

How to find a research problem

30,000 feet

- Information Security
- Software Engineering
- Database Systems
- HCI
- E-commerce
- Distributed Systems

20,000 feet

- Survivable Systems Engineering
- Database Security
- Privacy
- Intrusion Detection

10,000 feet

- Intrusion Detection in Wired Networks
- Intrusion Detection in Wireless Networks

5,000 feet

- Intrusion Detection in WLAN
- Intrusion Detection in ad hoc networks

3,000 feet

- Intrusion Detection in Static ad hoc networks
- Intrusion Detection in Mobile ad hoc networks (MANET)

Initial Literature Review

- Razi, M., Quamar, J. (2008). "A hybrid cryptography model for managing security in dynamic topology of MANET". International Symposium on Biometrics and Security Technologies.
- Sterne, D., Balasubramanyam, P., Carman, D., Wilson, B., Talpade, R., Ko, C., Balupari, R., Tseng, C.-Y., Bowen, T. (2005). "A general cooperative intrusion detection architecture for MANETs". Proceedings of the 3rd International Workshop on Information Assurance.
- Vigna, G., Gwalani, S., Srinivasan, K., Belding-Royer, E., and Kemmerer, R. (2004). "An Intrusion Detection Tool for AODV-based Ad Hoc Wireless Networks". In Proceedings of the Annual Computer Security Applications Conference.
- Zhang, Y., Lee, W., and Huang, Y. (2002). "Intrusion detection techniques for mobile networks". Wireless Networks, Volume 9, Issue 5.
- Fox, K. L., Henning, R. R., Reed, J. H., and Simonian, R. (1990). "A neural network approach towards intrusion detection". In Proceedings of the 13th National Computer Security Conference.
- Rhodes, B., Mahaffey, J., Cannady, J. (2000). "Multiple Self-Organizing Maps for Intrusion Systems" In Proceedings of the 23rd National Information Systems Security Conference.
- Mäntysalo, J., Torkkola, K., and Kohonen, T. (1992). "LVQ-based speech recognition with high-dimensional context vectors". In Proceedings of the International Conference on Spoken Language Processing, Edmonton, Alberta, Canada.
- Chang, K., and Lu, Y. (1994). "Feedback learning: a hybrid SOFM/LVQ approach for radar target classification". In Proceedings of the International Symposium on Artificial Neural Networks.
- Linde, Y. (1980, January). "An Algorithm For Vector Quantier Design", IEEE Transactions on Communications, vol. 28, No. 1.
- Cannady, J. (2009). "Distributed Detection of Attacks in Mobile Ad Hoc Networks Using Learning Vector Quantization". Proceedings of the 1st International Workshop on Wireless and Mobile Networks Security.
- Voegtlin, T. (2002). "Recursive self-organizing maps". Neural Networks, 15(8-9).
- Choe, Y. and Miikkulainen, R. (1997). "Self organization and segmentation with laterally connected spiking neurons". In Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI-97).
-

1,000 feet

- **Observation:** Current IDS approaches in MANETs use centralized approach

500 feet

- Problems with centralized approaches:
 1. Need to send data to centralized manager limits network bandwidth for other applications
 2. Loss of node hosting IDS results in loss of detection capability

Ground level

- “There is no efficient method of detecting attacks in a mobile ad hoc network”
 - What does “efficient” mean?
- or
- “There is no method of distributing intrusion detection components in mobile ad hoc networks”