Abstract: Wireless networks have seen unprecedented rise in their size and number of users in recent years. This unprecedented rise is attributed to the rise in the number of mobile computing devices. Moreover the amount of data that is handled by these wireless networks has increased in recent years. This increase in the flow of data over these wireless networks is due to increase in popularity of cloud computing, which is built on the concept of Software as a Service, where in all the data processing happens on the cloud. Although there has been an increase in the usage of the Wireless networks, little has been done to improve the security of these wireless networks and they still remain prone to attacks from a malicious user. One such wireless network that is widely used but is still prone to attacks is Wi-Fi. Wi-Fi protocol (IEEE 802.11), over the years has been upgraded many times, but these upgrades have mainly resulted in increase in the overall data rate of the communication. Little has been done to improve the security of the protocol.

As a part of this presentation we present two architectures that use Anomaly Behavior Analysis to detect, classify attacks on the Single access point and Distributed Wi-Fi networks and then track the location of the attacker. The presented system uses the approach of **ngrams** and **wireless_flows**(**WFlows**) to detect attacks on the network. The architectures are able to classify the attacks on the network by associating the number of different types of Wi-Fi frames in the WFlow with the Wi-Fi frames present in the attack types. The presented architectures use different approaches to track the location of the attacker. The first architecture uses an approach of clustering to track the location of the attacker, while the second architecture uses classification rules learnt from machine learning to track the location of the attacker. The attack detection modules of the IDS have no false positives or negatives even when the network has a high frame drop rate. The Clustering approach to track the location of the attacker performs well in static environments with 81% efficiency, while the Rule Classification approach to track the location of the attacker performs well in dynamic environment with 76% efficiency.

Bio: Pratik Sara is a graduate student completing his Master's in the department of Electrical and Computer engineering at the University of Arizona. He completed his bachelor's in Electronics and Tele-Communication studies from the University of Mumbai. His research interests include Computer Networks, Network Security, Wireless Networks, Big Data analysis and Machine learning. Some of the previous projects that he has worked on include Anomaly Behavior Analysis of Wireless Networks and Anomaly Behavior Analysis for the DNS protocol.