A Survey on Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

Amey K. Redkar, Dnyaneshwar A. Rokade

Abstract— **Wireless networks are susceptible or vulnerable to identity based attack such as spoofing attacks which are easy to launch. Conventional cryptographic schemes to authenticate the communicator and detect any adversaries requires huge infrastructure and computational overhead. This paper describes survey on detection and localalization of multiple spoofing attackers in wireless networks. We have spatial information a physical property of a node which have its no dependence on cryptography and also hard to falsify for 1)determining spoofing attack. 2)determining the number of attackers when multiple adversaries masqueariding as the same node identity 3)localizing multiple adversaries.RSS(received signal strength) is used to determine spatial correlation and cluster based mechanisms are used to determine number of attackers. We can further improve the performance of determining the number of spoofing attackers using the Support Vector Machines (SVM) method to accurately predict the number of attackers. In addition, we developed an integrated detection and localization system that can localize the positions of multiple attackers. Two test beds like 802.11 (WiFi) network and an 802.15.4 (ZigBee) network are be used to evaluate our techniques.**

***Index Terms*—wireless network security, spoofing attack, attack detection, localization**

I. INTRODUCTION

As more wireless networks are deployed, they will increasingly become tempting targets for malicious attacks and multiple adversaries can easily monitor any transmission. For a couple hundred dollars a user can buy an 802.11 access point and low cost wireless device this same widespread deployment makes 802.11-based networks an attractive target for potential attackers. Due to the openness of wireless networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks. 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.

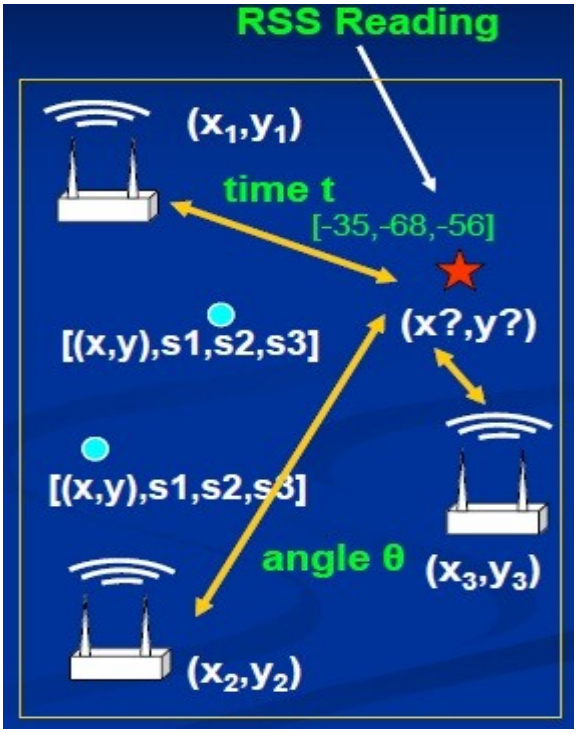

Fig1: Using spatial correlation to determine RSS

Spoofing attacks help in variety of traffic injecting attacks[1],[2],such as Denial-of-service attacks, access control list. Moreover Denial-of –service attacks and network source utilization attack can be easily launch in large networks where multiple adversaries act as same identity.[3],[4] shows a huge survey of possible spoofing attacks.

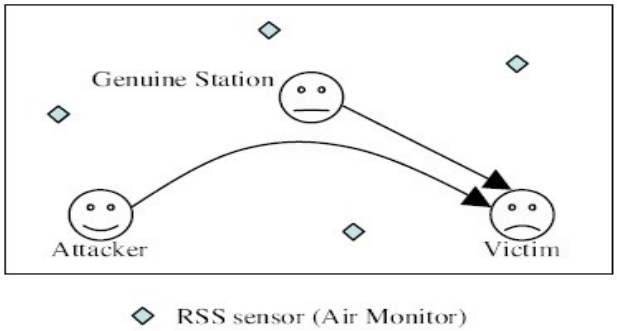

Fig 2: Roles involved in802.11 Mac layer spoofing

***Amey K. Redkar**, ME Research Scholar, Computer Engineering Department, University of Pune, Imperial College of Engineering and Research, Pune, Maharashtra, India, Mobile No +917507657841*
***Dnyaneshwar A. Rokade**, Asst. Professor, Computer Engineering Department, University of Pune, Imperial College of Engineering and Research, Pune, Maharashtra, India.*

The traditional approach to address spoofing attacks is to apply cryptographic authentication. Here cryptographic key requires manintaince, distribution mechanism also authentication requires additional infrastructural overhead and computational power associated. Due to the limited power and resources available to the wireless devices , it is not always possible to deploy authentication. Also cryptographic method are vulnerable to spoofing attacks as wireless nodes allow easy access to scan their memory 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. As we are dealing with attackers having different locations, spatial information helps in not only detecting spoofing attacks but also to localize the adversaries.

Spoofing scenarios have static node which is focus in the [7], also [8] shows spoofing attacks in mobile environments. Survey in[3][7][9] are closely related to our idea of detecting spoofing attacks.

[3]Deals with detecting spoofing attack using signal prints.[7]deals with using Gaussian mixture model and[9]deals with k-mean cluster analysis. however these methods would only detect spoofing attacks but could not handle nodes with different power levels.

Our main focus is on methods 1)GADE and 2)IDIOL. Gade works on the principle of cluster analysis of RSS readings to detect th spoofing attacks as well as detect the number of attackers.Idiol works on the same principle of as that of GADE but IDIOL can find out attackers when spoofing attackers has various power levels.

Problem Statement

Traditional method were using cryptographic authentication which has much

Overhead but existing system uses spatial correlation technique using RSS property of the nodes. These techniques not only detect spoofing attacks but also detect the number of attackers for these techniques we used GADE method and in addition we have IDIOL method to localize the number of attackers.

II. RELATED WORK

Mechanism based on cryptographic method

Traditionally cryptographic authentication mechanism were used to detect spoofing attacks.[5][6][10] focus on the traditional approach of detecting spoofing attacks.

1) Working in SEKM framework

[5] Unreliable wireless media, host mobility and lack of infrastructure, providing secure communications are the problems in mobile ad hoc networks, due to Usually, cryptographic techniques are used for secure communications in wired and wireless networks. In fact, any cryptographic means is effective if its key management is strong. Key management is also a central aspect for security inmobile ad hoc networks.This paper propose a secure and efficient key management (SEKM) framework for mobile ad hoc networks. SEKM has a public key infrastructure (PKI) and applies a secret sharing scheme and using multi-cast server groups. Giving detailed information on the formation and maintenance of the server groups. In this methodology SEKM, each server group creates a view of the certificate authority (CA) also provides certificate update service for all nodes which also includes the servers themselves.

2) Working for fully revoked and eavesdrop mechanism:

[6]In this paper we focus on a management problem IEEE 802.11 wireless LANs suffer from. IEEE 802.11 has been designed with static long term keys shared by all stations which has limited key management capabilities.These situation makes it difficult to fully revoke access from previously fully authorized host. A host is *fully* revoked when it can no longer associate with the network access point,and more importantly, when it can no longer *eavesdrop* and decrypt traffic generated by other hosts on the wireless LAN is reduced if the keys expire fast enough.The most natural setting for a WEP∗ implementation is in vendors' firmware.

3) Working for Tesla certificate mechanism

[10]Results show scalability problems for flat ad hoc networks. To represent the issue of scalability, self-organizing hierarchical ad hoc architectures are being search. In this paper, the task is to provide data and entity authentication for hierarchical ad hoc sensor networks. Sensor network consists of three tiers of devices with varying levels of computation and communication capabilities. Lowest tier consists of compute-constrained sensors that are unable to perform public key cryptography. This paper presents a new type of certificate, called a TESLA certificate that can be used by low-powered nodes to perform entity authentication. Our framework authenticates incoming nodes, maintains trust relationships during topology changes through an efficient handoff scheme, and provides data origin authentication for sensor data. Further, this framework assigns authentication tasks to nodes on their computational resources and resource-abundant access points performing digital signatures and maintaining most of the security parameters.

Mechanism based on using Physical properties

1) Working using WiSE ray-tracing tool

[11]Recent approaches include using the physical properties of the wireless network have neeb designed.The property that the wireless medium contains domain-specific information this information can be used to complement and enhance traditional security mechanisms.This paper shows a typical rich scattering environment of radio channel response and decorrelates quite rapidly in space.This methodology describe a physical-layer algorithm that consist of channel probing (M complex frequency response samples over a bandwidth W) with hypothesis testing to determine that the current and prior communication attempts are made by the same user (same channel response). In this way, legitimate users can be reliably authenticated and false users can be reliably detected. To evaluate the feasibility of our algorithm, we simulate spatially variable channel responses in real environments using the WiSE ray-tracing tool; and we analyze the ability of a receiver to discriminate between

transmitters (users) based on their channel frequency responses in a given office environment.

2) Working of PARADISE technique

[12]Technique called PARADISE is implemented to identify the source network interface card of IEEE 802.11 frame using passive radio-frequency analysis.PARAdise finds out minute imperfection of transmitter hardware.In PARADISE we can measure di_erentiating artifacts of individual wireless frames in the modulation domain, and can apply suitable machine-learning classification tools to achieve signifcantly higher degrees of NIC identication accuracy than prior best known schemes. We 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. This tech-nique, called PARADIS, leverages minute imperfections of transmitter hardware that are acquired at manufacture and are present even in otherwise identical NICs. These imper-fections are transmitter-speci_c and manifest themselves as artifacts of the emitted signals. In PARADIS,We experimentally demonstrate e_ectiveness of PARADIS in di_erentiating between more than 130 identical 802.11 NICs with accuracy in excess of 99%. Li and Trappe [4] introduced a security layer that used forgeresistant relationships based on the packet traffic, including MAC sequence number and traffic pattern, to detectspoofing attacks.MAC sequence number is also surveyed in

Mechanism using RSS method

The works [3], [7], [14] using RSS to defend against spoofing attacks are most closely related to us. Faria and Cheriton [3] proposed the use of matching rules of signalprints for spoofing detection. Sheng et al. [7] modeled the RSS readings using a Gaussian mixture model. building RSS profiles for spoofing detection. Experiments on the same testbed show that this method is robust against antenna diversity and significantly outperforms existing approaches. At a 3% false positive rate, this detect 73.4%,89.6% and 97.8% of attacks using the three proposed algorithms,based on local statistics of a single AM, combining local results from AMs, and global multi-AM detection, respectively.

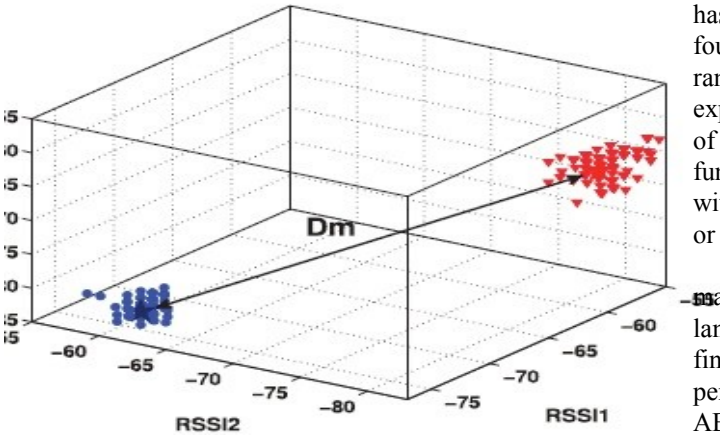

Fig 3:Illustration of RSS readings from two physical locations

Sang and Arora [14] proposed to use the node's "spatial signature,"This paper researches the feasibility of crypto-free communications in resource-constrained wireless sensor networks and exploit the spatial signature induced by the radio communications of a node on its neighboring nodes.This concept robustly realize our concept at the level of individual packets and when the network is relatively sparse.This concept design a protocol that robustly and efficiently validates the authenticity of the source of messages: authentic messages incur no communication overhead whereas masqueraded communications are detected cooperatively by the neighboring nodes. The protocol enables lightweight collusion-resistant methods for broadcast authentication, unicast authentication, non-repudiation and integrity of communication.

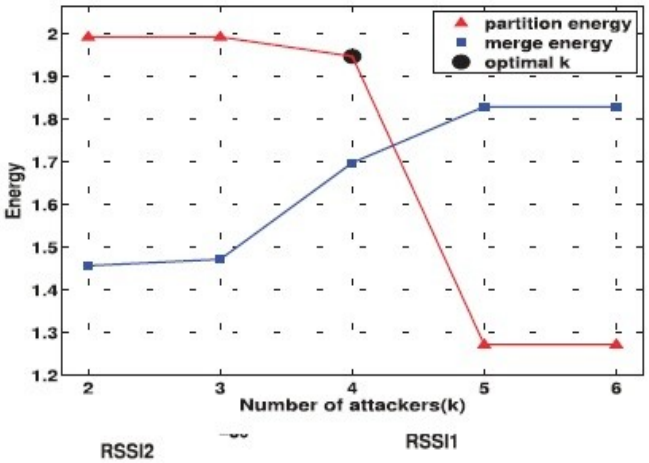

Fig. 4. System evolution: detection of four adversaries masquerading the same node identity.

Mechanisms for localizing attackers

Localizing techniques are shown in[15],[16],[17],[18].Here th an attractive approach because the existing wireless infrastructure and is highly correlated with physical locations and can be reuse fo localization.

[16] Shows the fundamental limits of localization using signal strength in indoor environments. Signal strength approaches are attractive because they are widely applicable to wireless sensor networks and do not require additional localization hardware. It shows that although a broad spectrum of algorithms can trade accuracy for precision, none has a significant advantage in localization performance. They founded that using commodity 802.11 technology over a range of algorithms, approaches and environments, one can expect a median localization error of 10ft and 97th percentile of 30ft.They present strong evidence that these limitations are fundamental and that they are unlikely to be transcended without fundamentally more complex environmental models or additional localization infrastructure.

[17]Shows that Derived an upper bound on the maximum location error given the placement of landmarks.Developed a novel algorithm, maxL-minE, for finding the optimal landmark placement.Significant performance improvement of a wide variety of algorithms ABP and RADAR: > 20%,LS: > 30%,BN: ~ 10% .Tension between optimized landmark deployment for localization vs. deployments that optimize for signal coverage.

[18] helps in Accurately obtaining the position of mobile devices is critical to high-level applications. In indoor environments, localization approaches employing RF-based fingerprint matching is an active research area because it can

reuse the existing communication infrastructure, as well as reduce the signal uncertainty to achieve better location accuracy. In this paper they provide a theoretical analysis of the localization performance when using fingerprint matching schemes.Particularly, they studied the effects of the number of sampling points and the distance between adjacent sampling points.

III. PROPOSED WORK

By studying above research works by researchers we are proposing spoofing attacks detection techniques ot secure system for transmission of data over wireless network based on these work as follows:

We have two model on which our system will work GADE and IDIOL.We are using spatial correlation mechanism to find RSS reading which are related to physical property of the node use to determine spoofing attacks.This techniques work with cluster analysis which is use to detect the spoofing attackers. RSSS using signalprints[3],gausssian mixture[7]or spatial siganature [14] can be used to determine the RSS readings.

Architecture

In GADE the partitioning around mediod technique of cluster analysis is used to detact the spoofing attacks and problem is formulated as a multiclass detection problem.Cluster based method are used to determine the number of attackersFurthur sillhoute and SILENCE mechanisn are used to determine the accuracy of determing the position of attackers.Also for further accuracy Support vector machine technique is used to determine the position of attackers.

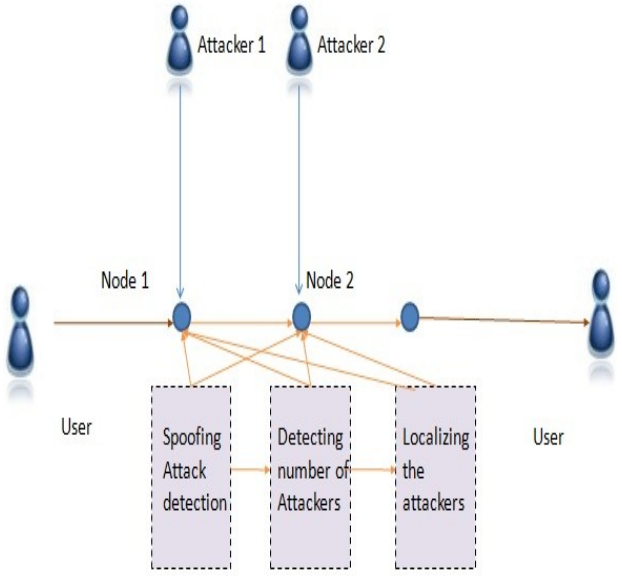

Fig-5 Architecture of our model

IDIOL method uses the output from the GADE method to find out the number of attackers and IDIOL method has the mechanism to localize the multiple adversaries which varies their power level.IDIOL can handle the number of attackers which have different transmission power levels.

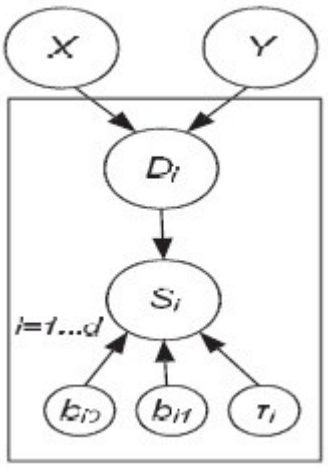

Fig 6: Bayesian model in our study

Algorithms

- Area-based probability

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.

- RADAR-gridded.

The RADAR-Gridded algorithm is a scene-matching localization algorithm extended from [15]. RADAR-Gridded uses an interpolated signal map, which is built from a set of averaged RSS readings with known ðx; yÞ locations. 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.

IV. CONCLUSION

In this paper we have done survey on attack detection in wireless network. We have studied all the references by scholars to develop a mechanism to develop a spoofin attack detection technique and localize the number of attackers by following GADE model.

We have studied a spoofing attack detection techniques where it is used and today world as much of data is send through wireless device it is very important to use these technique. It is very precise and efficient in detecting attacker.

As these attack detection techniques are use to determine the number of attackers.We are further proposing to increase their accuracy of finding their position accurately and localizing it using IDIOL techniques and its algorithm

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. (IPDPS), 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] 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.
[9] 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.
[10] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.
[11] 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.
[12] 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.
[13] 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.
[14] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.
[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] 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.
[18] 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.
[19] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.
[20] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.
[21] 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.
[22] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.
[23] A. Goldsmith, Wireless Communications: Principles and Practice. Cambridge Univ. Press, 2005.
[24] 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.
[25] M. Abramowitz and I.A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables. Courier Dover, 1965.
[26] L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. Wiley Series in Probability and Statistics, 1990.
[27] 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.
[28] 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.
[29] C. van Rijsbergen, Information Retrieval, second ed. Butterworths, 1979.
[30] T. Fawcett, "An Introduction to ROC Analysis," Pattern Recognition Letters, vol. 27, pp. 861-874, 2006.
[31] 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.
[32] 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.

AMEY K. REDKAR is M.E Research Scholar from the Imperial College of Engineering & Research, Pune, Maharashtra, India. Main research areas: wireless networks, Cloud Computing, Computer network, Network Security.

DNYANESHWAR A. ROKADE is an Asst. Professor from the Imperial College of Engineering & Research, Pune, Maharashtra, India. Main research areas: Computer network, Data Mining, Network Security, cloud computing .

