Attacker Traceback and Countermeasure with Cross-layer Monitoring in Wireless Multi-hop Networks

Yongjin Kim
Electrical Engineering Dept.- Systems
University of Southern California
Email: yongjkim@usc.edu
Introduction

- Wireless multi-hop networks are especially vulnerable to DoS/DDoS attack due to its limited resource (bandwidth, host resources)

- DoS/DDoS attack can be classified into
  - Software exploitation
  - Flooding-type attack

- Attacker traceback is an essential security component for DoS/DDoS attacks
  - To take a proper countermeasure near attack origin
  - For forensics
  - To discourage attacker in advance

- Wireless multi-hop networks have different characteristics from the Internet, which makes it difficult to directly apply existing attacker traceback schemes to wireless multi-hop networks
  - No infrastructure
  - Dynamic topology (Node mobility, power outage, etc.)
  - Limited network/host resources
On Attacker Traceback

Goal of attacker traceback:
- Identify sequence (time & space) of intermediate nodes carrying the attack traffic
- Identify the neighborhood of attacker(s)
- Identify the attack machine(s)

To accomplish the mission

• State diagram for IP traceback
  - Abnormality detection
  - Abnormality characterization
  - Abnormality searching
  - Abnormality matching
  - Attacker identification & countermeasure
Requirements Analysis in Wireless Multi-hop Networks

Traceback protocol building blocks

(I) Information searching & gathering
- Robustness against node compromise
- Robustness against route instability
- Low bandwidth requirement
- Low energy consumption

(II) Information storage
- Low Storage requirement of intermediate node
- Low Storage requirement of victim node

(III) Information analysis
- Low computational overhead of intermediate node
- Low computational overhead of victim node
Existing Scheme: (1) Link test

**Advantages:**
1. No memory overhead
2. Low computational load

**Disadvantages:**
1. Another form of DoS
2. Traceback needs to be done during attack period
3. Weakness in DDoS attack

Existing Scheme: (2) Logging-based Traceback

Advantages:
1. Can trace back with single packet
2. Applicable to both DoS and DDoS attack
3. Low bandwidth requirement

Disadvantages:
1. Large storage requirement
2. High processing load

Overall Picture of Our Proposal

We try to solve the following problems.

- How do we characterize attack signature efficiently under address spoofing?
- How do we find the attack path efficiently (vs. flooding or ERS) in large-scale networks?
- Use protocol layer (network, MAC, Cross-layer) abnormality for attack signature characterization.
- Propose (multi-) directional searching and (multi-) directional expanding search, which is based on small-world model

Challenges:
- Under DDoS attack, low level of abnormality is observed near distributed attack origins
- High background traffic lower traffic level or regional abnormality
Problem Definition

(1) **High background traffic** can negatively affect the accuracy of abnormality characterization and matching.

(2) **In DDoS attack**, low abnormality is observed near attack origin.

Can be effectively handled by cross-layer monitoring.
Overall Traceback Framework

Abnormality detection
- Monitoring window
- Normal Profile Calculation
- Threshold
- Cross-layer Monitoring

Abnormality Characterization
- Unit signature window
- Total Signature window
- Total vs. residual
- Cross-layer Monitoring

Abnormality Matching
- Correlation coefficient (Traffic pattern)
- Least-square method (Traffic volume)
- K-S Fitness test (sample distribution)

Abnormality Searching
- Flooding
- Expanding ring search
- Directional search
- Multi-Directional search

Countermeasure
- Packet filtering
- Rate-limiting
- Confidence index-based
- Cross-layer Monitoring
Cross-layer Monitoring

- Both forward and backward noise can be drastically reduced with hybrid monitoring.
- Cross-layer monitoring is necessary for efficient abnormality detection, characterization, matching, and countermeasure.
Definition of Signature Energy for Efficient Searching

How do we incorporate all the MAC abnormality information? i.e.,
- Number of abnormality observers
- Abnormality matching level
- Closer contact

We define attack signature energy

- Attack signature energy is classified as,
  - Individual attack signature energy (atomic unit)
  - Local attack signature energy (to detect attack path region)
  - Global attack signature energy (for analysis purpose)
Individually, we define the attack signature energy observed by node $i$, as:

$$E_i(t) = \frac{1}{D_i(t)}$$

where $D_i(t)$ is the distance between attack signature and candidate attack signature in K-S fitness test.

Local attack signature energy (for protocol/searching purpose):

$$LE(t) = \frac{E_{1/2}^u(t)}{\mu_{1/2}}$$

Where; $\alpha = \frac{n}{N} > \delta$

$$X_{1/2} \equiv Y_{(N+1)/2}$$

$$\equiv \frac{1}{2}(Y_{N/2} + Y_{1+N/2})$$

Global attack signature energy (for analysis purpose) is defined as follows:

$$GE(t) = \sum_{i=1}^{n} E_i(t)$$

Where, $E_i(t) = \frac{1}{D_i(t)}$

We use median instead of average to provide robustness against node compromise.
Searching Description

- Local region that shows high signature energy is recursively selected
- In DDoS attacker traceback, combinational test is done
Traceback-Assisted Countermeasure

- After finding closest (one-hop neighbor) nodes to the attacker, countermeasures needs to be taken

- Packet filtering
  - Attack packets are filtered out and dropped at the ingress point
  - How to distinguish between the good packets and bad packets exactly?

- Rate-limiting
  - Allows a relay node to control the transmission rate of specific traffic flows
  - Rate-limiting mechanisms are deployed when the attack detection has a high false positives or cannot precisely characterize
  - How much rate we need to limit? – NOT well defined so far

We propose hybrid – between packet filtering and rate-limiting countermeasure based on abnormality matching level. Abnormality matching level is quantified by Confidence Index (CI)
Confidence Index (CI)-based Hybrid Countermeasure

- We define attack CI level
  1. CI with TPM/TVM = \( r(A, B) \cdot \alpha \)
  2. CI with K-S = \( \frac{1}{D_n} \)

- Based on the CI, rate-limiting level (P) is determined as follows
  \[ P = \text{MaxP} \cdot \frac{CI - \text{MinCIThresh}}{\text{MaxCIThresh} - \text{MinCIThresh}} \]

- The scheme reduces to packet filtering, when CI > MaxCIThresh

- Important parameters:
  1. MinCIThresh, MaxCIThresh, MaxP
  2. Attack mitigation level
  3. Negative impact on legitimate traffic
Traceback Success Rate Comparison

- DDoS attacker Traceback success rate comparison (50% background nodes, 6 attackers)

*6 average number of one-hop neighbors

Cross-layer monitoring-based traceback shows higher performance increase
Countermeasure

- Gain (Dropped attack packet) surpass disadvantage (Lost legitimate packet)
- LPP is the Product of Lost attack packet count and Passed legitimate packet count
- By using CI-based scheme and coarse-grained information, LPP is drastically increased
Conclusions

- We proposed a complete set of attacker traceback framework. (i.e., Abnormality detection, characterization, matching, searching, countermeasure)
- Using Cross-layer Monitoring we can achieve the following merits
  - Robust against high background traffic
  - Robust against DDoS attack
- Use of attack signature energy has the following advantage
  - Robust against node compromise (Majority-voting using MAC layer abnormality overhearing nodes)
- Use of CI-based countermeasure has the following advantage
  - Reduced negative impact on legitimate traffic
  - Increase attack packet dropping efficiency