Relationship-based Detection of Spoofing and Anomalous Traffic in Wireless Networks

Qing Li
Wade Trappe
Talk Overview

- Motivation: The problem of spoofing
- Attacks that are facilitated by spoofing
  - Packet Injection
  - Association Request Flooding
  - Evil Twin AP
- Non-cryptographic solution: Relationship-based detection
- Individual strategies:
  1. Sequence number monotonicity
  2. One-way temporary identifier fields (not presented)
  3. Signal strength consistency and discrimination
  4. Traffic statistics consistency and discrimination
- Conclusions and Future Work
Motivation: Problem with Spoofing

- Many wireless networks are susceptible to spoofing attacks…
- A spoofing attack involves one network device assuming the identity of another network entity
- Is spoofing easy?
  - Unfortunately, yes!
  - Commodity wireless devices means that wireless devices are easy to acquire and program… for the good guys and for the bad guys!
  - In 802.11 networks, it is easy to assume the MAC address of another device through the `ifconfig` command
  - Sensor networks are no better!
Problem with Spoofing (2)

- Spoofing is easy. So what?
- Spoofing facilitates a broad variety of other security threats that can be launched against wireless networks:
  - Denial of service attacks
  - Session hijacking
  - Attacks on access control lists
  - Evil twin AP
- Let us look at several of these attacks.
DoS Attack: Packet injection attack

- The Attack is a form of session hijacking:
  - Attacker armed with a laptop having 2 wireless cards.
  - One card monitors all TCP traffic on the AP channel
  - Second card sends back TCP replies to select TCP requests (e.g. all requests for a particular web page). These are sent as if appearing from the server the user was connecting to.
  - At the MAC layer the attacker spoofs AP by injecting custom 802.11x frames with AP’s source MAC address.

- Result: The user session is hijacked, and service can be DoSed.
DoS Attack: Evil Twin AP

The Attack:
- An adversary installs a rogue AP near a regular AP.
- This rogue AP may use the same SSID as the regular AP. It may or may not use the same MAC address as the regular AP. Rogue AP transmits with a stronger signal power.

Result:
- Clients automatically associate with rogue AP due to higher signal strength.
- The rogue AP may drop all traffic from the clients that connect to it.

Defenses:
- Perform network authentication. Requires the establishment of a known, shared key!!!
- For open networks, always try both AP’s and see which one provides service. Once a good AP is found, use signal strength as a consistency check.
Defense: Anomaly Detection
Relationship-based Detection

- The basic scenario:
  - Suppose we have two devices A and B claiming the same identity
  - Let X be a separate monitoring device

- There should be “relationships” present within the stream of packets coming from this identity

- These relationships and the rules by which they are verified should be difficult for an adversary to forge

- There are two types of relationships:
  - Relationships introduced into packets through auxiliary fields
  - Relationships associated with inherent properties of packet transmission/reception

Normal Case: Only one device using an identity, then X will see packets following a particular pattern

Anomalous case: Two or more devices using the identity, then X will see a mix of different packets
Strategy 1: Sequence Number Monotonicity

- Wireless NICs typically have MAC-layer packet sequencing in firmware.
- In 802.11 Sequence Numbers increase monotonically.
- During a spoofing attack, the observed sequence numbers for a particular MAC address will not behave monotonically.
- OK, but can’t I change the sequence numbers?
  - Yes, use Software MACs
  - Won’t help you that much!
  - A sends #101, #102…
  - B can now send #103…
  - But A will eventually send #103
  - Assume Retransmission Disabled
Sequence Number Anomaly Detector

- Can we turn these observations into a fast MAC-layer detection mechanism? Yes.
- Suppose \( s(n) \) and \( s(n+1) \) are two consecutive observed sequence numbers
- Basic rule:
  - \( s(n+1) - s(n) = 1 \mod 4096 \) is an automatic test:
    - if we see \( s(n+1) - s(n) > 1 \mod 4096 \) or \( s(n+1) = s(n) \) then declare anomaly!
- More generally, there is packetloss and we want the rule to be robust lost packets
  - \( s(n+1) \) should not be too much bigger than \( s(n) \)
    - If \( s(n+1) - s(n) > K \mod 4096 \) then declare anomaly
    - This allows for up to \( K-1 \) lost packets
- We may determine thresholds based on target Probability of False Alarm and Probability of Missed Detection according to packetloss rate \( p \).
- We have conducted experiments on ORBIT to validate the feasibility of this method for detecting anomalous traffic.
Strategy 3: Signal Strength Discrimination

- Signal strength can be used as a discriminator to identify the presence of two or more sources using the same MAC address.

- Idea: (Requires Stationary Sources)
  - A talks to X or B talks to X then there is a particular distribution.
  - When A and B talk to X (alternating) then we see two types of distributions
    - Bimodal: The two distributions are “added” together
    - Unimodal: Automatic gain control performs smoothing between readings
  - Key point: Neither distribution looks like the original distribution!
Suppose the monitor X has a distribution for the signal strength readings from A.

Later, we may test observed signal strength readings against this distribution.

Assuming devices have not changed their configuration

Suppose our initial distribution is \( f_A(r) \), and we have broken the dynamic range into \( k \) histogram bins \( p_j \).

Later, we conduct \( n \) RSSI readings.

If we observe \( N_j \) RSSI readings in bin \( j \), then the Chi-Squared Test Statistic is

\[
\chi^2 = \sum_{j=1}^{k} \frac{(N_j - np_j)^2}{np_j}
\]

If the test statistic is greater than a threshold, we declare that the new, observed distribution is not a good fit for the original distribution.
Signal Strength: ORBIT Validation

- We conducted experiments on ORBIT to validate the proposed idea.
- Nodes A (2,1) and B (4,5) send packets at 100mW to monitor X (5,4)
- Spoofing case (denoted E): Alternate between A and B

\[
\chi^2(E,A_X) = 42622
\]
\[
\chi^2(E,B_X) = 41278
\]

- For this experiment, the 1\% Chi-Squared Test Threshold is 9.21
Signal Strength: ORBIT Validation (2)

- What if A and B are at the same distance from X?
- Nodes A (4,3) and B (4,5) send packets at 100mW to monitor X (5,4)
- Spoofing case (denoted E): Alternate between A and B

$$\chi^2(E,AX) = 7121$$
$$\chi^2(E,BX) = 21481$$

- The 1% Chi-Squared Test Threshold is 9.21
Strategy 4: Traffic Statistics Discrimination

- In this strategy, we assume that all devices must follow a specified traffic pattern.
- For example, the network policy might be that all wireless devices transmit at a constant bit rate (CBR) source with a fixed interarrival time.

Idea:
- When A talks to X there is a particular observed inter-arrival distribution at X.
- When A and B talk to X then the extra source adds extra traffic claiming to come from this network identity.
- The interarrival statistics will change significantly.
We conducted experiments on ORBIT to validate the proposed idea.

Nodes A (3,2) and B (4,5) send packets to monitor X (5,4)

A is a 200msec CBR source

Two spoofing cases:
- Case E1: B is a 200msec source
- Case E2: B is a 50msec source

\[ \chi^2(E1) = 941348 \]
\[ \chi^2(E2) = 2297731 \]

The 1% Chi-Squared Test Threshold is 9.21

The large values suggest this test is very powerful, at the expense of restricting traffic behavior
Conclusions and Future Work

- The relationships between packets coming from a network identity allow for the detection of more than one device using a network identity (spoofing).

- We presented 3 relationships:
  - Monotonicity of Sequence Numbers; Signal Strength Statistics; Traffic Statistics
  - These relationships do not require cryptographic tools, nor do they require the establishment/maintenance of cryptographic material.

- A few caveats:
  - Relationships do not replace authentication!
  - They do not catch cases where only the adversary uses a network identity… That is, they detect multiple sources not identity fraud!
  - The tools presented are only meant as a means to warn of possible anomalous network behavior! Its good to be conservative when sending warnings…
  - There are restrictions for the signal strength (stationarity) and for traffic statistics (QoS limitations).

- This is ongoing work
  - Integrate these methods into MAC-layer detection
  - We are quantifying the probability of missed detection and false alarm for these detectors
  - Looking into the issue of devices moving or changing configuration.