

Detecting identity based attacks in wireless networks

Jie Yang
ECE Department
May 6, 2009

Introduction

- Wireless and sensor networks are vulnerable to **identity based attacks**
- Sybil attack: Adversary **forges multiple identities** to trick the network and conduct harmful attacks
- Spoofing attack: Adversary forges its identity to masquerade as another device, e.g. forges MAC address, or creates multiple illegitimate identities
- Serious impact on the network performance
 - Group-based voting techniques
 - Fault-tolerant schemes: redundancy mechanisms, distributed storage
 - Geographic routing protocols

It is important to detect the presence of Sybil attacks in the network!!

Motivation



- Conventional approach – key distribution method and identity-based encryption schemes
 - Requires reliable key distribution, management, and maintenance mechanisms
 - Computational requirement, and infrastructural maintenance on the nodes
 - Susceptible to node compromise
- Our approach
 - Received Signal Strength (RSS), cluster analysis
 - Reuse existing communication infrastructure
 - Not require any overhead on wireless devices

Algorithmic Approaches



- Clustering analysis and threshold methods
 - K-means clustering
 - PAM: Partitioning Around Medoids method
 - Suitable for both static and mobile environments
- Time-series-based correlation analysis
 - Suitable for high dynamic and noisy environment

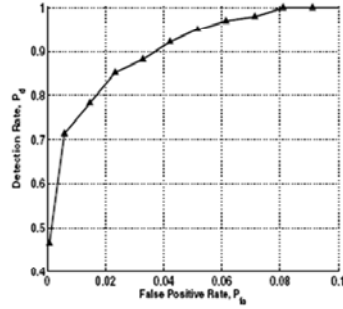
Case Study: Sybil attack in static environment

- WiFi networks
- Real office environments
- Data collection test bed

- Initial Results: Sybil attack
- Detection rate vs. false positive rate



- 802.11 (WIFI) network
- Deployment of 5 landmarks
- 200X170 feet, 101 locations
- 300 RSS samples per location



Detection rate over 95% with less than 5% false positive rate