Using Active Scanning to Identify Wireless NICs

Raheem Beyah
Communications Assurance and Performance Group
Georgia State University

(with Cherita Corbett and John Copeland at Ga. Tech)
Presentation Outline

- Motivation & Background
- Objective
- Opportunities for Distinction
- Approach to NIC Identification
- NIC Identification using Active Scanning
  - Impact on wireless stream
  - Spectral analysis
    - Qualitative evaluation
    - Quantitative evaluation
- Summary
Presentation Outline

- **Motivation & Background**
- Objective
- Opportunities for Distinction
- Approach to NIC Identification
- NIC Identification using Active Scanning
  - Impact on wireless stream
  - Spectral analysis
    - Qualitative evaluation
    - Quantitative evaluation
- Summary
802.11 Security

- WLANs are attractive targets for malicious activity
  - Lack of physical boundaries
  - Use of open-air medium
  - Advertisement of existence so that clients can connect

- IEEE 802.11 standard encompasses security services to maintain confidentiality, integrity, and access control for WLANs

- Wired Equivalent Privacy (WEP)
  - RC4 & CRC-32

- 802.11i – solves the currently known security vulnerabilities of WEP
  - AES, crypto MIC, & dynamic key management
  - Requires new hardware & must be commonly applied to all systems on WLAN
Unauthorized Access

- Prevention only effective on systems that are owned, managed, and controlled
- Rogue client & AP
  - Authorized user installs unauthorized device
  - Attacker uses rogue system to lure victims to gather user credentials
- Flawed legacy equipment – exploit design flaws of WEP
- Stealthy intrusions – phishing evades preventive measures

► Need for detecting unauthorized access to respond and reduce potential damage
Current Solutions

- Intrusion detection systems – monitor WLAN traffic for sequence of events that exhibit anomalous behavior or match the pattern of known attacks
  - False positives, signature updates
  - Effectiveness reduced by novel attacks & stealthy intrusions

- Identification Systems
  - Commercial products – WiMetrics, DeviceID
    - Active approaches that probe client or rely on cooperation of user
  - RF Fingerprinting – Jeyanthi Hall, et al. (CIIT)
    - Difficult to incorporate into existing WLAN infrastructure
    - TCP timestamp options can be set to arbitrary value
Proposed Scheme

- NIC ID based on packet frequency patterns in wireless stream to help control access to WLANs

Advantages

- Passive – only requires the capturing of 802.11 frames
- Software implementation – incorporate into existing WLAN infrastructure
- Operates independent of higher layer protocols
- Operates with encrypted streams
- Detection is independent of attack that lead to unauthorized access
Presentation Outline

- Motivation & Background
- **Objective**
- Opportunities for Distinction
- Approach to NIC Identification
- NIC Identification using Active Scanning
  - Impact on wireless stream
  - Spectral analysis
    - Qualitative evaluation
    - Quantitative evaluation
- Summary
Objective

- Establish the identity of a wireless NIC by analyzing the temporal behavior of a wireless stream

- Implementation of 802.11 standard influences transmission patterns of wireless stream

- Different implementations will have different impact on time-variant properties of wireless stream

- Use signal processing to extract the periodic components of stream for the identity of NIC

- Support the detection of unauthorized systems that use NICs different from legitimate systems
Presentation Outline

- Motivation & Background
- Objective
- Opportunities for Distinction
- Approach to NIC Identification
- NIC Identification using Active Scanning
  - Impact on wireless stream
  - Spectral analysis
    - Qualitative evaluation
    - Quantitative evaluation
- Summary
Opportunities for Distinction

- Functions of 802.11 that facilitate the transmission of data and maintain connectivity
  - **scanning**
  - retransmission
  - transmission rate adaptation
  - association/authentication
  - link reservation
  - encryption
- Implementation of functions varies between vendors
- Affects temporal behavior traffic stream
- Configuration of NIC – tune 802.11 functions
  - fragmentation threshold
  - RTS/CTS threshold
  - transmission power
  - power save mode
  - Different settings will invoke different services of 802.11 at different moments
- Proprietary hardware and software enhancements
  - frame bursting
  - overhead management
  - data compression
  - client-to-client transfer
Opportunity for Distinction

Implementation of active scanning influences traffic patterns of initial portion of wireless stream
Presentation Outline

- Motivation & Background
- Objective
- Opportunities for Distinction
- **Approach to NIC Identification**
  - NIC Identification using Active Scanning
    - Impact on wireless stream
    - Spectral analysis
      - Qualitative evaluation
      - Quantitative evaluation
- Summary
Approach in a Nutshell

- Exploit differences in the implementation of the active scanning mechanism
- Capture traffic generated during active scanning
- Convert traffic capture into a time series of data frame arrivals
- Apply power spectrum density function to analyze periodicity embedded in traffic
- Generate spectral profile from most prevalent periodic components → identity of NIC
- Compare spectral profiles to discern between NICs
Spectral Analysis

- Useful in extracting periodic phenomena from noisy signals
- Shown to work well in network traffic analysis
- Must represent wireless traffic as a signal
  - Describe the frame transmission process as a discrete event $x$ that occurs as a function of time $t$
  - Choice of events: frame type, frame size, transmission rate of frame, etc
  - Uniformly sample the signal
Power Spectrum Density

- Captures power of signal over a range frequencies
- Theoretical description
  - Convert signal $x[n]$ into frequency domain
  - Compute the signal power (spectral density) of the frequency data

\[ X_N(f) = \sum_{n=0}^{N-1} x_N[n]e^{-j2\pi fn/f_s} \]

- Compute the signal power (spectral density) of the frequency data

\[ \hat{P}_{xx}(f) = \frac{|X_N(f)|^2}{f_sN} \]

- Magnitude of power indicates the amount of regularity of the periodicity in the arrival rates of wireless frames at the corresponding frequency
Spectral Profile

- Systematic way to numerically compare spectral content
- Use subset of values from PSD to capture the trend in frequency distribution of the spectra
- Generate spectral profile using $N$ frequency points that exhibit the greatest amount of power

$$F = \{f_1, f_2, f_3, \ldots, f_N\}$$
Presentation Outline

- Motivation & Background
- Objective
- Opportunities for Distinction
- Approach to NIC Identification
- NIC Identification using Active Scanning
  - Impact on wireless stream
  - Spectral analysis
    - Qualitative evaluation
    - Quantitative evaluation
- Summary
NIC Identification Using Active Scanning

- Broadcast probe request frames to discover networks to join
- Automatically engaged upon powering on NIC
- 802.11 standard procedure:
  - Wait until $ProbeDelay$ time has expired.
  - Send a probe request with broadcast destination, SSID and broadcast BSSID.
  - Start a $ProbeTimer$.
  - If medium idle when $ProbeTimer$ reaches $MinChannelTime$, scan the next channel; else, when $ProbeTime$ reaches $MaxChannelTime$, process all received probe responses and scan next channel.
NIC Identification Using Active Scanning

- Parameters that can vary per vendor
  - values for *ProbeDelay*, *MinChannelTime*, *MaxChannelTime*
  - number of probe request frames to transmit per channel
  - delay between probe request frames on the same channel
  - channel probe frequency
  - order of channels to probe

- Setting of these parameters define the behavior of the wireless stream
Scanning: Experimental Setup

- **Client**
  - 6 NICs: 2 Lucent/Orinoco Gold, 2 Linksys WPC11, 1 DLink DWL-650, 1 Cisco 350
  - Software drivers: orinoco_cs, prism2_cs, airo_cs
  - Insert NIC and allowed to scan for 4 minutes
  - Used perl script to repeat process 100 times for each card

- **Data collection**
  - Sniffed 5 (sometimes 6) channels simultaneously
  - Tools: tcpdump, iwconfig, wlanctl-ng
  - 3300 traffic capture files
Presentation Outline

- Motivation & Background
- Objective
- Opportunities for Distinction
- Approach to NIC Identification
- NIC Identification using Active Scanning
  - Impact on wireless stream
  - Spectral analysis
    - Qualitative evaluation
    - Quantitative evaluation
- Summary
Scanning: Spectral Analysis

- Configuration of Welch Method
  - sampling interval: 0.002 seconds
  - nfft: 1024
  - segment size: 64
  - overlap: 50%
Scanning mechanism exhibits periodicity – distinguishable peaks at certain frequencies

PSD is stable – trials repeated on the same channel have similar peaks
Scanning: Quantitative Evaluation

- Selected $N=50$ to generate the spectral profile
  \[ F = \{f_1,f_2,f_3, \ldots f_{50}\} \]
- Generated spectral profile for each trial
Trials on same channel have similar spectral content indicated by horizontal line

Channel 4: 90%+ match for each NIC
**Scanning: Spectral Profile (Channel 4)**

- **Cisco**
  - 49-59Hz → 0.0169-0.0204 s
  - 125-129Hz → 0.0078-0.008 s
  - 180-190Hz → 0.0053-0.0056 s

- **DLink/Linksys1/Linksys2**
  - 55-65Hz → 0.0154 to 0.0182 s

- **Lucent1/ Lucent2**
  - 126-149Hz → 0.0076 to 0.0079 s
  - 210-225Hz → 0.0044 to 0.0048 s
Presentation Outline

- Motivation & Background
- Objective
- Opportunities for Distinction
- Approach to NIC Identification
- NIC Identification using Active Scanning
  - Impact on wireless stream
  - Spectral analysis
    - Qualitative evaluation
    - Quantitative evaluation
- Summary
Scanning: Summary

- Scanning algorithms tend to favor some channels over others
- Lucent and Cisco cards were more aggressive
- Of the channels we examined, channel 4 was best channel for profiling
- Discerned between Cisco, Lucent and Linksys/Dlink
- Linksys and Dlink had identical spectral profiles likely because they used same driver software → scanning implemented in driver

- Scanning is a periodic process and a viable attribute for discerning between NICs
Questions

Georgia State Communications Assurance and Performance Group

www.cs.gsu.edu/cap

Georgia Tech Communications Systems Center

www.csc.gatech.edu

rbeyah@cs.gsu.edu