Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Detecting and Localizing Wireless Spoofing Attacks

M.Loganathan,
ECE & KCT Tamilnadu, India

V.Navaneethakrishnan,
ECE & AERI Tamilnadu, India

Abstract −Wireless networks are vulnerable to spoofing attacks, which allows for many other forms of attacks on the networks. Although the identity a node can be verified through cryptographic authentication, the authentication is not always possible because it requires key management and additional infrastructural overhead. In this project we propose a method for detecting spoofing attacks and locating the positions of adversaries which performs the attacks. At first we introduce an attack detector for wireless spoofing that utilizes K-means cluster analysis. Here we describe how integrate our attack detector into a real time indoor localization system, which is capable of localizing the positions of the intruders. Then we indicate the position of the attackers can be localized using either area-based or point-based localization algorithms with the same relative errors as in the normal case. Here we evaluated our methods through experimentation using both an 802.11 (WiFi) network and 802.15.4 (ZigBee) network. Our results show that is possible to detect wireless spoofing with both a high detection rate and a low false positive rate, thereby providing strong evidence of the effectiveness of the K-means spoofing detector as well as the attack localizer.

Keywords— Wireless network security, spoofing attack, attack detection, localization, MD 5 (Message Digest 5).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) in the military, environmental monitoring, earthquake and climate prediction, the exploration of deepwater, underground and outer space, and many other aspects has a wide range of application prospects [1]. However, its security is also facing the huge challenge, especially in the field which requires high security [2] [3]. To prevent eavesdropping and attack, there are many security schemes which are using point to point communication have been proposed [4]. However, due to node's computing ability, communication ability, storage ability and other aspects limited, the node cannot rely on itself to decide the security algorithm, and should rely on the security key-pair and intelligent routing to transmit information safely.

This paper introduces the risk and trust mechanism; ensure that the system can make a crucial decision during sharing information between nodes. Most existing approaches to address potential spoofing attacks employ cryptographic schemes [5], [6]. However, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanism. Further, cryptographic methods are susceptible to node compromise, it is a serious problem as more wireless nodes are easily accessible, allowing their memory are to be easily scanned. In this work, we propose to use received signal strength (RSS)-based spatial correlation, is a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Here we are concerned with attackers who have different locations than legitimate wireless nodes; utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localizing adversaries. An added advantage of employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves. We are focus on static nodes in this work, which are common for spoofing scenarios [7].

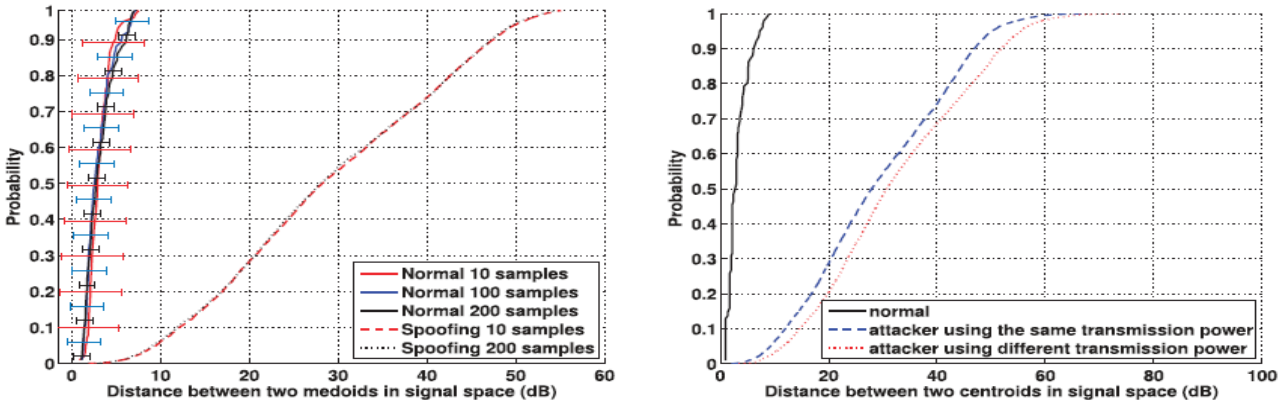
II. RELATED WORKS

2.1 Results of Attack Detection

2.1.1 Impact of Threshold and Sampling Number

The thresholds of test statistics define the critical region for the significance testing. Appropriately setting a threshold τ enables the attack detector to be robust to false detections.

Fig. 1 shows the Cumulative Distribution Function of Dm in signal space under both normal conditions as well as with spoofing attacks. We observed that the curve of Dm shifted greatly to the right under spoofing attacks. Thus, when $Dm > \tau$, we can declare the presence of a spoofing attack. The short lines across the CDF lines are the averaged variances of Dm under different sampling numbers. We observed that the CDF together, which indicate that for a given threshold τ similar detection rate will be achieved under different sampling numbers. However, the averaged variance decreases with the increasing number of samples—the short-term RSS samples are not as stable as the long-term RSS samples. The more stable the Dm is, the more robust the detection mechanism can be. Therefore, there is a trade off between the number of RSS samples needed to perform spoofing detection and the time the system can declare the presence of an attack. For this study, we use 200 RSS samples, which has a variance of 0:84 dB2.



(a) Sampling number study (b) Different transmission power

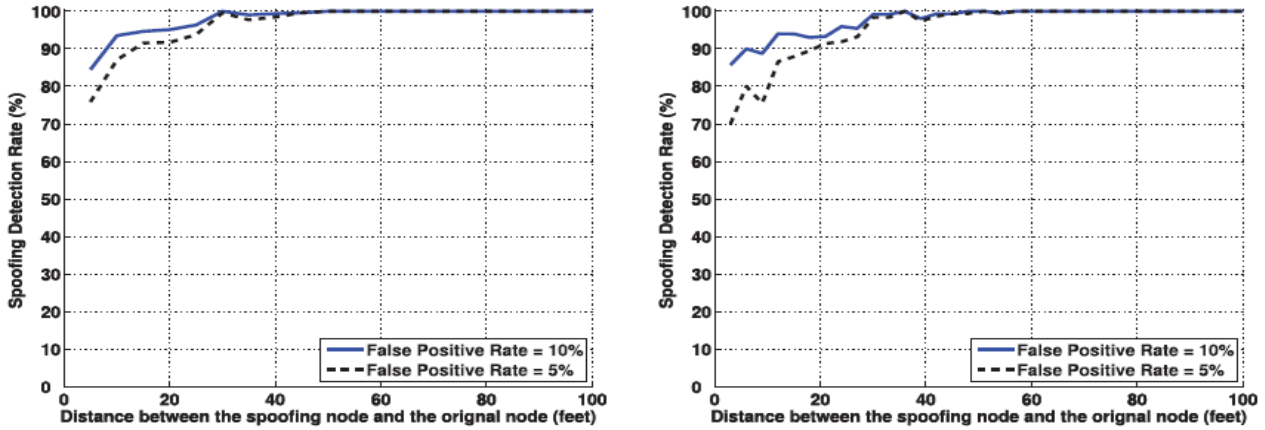
Fig.1 802.11 network: cumulative distribution of distance between Medoids Dm in signal space

2.1.2 Handling Different Transmission Power Levels

If a spoofing attacker sends packets at a different transmission power level from the original node, based on our cluster analysis there will be two distinct RSS clusters in signal space (i.e., Dm will be large). We varied transmission power for an attacker from 30 mW (15 dBm) to 1 mW (0 dBm). We found that in all cases Dm is larger than normal conditions. Fig. 5b presents an example of the Cumulative Distribution Function of the Dm for the 802.11 network when the spoofing attacker used transmission power of 10 dB to send packets, where the original node uses 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. 802.15.4 network, the detection rate is above 90 percent when the distance between Pspoof and Porg is about 20 feet by setting the false positive to 5 percent. This is in line with the average localization estimation errors using RSS [8] which are about 15 feet. If the nodes are less than 15 feet away, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90%, but still greater than 70 %. However, when Pspoof moves closer to Porg, the attacker also increases the probability to expose itself. The detection rate goes to 100% when the spoofing node is about 45-50 feet away from the original node. So in these related operations were give a better performance But we proposed MD5 has higher performance of its operations when compare to existing all methods.

2.1.3 Performance of Detection

To evaluate the effectiveness of using cluster analysis for attack detection, Fig. 3 presents the Receiver Operating Characteristic curves of using Dm as a test statistic to perform attack detection for both of 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 significant, shows that for false positive rates less than 11 percent, the detection rate are higher than 97 percent when the threshold τ 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.



(a) 802.11 network (b) 802.15.4 network

Fig.2 The detection rate as a function of the distance between the spoofing node and the Original node

2.1.4 Impact of Distance between the Spoofing Node and the Original Node

We further study how likely a spoofing device can be detected by our attack detector when it is at various distances from the original node in physical space. Fig. 2 presents the detection rate as a function of the distance between the spoofing node Pspoof and the original node Porg. We found that the further away Pspoof is from Porg, the higher the detection

rate becomes. This observation is consistent with our theoretical analysis presented in Section 2.1. In particular, for the 802.11 network, the detection rate goes over than 90% when Pspoof is about 15 feet away from Porg when the false positive rate is 5 percent.

III. PROPOSED METHOD

3.1 MD 5 Proposal (Message Digest 5)

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. RFC 1321, MD5 message-digest algorithm takes input as a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. The MD5 algorithm is used for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA. We proposed this algorithm for an approach for a Detecting and Localizing Wireless Spoofing Attacks. Whenever compare to existing methods this issue deliver a better result.

The Following algorithm elaborate deals on MD 5 proposal on Localizing wireless Spoofing Attacks,

Algorithm: Spoofing Detection and Localization

Step 1: Generate Unique ID for all nodes in the network using MD5 algorithm
Declare Variables number of node, time and round trip
Input message converted to 128 bits
Input message broken to512-bit blocks called chunks. These are 16, 32-bit little endian
md5 operates 128 bit state. i.e. 4, 32 bit words like A,B,C,D, which are all initialized to fixed contents
Main algorithm operates on each 512 bit message block consists of 4 rounds.
Step 2: Define the cluster and the nodes in clusters
Step 3: Let Clusters in Network be 'Cn'
Step 4: For (i=0; i<=Cn)
{
Attacker Node A=0;
Perform spoofing attack detection by checking the node key value in every cluster
A=A++;
//Node, which has replicated key value, is identified as attacker node
}
Step 5: Do the detection in every cluster
Step 6: Identified number of attackers 'A'
Step 7: Localize the Attacker, by indentifying their (X, Y) coordinate values of position.
In this arena we deliver a flow graph for this new proposal.

3.2 Spoofing Attack Detection

Spoofing attack detection is performed using Cluster Analysis. As the wireless network is deployed as clusters, the attackers are identified in each and every cluster separately. Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets (i.e., spoofing node or victim node). Since under a spoofing attack, the data packets from the victim node and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top spatial correlation to find out further detect the presence of spoofing attackers in physical space.

The following figure shows the spoofing attack detection on wireless sensor network,

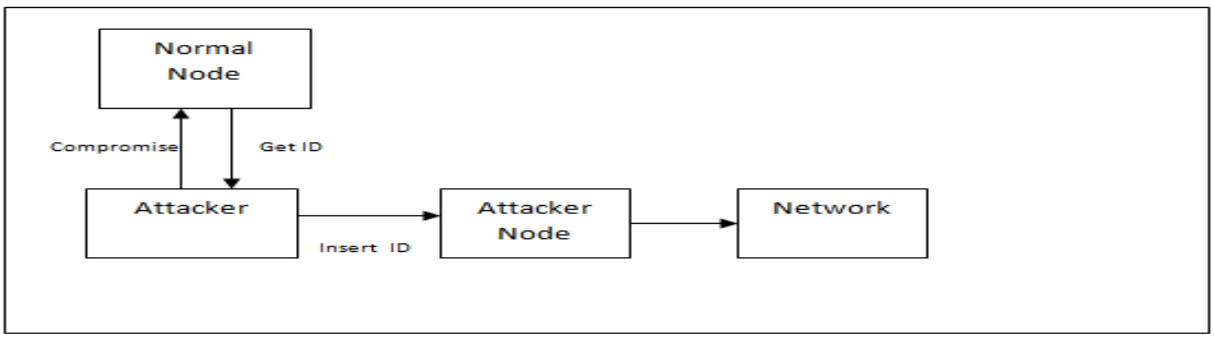


Fig.3: Spoofing Attack Detection

3.3 Detection of Multi-Spoofing Attack

The Partitioning Around Medoids (PAM) Method is used to perform clustering analysis. The PAM Method is a popular iterative descent clustering algorithm. Spoofing detection is identified as statistical significance testing problem, where the null hypothesis is: H0 : normal (no spoofing attack). In attack detection phase, the same node identity is partitioned into 2 clusters (i.e. K = 2) no matter how many attackers are using this identity. Distance between two medoids Dm is taken, significance testing for spoofing detection, Dm = ||Mi−Mj||, where Mi and Mj are the medoids of two clusters.

Under normal conditions, the test statistic Dm should be small, under a spoofing attack Dm will be large, there is more than one node at different physical locations claiming the same node identity. Initially the attacker 'A' is given a value 0. Whenever, the attackers are indentified, the value of A is incremented.

Normal node established the unique ID, Send location claim to all nodes, it undergoes cluster analysis, verify secret key, when the replication of key found, then the node is identified as attacker.

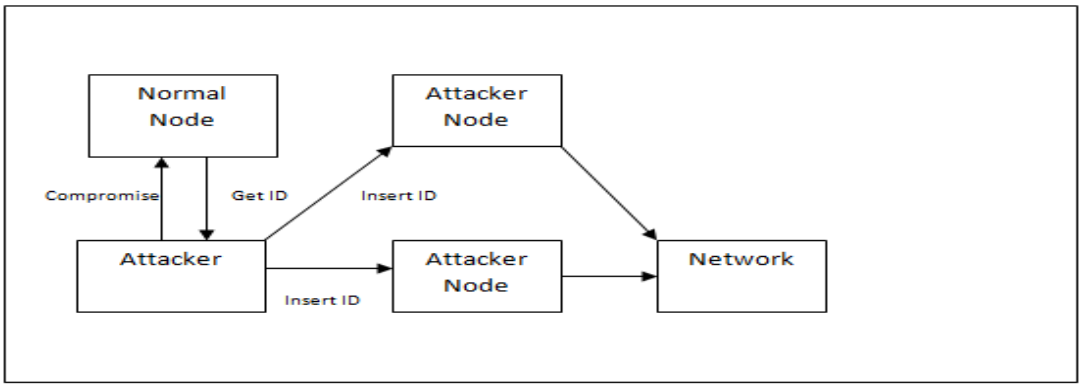


Fig 4: Detection of Multi Spoofing Attack

A scheme for both detecting spoofing attacks, as well as localizing the positions of the adversaries performing the attacks is proposed. Node identity is generated using MD5 algorithm, which derives key using hash function. A unique key is assigned for nodes, which is checked for duplication.

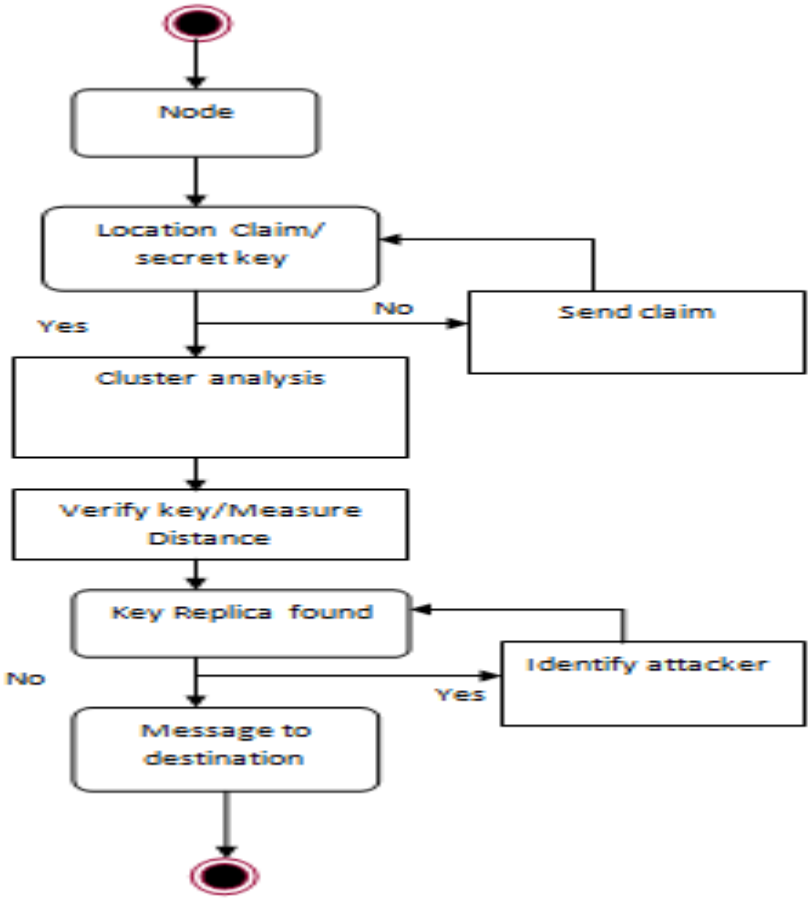


Fig .5 Activity Diagram

This method can be support us to identify Spoofing attack in the system when multiple adversaries masquerading as the same node identity. Under the spoofing attack, the victim and the attacker are using the same ID to transmit data packets. And also identify multiple spoof attackers in the network, we use cluster analysis to perform this. Each cluster in the networks is analysed for spoofing attack.

3.4 Localization of Attackers

The simulation is performed under Linux environment on NS2. Let us consider the number of nodes deployed in the simulation window for e.g. 3000X3000. The nodes are deployed in 2D platform. Each and every position of nodes are defined, thus from the initialized value, the attackers location in the 2D area can be determined accurately.

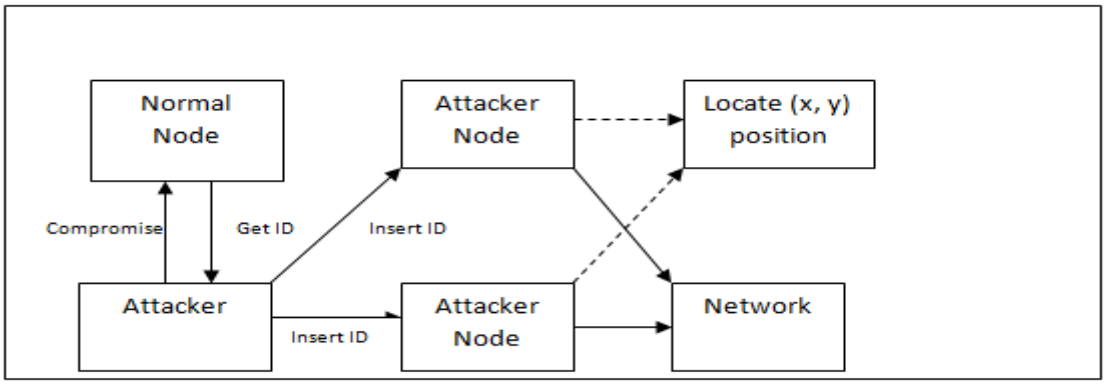


Fig 6: Localization of Attackers

The following flow graph shoes its operational wing,

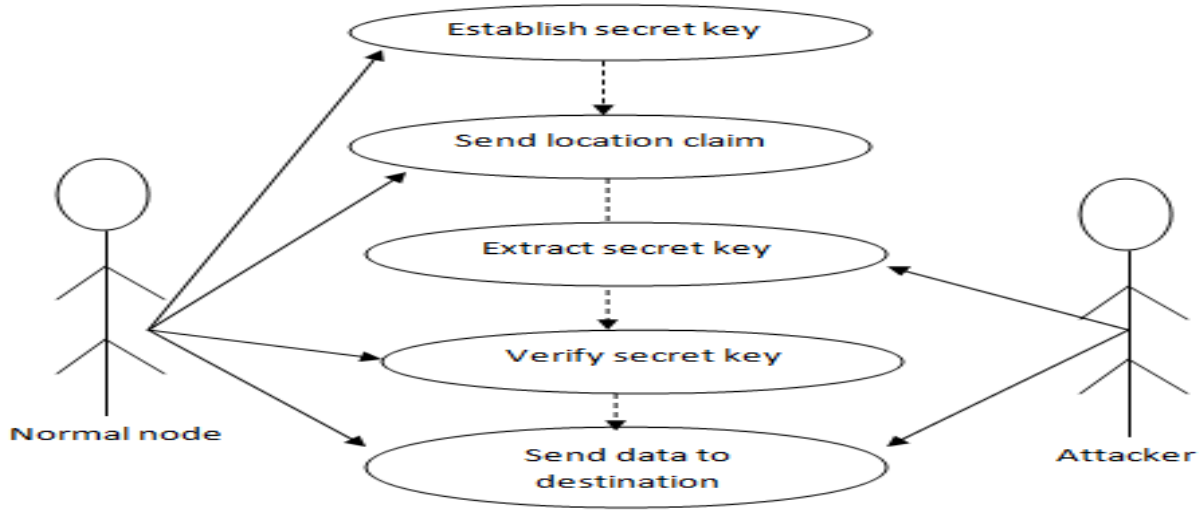
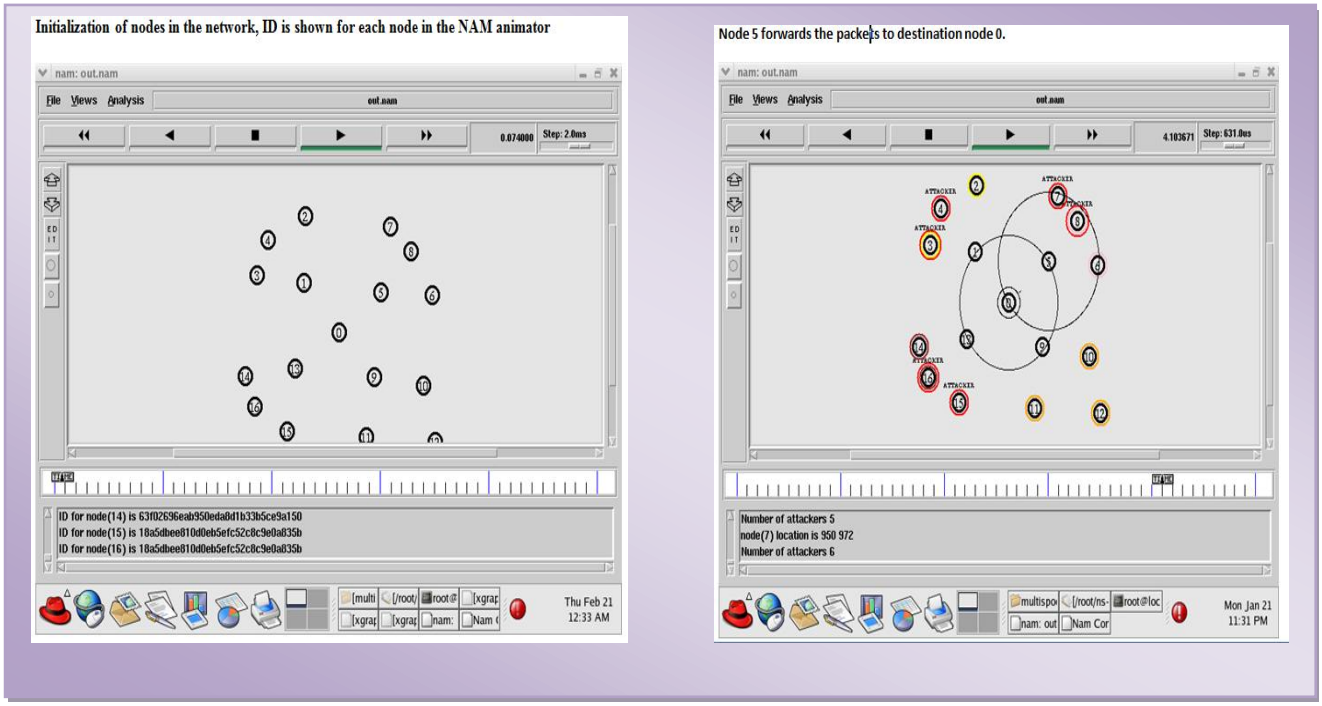


Fig 7: Use Case Diagram

Normal node established the unique ID, Send location claim to all nodes, verify secret key, when the packets arrive to the node, the acts as relay to send packets to destination. Whereas attacker node extracts secret ID from the normal node, try to send packets to destination.

IV. RESULT AND DISSCUSSION



MD5: Hit Rate, Precision, and F-Measure of Determining the Number of Attackers

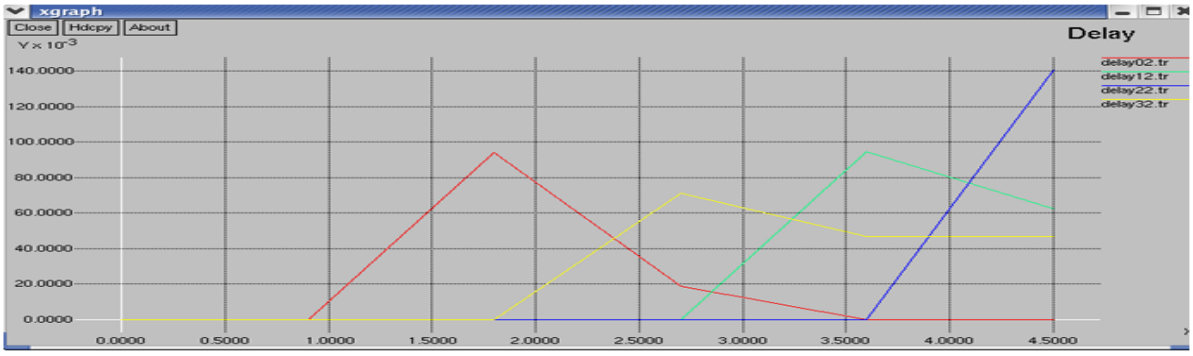
Number of Attackers	2	3	4
802.11Network,Hit Rate	99.87%	98.32%	90.16%
802.11Network,Precision	98.88%	91.52%	99.76%
802.11Network,F-measure	99.31%	95.65%	95.32%
802.11Network,Hit Rate	99.95%	96.14%	88.82%
802.11Network,Precision	96.95%	89.16%	99.87%
802.11Network,F-measure	98.56%	93.21%	93.43%

This is the most trendy method when through via MD5 (Message Digest 5) for an 802.11 wireless sensor networks. The simulation graphs and analysis reports deals and supported to this performance spoofing.

V. PERFORMANCE ANALYSIS

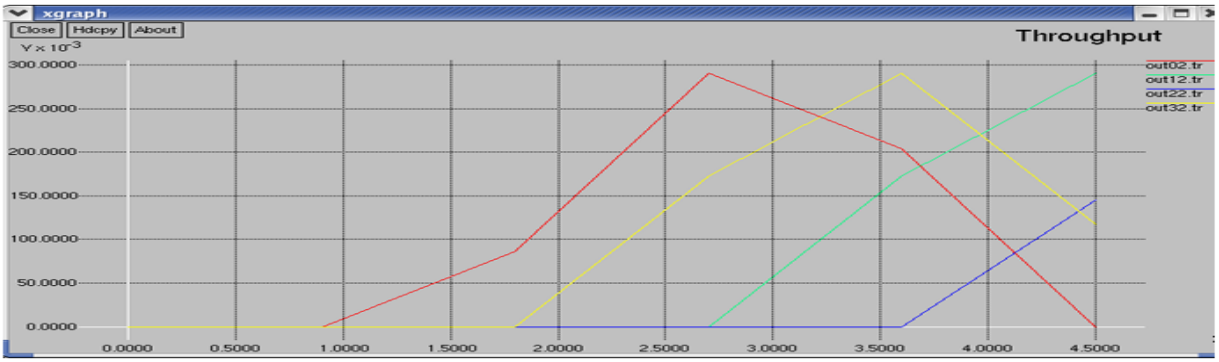
The NS2 simulation is done and we analysed Throughput, delay for the flow taken.

Delay



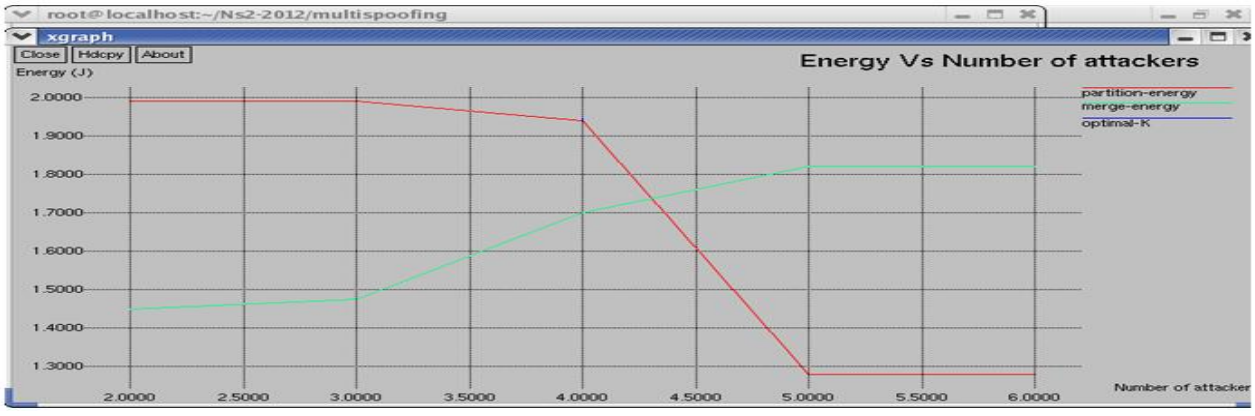
The above graph defines the delay in the simulation phase. The experiment was running 4.5 seconds of time. End to End Delay refers to the time taken for a packet to be transmitted across a network from source to destination during the simulation time.

Throughput



The above graph defines the throughput for the proposed protocol. The experiment was running 4.5 seconds of time. Throughput is the rate at which a network sends receives data. It is a good channel capacity of net connections and rated in terms bits per second (bit/s).

Energy Vs Number of Attackers



These are the model ethical analysis when compare to already exiting methods.

VI. CONCLUSION

The proposed approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so it can localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. This mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution, that use cluster analysis alone.

Further, based on the number of attackers determined by the mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. Here performance of localizing adversaries achieves same results as those under normal conditions by providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determines the number of intruders and to localize the adversaries.

REFERENCES

[1] Jie Yang, Student Member, IEEE, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe, Member, IEEE, and Jerry Cheng"Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.

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

[3] 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.

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

[5] 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.

[6] 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.

[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," Proc. IEEE INFOCOM, Apr. 2008.

[9] 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.

[10] Y. Chen, W. Trappe, and R.P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.

[11] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.

[12] 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.

[13] 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.

[14] 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.

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

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

[17] 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.

[18] 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.

[19] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS), Apr. 2008.

[20] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.

[21] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.

[22] T. He, C. Huang, B. Blum, J.A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Networks," Proc. MobiCom '03, 2003.

[23] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.

[24] A. Goldsmith, Wireless Communications: Principles and Practice. Cambridge Univ. Press, 2005.

[25] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A Survey of Various Propagation Models for Mobile Communication," IEEE Antennas and Propagation Magazine, vol. 45, no. 3, pp. 51-82, June 2003.
[26] M. Abramowitz and I.A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Courier Dover, 1965.
[27] L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. Wiley Series in Probability and Statistics, 1990.
[28] 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.
[29] Y. Chen, K. Kleisouris, X. Li, W. Trappe, and R.P. Martin, "The Robustness of Localization Algorithms to Signal Strength Attacks: A Comparative Study," Proc. Int'l Conf. Distributed Computing in Sensor Systems (DCOSS), pp. 546-563, June 2006.
[30] C. van Rijsbergen, Information Retrieval, second ed. Butterworths, 1979.
[31] T. Fawcett, "An Introduction to ROC Analysis," Pattern Recognition Letters, vol. 27, pp. 861-874, 2006.

Authors Details

M.Loganathan received his DEEE (Electrical and Electronics Engineering) from Thiyagarajar Polytechnic College, Salem, and BE (Electronics and Communication Engineering) Anna University of Technology, Coimbatore, Tamilnadu, India. Now he is pursuing Master of Engineering (Communication Systems) in Kumaraguru College of Technology, Coimbatore, India. His areas of interest include Network Security, communication Theory, and optical communication, Digital Communication. He presented papers on Information and Communication Technology.

V.Navaneethakrishnan received his DEEE (Electrical and Electronics Engineering) from Andaavar Polytechnic College, Erode, and received his BE (Electronics and Communication Engineering) Anna University of Technology, Coimbatore, Tamilnadu, India. Now he is pursuing Master of Engineering (Communication Systems) in Adhiyamaan College of Engineering, Hosur, Krishnsgiri, Tamilnadu, India. His areas of interest include Network Security, communication Theory, and optical communication. He presented papers on Information and Communication Technology

.

