADAR Algorithm:-

The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from [15].Here the proposed RADAR-Gridded makes use of an highly focused interpolated signal map, Here the set of averaged RSS readings with known (X, Y) locations can be used to build a focused map. From the observed RSS reading with an unknown location, in response the RADAR gives back co-ordinates such as 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 as n-signal space, Here N is denoted as the number of landmarks.

Further it makes use of Euclidean's distance formula to get actual position (X, Y) co-ordinates of location. So gives the exact location of spoofing attackers.

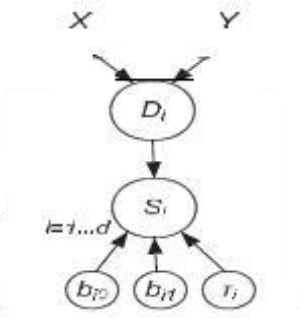

Fig 2: Probable location Area

4. THE SERVICE REJECTION DENIAL OF SERVICE ATTACK DETECTION

The DSR Algorithm can be used further for detection of Denial of Service Attack.

Initially R= i = Request, S – Service;

1. For (i=0; i<=2; i++)
   a. S++
2. If (i= Infinity || >= T)

   // No response from Server

   S= NULL;

   // i.e. Denial of Service Attack detected

   D= Attack Detected=1;

   // D=0 if attack not detected

3. Printf("Attack is detected");

This algorithm accurately detects the Denial of Service Attack. Experimental results show that this gives the efficient and effective way of Attack detection of type Denial of Service Attack.

5. EXPERIMENTAL RESULTS AND COMPARISON

The Evaluation results obtained from these models result into some effective graphs as follows:-

These techniques evaluated for 802.11(Wi-Fi) and 802.15(Zigbee) networks resulted into high detection rate as compared to previous approaches.

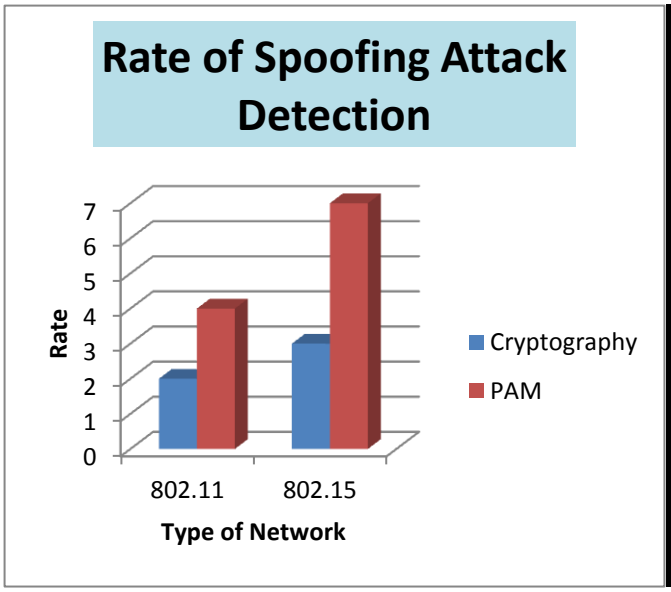

Fig 3: Graph for Attack Detection Rate

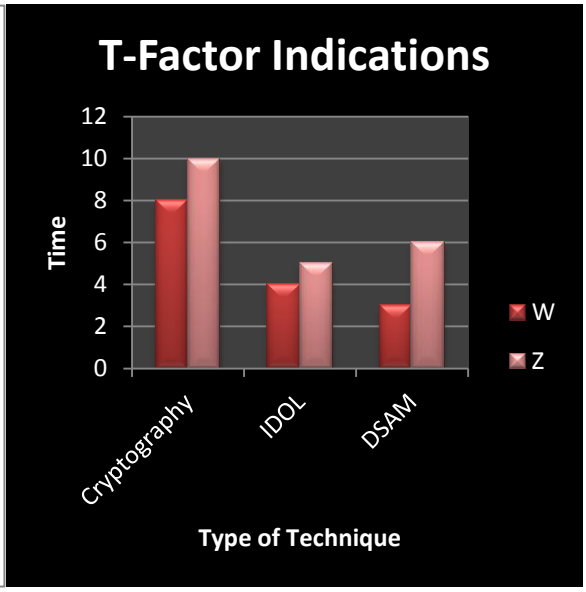

Fig 4: Graph for Time Factor Requirement

Here the plotted graph Fig.3 indicates the Spoofing attack detection in both Previous and proposed techniques. The detection rate is higher in case of PAM (Partitioning around Medoids) showed that---here the attacks are detected with more high speed as compared to previous one. Also the RSS based PAM needs less time than Cryptography hence it is more effective.

Fig.4 shows the comparison among the timings of each technique. Hence from the graph conclusion can be given as IDOL model takes less time for all the computations than Cryptography. DSAM also takes very small amount of time than others.

6. CONCLUSION

Here the core idea is to use Received signal strength (RSS) instead of previous approaches like Cryptography, so as to detect Identity-based spoofing attacks and in advancement the Denial-of-Service attacks more effectively as compared to the existing one. RSS it's a physical property associated with each node, which is hard to falsify and also not reliant on cryptography. Here we proposed PAM technique for spoofing attack detection, further System Evaluation technique consist of twin-cluster model so as to get the exact number of attackers in the system(i.e.-MOAD) and also IDAL-M model to localize spoofing attackers in the network. As enhancement here DSA- algorithm would be proposed to detect Denial-of-Service attack. Evaluation results shows that all these proposed techniques are more efficient and effective than existing ones. Also that sufficiently reduces the overhead requirements of existing approaches, as those proposed techniques don't require any additional implementations. Hence result into high hit rate and precision, additionally high accuracy of localizing multiple adversaries.

7. FUTURE ENHANCEMENT

This proposed system can be further extended to detect all types of attacks and specifically Man-In-The-Middle attack.

8. REFERENCES

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

[2] 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.

[3] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[4] Q. Li and W. Trappe, "Relationship-Based Detection of Spoofing- Related Anomalous Traffic in Ad Hoc Networks," Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.

[5] 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. (IP DPS), 2005.

[6] 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.

[7]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.

[8]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.

[9] 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.

[10] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.

[11] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization,"Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks. (SECON), Sept. 2006.

[12] L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. Wiley Series in Probability and Statistics, 1990.

[13] G. Zhou, T. He, S. Krishnamurthy, and J.A. Stankovic, "Models and Solutions for Radio Irregularity in Wireless Sensor Networks,"ACM Trans. Sensor Networks, vol. 2, pp. 221-262, 2006.

[14] C. van Rijsbergen, Information Retrieval, second ed. Butterworths, 1979.

[15] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

[16] 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.

[17] P. Rousseeuw, "Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis," J. Computational and Applied Math., vol. 20, no. 1, pp. 53-65, Nov. 1987.

[18] K. Wang, "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, 2007.

[19] 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.