By comparing the results of SVM to those of Silhouette Plot, System Evolution and SILENCE methods, here observation is that there is a significant increase of Hit Rate, Precision and F measure for all the cases of the number of attackers under study. These results demonstrate that SVM-based mechanism, a classification approach that combines training data and different statistic features is more effective in performing multiclass attacker detection when multiple attackers are present in the system.

4.3 Idol: Integrated Detection And localization Framework

IDOL: an Integrate DetectiOn and Localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels.

CONCLUSION

This project proposed to use received signal strength mechanism and implement the clustering, SVM to identify the attack, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. It provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. It derived the test statistic based on the cluster analysis of RSS readings. The approach can both detects the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, also that can localize any number of attackers and eliminate them.

References:-

1.P. Bahl and V.N. Padmanabhan, “RADAR: An in-Building RF- Based User Location and Tracking System,” Proc. IEEE INFOCOM, vol. 2, Page(s): 775 – 784, 2000

2.Modern Promising Algorithm to avoid Spoof Attack by Cryptography :- **Murthy, K. N. B.; Sudheendra, H. USA ,4 New orleans conference**

PUB. DATE August 2008 SOURCEProceedings of World Academy of Science: Engineering & Technolog;Aug2008, Vol. 44, p690.,Singapore.WASET.

3. Daniel B. Faria and David R. Cheriton, “DoS and Authentication in Wireless Public Access Networks,” In Proceedings of the First ACM Workshop on Wireless Security (WiSe’02), September 2002

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

5. B. Wu, J. Wu, E. Fernandez, and S. Magliveras, “Secure and Efficient Key Management in Mobile AdHoc 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. F. Guo and T. Chiueh, “Sequence Number-Based MAC Address Spoof Detection,” Proc. Eighth Int’l Conf. Recent Advances inIntrusion Detection, pp. 309-329, 2006.

8. Xiao L and Trappe W, “Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication,”

Proceedings of IEEE International Conference on Communications (ICC), pp. 4646-4651, 2007

9. Y. Chen, W. Trappe, and R. P. Martin, “Detecting and localizing wireless spoofing attacks,” in SECON’07: Proceedings of the 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks, June 2007.

10 Z. Yang, E. Ekici, and D. Xuan, “A Localization-Based Anti-Sensor Network System,” Proc. IEEE INFOCOM, pp. 2396-2400, 2007.

11 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

12 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.

13 Lifeng Sang and Anish Arora, ”Spatial Signatures for Lightweight Security in Wireless Sensor Networks,” proc. IEEE INFOCOM, page 2137-2145, 2008.

14. 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.

15. Gayathri Chandrasekaran, John-Austen Francisco, Vinod Ganapathy, Marco Gruteser and Wade Trappe, “Detecting Identity Spoofs in IEEE 802.11e Wireless Networks,” proc. IEEE GLOBECOM, 2009.

15. Jeong Heon Lee and R. Michael Buehrer, ”Location Spoofing Attack Detection in Wireless Networks,” proc. IEEE GLOBECOM,2010

16.Liang Xiao, Alex Reznik, Wade Trappe, Chunxuan Ye, Yogendra Shah, Larry Greenstein and Narayan Mandayam, “PHYAuthentication Protocol for Spoofing Detection in Wireless Networks,” proc. IEEE Global Telecommunications Conference (GLOBECOM), 2010.

17. F.A. Barbhuiya, S Biswas and S Nandi, “An Active DES based IDS for ARP Spoofing,” IEEE International Conference on Systems, Man, and Cybernetics (ICSMC), Page(s): 2743 – 2748, 9 Oct 2011.

18. Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen and Gérard Lachapelle, “GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation,” IEEE/ION PLANS April 24-26, 2012

19. Jie Yang, Yingying Chen and Wade Trappe, “Detection and Localization of Multiple Spoofing Attackers in Wireless Networks”, IEEE Transaction on parallel and distributed system, Vol. 24, NO. 1, January 2013