Detecting service violation in Internet and mobile ad hoc networks

Bharat Bhargava
CERIAS security center and Department of computer sciences
Purdue University
bb@cs.purdue.edu
www.cs.purdue.edu/people/bb
Joint work with A. Habib, Y. Lu, X. Wu, and W. Wang
Problem Statement

• Detecting service violation in networks is the procedure of identifying the misbehaviors of users or operations that do not adhere to network protocols.
Contributions

- Infer internal behaviors based on SLA parameters
- Advance probing technology
- Advance Intrusion Detection, QoS and DiffServ, intruder identification, and Fault-tolerant authentication
- Integrate cellular networks with ad hoc networks to
  - Enable cellular providers to add services
  - Ad hoc networks get central trusted authority
- Enable the deployment of security sensitive applications
Example of service violation

• In Internet:
  – DoS attacks, exploit known vulnerabilities that make victim un-operable, flood network
  – Attacks/ Service Violations in QoS domains

  • Impersonate a legitimate customer by spoofing flow identity
  • Mark Packets to a higher class of services
  • Bypassing the ingress routers and using best effort traffic.
Example of service violation

• In cellular networks:
  – Cellular user impersonation
  – Control channel spoofing and jamming

• In mobile ad hoc networks
  – Node misbehaviors (selfish, malicious, malfunctioning, compromised node, Byzantine behavior)
  – Passive attacks (eavesdropping)
  – Node impersonation and gang attack
  – DoS and link layer flood
  – Energy depletion attacks
Content

- Research motivation
- Classification of attacks and detection mechanisms
- Network topology
- Examples
  - Detecting service violation by distributed monitoring [NSF ITR-ANIR, IBM]
  - Intruder identification in mobile ad hoc networks [CISCO]
  - Fault tolerant Authentication in movable base station [NSF CCR]
  - Cellular assisted mobile ad hoc networks (in progress) [Motorola]
- Conclusion
Research Motivation

• The hybrid of Internet, cellular system and mobile ad hoc networks introduce more vulnerabilities. [S. Bush, GE Research ’99]

• The popularity of mobile system puts difficult requirements for security [Hubaux et al, MobiCom ’01]

• The release of National Strategy to Secure Cyberspace [Pres G. W. Bush, ’02 ]
Research Motivation

- Vulnerabilities allows attacks to cause threat to assets
- Adapt to type, duration, extent, and severity of attack
- Need to reduce threat and risk
- Observe, analyze, alert, avoid, and tolerate attacks and deal with threat
Monitoring network activities to deal with

- **Outside attacks...**
  - 13,000 DoS attacks recorded in 3 weeks!!
  - Some attacks last for hours!! [*Moore et al., Usenix ’01]*
  - Can network monitoring alert for possible DoS attacks in early stages

- **QoS-enabled networks have inside attacks like Stealing bandwidth by**
  - Marking packets with higher priority classes
  - Spoofing flow ID
Fundamental Notions

- Vulnerabilities and threats
- Adaptability
- Trust
- Fault-tolerance and security
- Observe misbehavior flows through service level agreement (SLA) violation detection at the
  - Core routers
  - Edge routers
  - Link layer
Ideas from Distributed Systems

- Distance vector
- Sequence number
- Replication
- Atomicity
- Election protocols
Measures

- Efficiency: communication and processing overheads
- Accuracy
- Effectiveness
- Robustness
Defeating DoS attacks in Internet

DoS Attacks

Detection

Traceback

Packet Marking

Deterministic

SPIE

Probabilistic

ICMP

Ingress/Egress Filtering

Core based

Edge based

Prevention

Route-based Filtering

Monitoring

Stripe

Distributed
Attacks on routing in mobile ad hoc networks

- Active attacks
  - Routing procedure
    - False reply
    - Wormhole attacks
  - Flood network
    - Route request
    - Route broken message
- Passive attacks
  - Packet silent discard
  - Routing information hiding
Attacks on Cellular system

Security in 3G cellular network

Access security
- Mutual Authentication
- Cryptography for authentication
- Temporary identities
- UTRAN encryption
- Integration protection for RRC signaling

Network and system security
- Application layer
  - S-MINE
  - PGP
  - SET
  - SSL
  - SOCKS
  - RADIUS
- Session Layer
- Network layer
  - IPSecurity
A1 spoofs H5’s address to attack V

A3 uses reflector H3 to attack V

Victim, V
Topology Used (Cellular assisted system)

- Mobile ad hoc user (MT)
- Mobile cellular user
- Cellular channel for ad hoc control
- Cellular channel for cellular traffic
- Ad hoc channel

Base station (BS) → Cellular Backbone → CAMA agent

Cellular Backbone

Cell → Ad hoc network → Cell
Example: Detecting service violation in Internet by distributed monitoring

• Idea:
  – Excessive traffic changes internal characteristics inside a domain (high delay & loss, low throughput)
  – Monitor network domain for unusual patterns
  – If traffic is aggregating towards a domain (same IP prefix), probably an attack is coming

• Measure delay, link loss, and throughput achieved by user inside a network domain

• Study and analysis of detecting/preventing attacks [Habib et al., Network and Distributed System Security Symposium (NDSS) ’03]
Core-assisted loss measurements

• Core reports to the monitor whenever packet drop exceeds a local threshold
• Monitor computes the total drop for time interval $t$
• if the total drop exceeds a global threshold
  a. The monitor sends a query to all edge routers requesting their current rates
  b. The monitor computes total incoming rate from all edge
  c. The monitor computes the loss ratio as the ratio of and the total incoming rate
  d. If the loss ratio exceeds the SLA loss ratio, a possible SLA violation is reported
Edge-to-Edge (E2E) Approaches

• Stripe-based
  – Back-to-back packets experience similar congestion in a queue with a high probability
  – Receiver observes the incoming pattern
  – Infer internal characteristics using topology

• Distributed (Overlay-based)
  – Edge routers form an overlay network for probing
  – Each edge router probes part of the network
  – Topology and probing reveal internal characteristics
Inferring Loss

• Calculate how many packets are received by the two receivers. Transmission probability $A_k$

$$A_k = \frac{Z_{R1} Z_{R2}}{Z_{R1 \cup R2}}$$

where $Z_i$ binary variable which takes 1 when all packets reached their destination and 0 otherwise.

• Loss is $1 - A_k$

• For general tree, send stripe from root to every order-pair of leaves.
Stripe-based Monitoring [Habib et al., Journal of Computer Communications '03]

- The research correlates Edge to Edge measurements with internal behaviors. Send stripes from each edge router to every pair of edge routers.
- Can deal with different attacks such as
  - QoS agreement violation, DoS attacks, Bandwidth theft
- Monitor the network for link delay
- If \( \text{delay}_i > \text{SLA}_{\text{delay}}^i \) for path \( i \), then probe the network for loss
- If \( \text{loss}_i > \text{SLA}_{\text{loss}}^i \) for any link \( i \), then probe the network for throughput
- If \( \text{BW}_i > \text{SLA}_{\text{BW}}^i \), then flow \( i \) is violating SLA by taking excess resources
Probing Strategy

- Each ingress router copies the header of user packets with probability to probe the network for delays.

- The egress computes the edge-to-edge delay. If the delay exceeds a certain threshold, it reports delay along with the identity of both the ingress and egress routers to the monitor.

- The monitor maintains the set of edge routers $E'$ to send stripes, in order to infer loss on active links.

- Monitor probes the network for throughput approximation only when the inferred loss is higher than the pre-configured threshold.

- Using delay, loss, and throughput approximations, the monitor can detect violations or bandwidth theft attacks.
Overlay-based monitoring

- E2E approach, i.e., infer internal characteristics from edge to edge measurements
- The probes are tunneled through the overlay network formed by the edge routers.
- Do not need individual link loss to identify all congested links
- Delay and throughput measurements are same as Stripe-based method
- Provide Simple and Advanced methods to identify congested links
Overlay-based Probing

• Each peer probes both of its neighbors
• Detect congested link in both directions
• Not all congested links can be correctly labeled
False Positive (theoretical analysis)

- The simple method does not correctly label all links
- The unsolved “good” links are considered bad
  hence false positive happens
- Need to refine the solution → Advanced Method
• Example:
  if 100 links in the network and 20 of them are congested and 80 are “good”. The basic probing method can identify 15 congestion links and 70 good links. The other 15 are labeled as “unknown”. If all unknown links are treated as congested, 10 good link will be falsely labeled as congested. When the false positive is too high, the available paths that can be chosen by the routers are restricted, thus network performance is impacted.
Performance of advanced method (theoretic analysis)

Advanced method uses output of simple method and topology to find a probe that can be used to identify status of an unsolved link in simple method.
Dealing with service violations

- Identify misbehaving flows
- Identify ingress routers through which flows are entering into the domain
- Activate ingress filters at those ingress routers
- If it is not an attack, ignore it
Experiment: Delay measurements

Attack changes delay pattern in a network domain. The graph shows idle link delay, delay when no attack, and delay under attack.
Experiments: Loss measurements

Core-assisted measurement is more precise than stripe-based, however, it has high overhead.
Identified Congested Links (Overlay-based probing)

(a) Counter clockwise probing

(b) Clockwise probing

Probe46 in graph (a) and Probe76 in graph (b) observe high losses, which means link C4 → E6 is congested. Probes are among edge routers in the topology.
Probing DiffServ using Red, Yellow, and Green Drop precedence in Stripe-based Monitoring
Loss pattern during attack (Generic)

Attack changes loss pattern in a network domain
We need to know the loss pattern when there is not attack
Bandwidth approximation of some flows.
Overhead comparison (theoretic analysis)

- Core has relative low processing overhead
- Distributed scheme has an edge over other two schemes
Comparative Evaluation

![Graph showing comparative evaluation of communication overheads, accuracy, convergence time, and implementation overheads for different scenarios.](http://www.cerias.purdue.edu)
Monitoring evaluation observing

• Accuracy
  – Flash crowd and popular sites might give false positive

• Effectiveness
  – Delay, link loss, and throughput can effectively identify misbehaving flows

• Robustness (Future work)
  – If monitoring agents are not compromised, the scheme works well
Summary for Internet Research

- Monitoring can detect attack in early stage. Filter can be used to stop the attacks.
- Overlay-based monitoring requires only $O(n)$ probing with a very high probability, where $n$ is the number of edge routers.
- Overlay-based monitoring can be used to monitor large scale overlay network.
- Stripe-based inference is useful to annotate a topology tree with loss, delay, and bandwidth. Can be used in monitoring, high quality streaming.
Example: Intruder identification in mobile ad hoc networks

• Goals:
  • locate the source of attacks
  • safely combine the information from multiple hosts and enable individual host to make independent decision
  • achieve consistency among the conclusions of a group of hosts
Architecture
Approach: Reverse Labeling Restriction

- Detecting False Destination Sequence Attacks
- Establishing false route trees through reverse labeling
- Establishing new routes by invalid packets
- Marking suspicious hosts and attackers
- Achieving consistent conclusions by quorum voting
Detecting false destination sequence attack

(1). S broadcasts a request that carries the old sequence + 1 = 21

RREQ(D, 21)

S

S1

S2

S3

D

M

S4

Propagation of RREQ

(2) D receives the RREQ. Local sequence is 5, but the sequence in RREQ is 21. D detects the false destination sequence attack.
Constructing false routing trees

RLR creates suspicion trees. If a host is the root of a quorum of suspicion trees, it is labeled as the attacker.
Establish routes to the destination host

- When the destination host sends out INVALID packet with digital signature, every host receiving this packet can update its route to the destination host through the path it gets the INVALID packet.
• Update Blacklist by INVALID Packet
  • Next hop on the invalid route will be put into local blacklist, a timer starts, a counter ++
  • Labeling process will be done in the reverse direction of route
  • When timer expires, the suspicious host will be released from the blacklist and routing information from it will be accepted
  • If counter > threshold, the suspicious host will be permanently put into blacklist
• Update blacklist by quorum voting
  • Attach local blacklist to INVALID packet with digital signature to prevent impersonation
  • Every host will count the hosts involved in different routes that say a specific host is suspicious. If the number > threshold, it will be permanently added into local blacklist and identified as an attacker.
  • Threshold can be dynamically changed or can be different on various hosts
Evaluation parameters

• Accuracy
  • False coverage: Number of normal hosts that are incorrectly marked as suspected.
  • False exclusion: Number of malicious hosts that are not identified as such.

• Overhead
  • Overhead measures the increases in control packets and computation costs for identifying the attackers (e.g. verifying signed packets, updating blacklists).
  • Workload of identifying the malicious hosts in multiple rounds
Evaluation parameters

• Effectiveness
  - Effectiveness: Increase in the performance of ad hoc networks after the malicious hosts are identified and isolated. Metrics include the increase of the packet delivery ratio, the decrease of average delay, or the decrease of normalized protocol overhead (control packets/delivered packets).

• Robustness
  - Robustness of the algorithm: Its ability to resist different kinds of attacks.
Experiment results

X-axis is host pause time, which specifies the mobility pattern. Y-axis is delivery ratio. 25 connections and 50 connections are considered. RLR brings a 30% increase in delivery ratio. 100% delivery is difficult to achieve due to network partition, route discovery delay and buffer.
X-axis is number of attackers. Y-axis is delivery ratio. 25 connections and 50 connections are considered. RLR brings a 20% to 30% increase in delivery ratio.
<table>
<thead>
<tr>
<th>Host Pause time (sec)</th>
<th>30 hosts, 25 connections</th>
<th>30 hosts, 50 connections</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># of normal hosts identify the attacker</td>
<td># of normal hosts marked as malicious</td>
</tr>
<tr>
<td>0</td>
<td>24</td>
<td>0.22</td>
</tr>
<tr>
<td>10</td>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>24</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>28</td>
<td>0</td>
</tr>
<tr>
<td>40</td>
<td>24</td>
<td>0</td>
</tr>
<tr>
<td>50</td>
<td>24</td>
<td>0.07</td>
</tr>
<tr>
<td>60</td>
<td>24</td>
<td>0.07</td>
</tr>
</tbody>
</table>

The accuracy of RLR when there is only one attacker in the system
<table>
<thead>
<tr>
<th># of attackers</th>
<th>30 hosts, 25 connections</th>
<th>30 hosts, 50 connections</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># of normal hosts identify all attackers</td>
<td># of normal hosts marked as malicious</td>
</tr>
<tr>
<td>1</td>
<td>28</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>28</td>
<td>0.65</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>21</td>
<td>0.62</td>
</tr>
<tr>
<td>5</td>
<td>15</td>
<td>0.67</td>
</tr>
</tbody>
</table>

The accuracy of RLR when there are multiple attackers
X-axis is host pause time, which specifies the mobility pattern. Y-axis is normalized overhead (# of control packet / # of delivered data packet). 25 connections and 50 connections are considered. RLR increases the overhead slightly.
X-axis is host pause time, which specifies the mobility pattern. Y-axis is the number of signed packets processed by every host. 25 connections and 50 connections are considered. RLR does not severely increase the computation overhead to mobile host.
X-axis is number of attackers. Y-axis is number of signed packets processed by every host. 25 connections and 50 connections are considered. RLR does not severely increase the computation overhead of mobile host.
Summary for ad hoc research

- Establish quantitative criteria to evaluate intruder identification algorithms
- Present a distributed approach to defend false destination sequence attacks and locate the attackers
- The mechanism is robust to independent attackers
- The threshold value determines its robustness to gang attacks
Example: Fault tolerant authentication in movable base station system

Mobile Computing Environment are:

- Vulnerable to failures, intrusion, and eavesdropping.
- Adhoc mobile systems has everything moving (hosts, base-stations, routers/agents, subnets, intranet).
- Need survivability from intentional and unintentional attacks.
Research Ideas

• Integrate ideas from Science and Engineering of security and fault-tolerance.

Examples:
• Need to provide access to information during failures
  ↔ need to disallow access for unauthorized users.
  – Duplicate routers & functions, duplicate authentication functions, duplicate secret session key database, secure database that provides public keys.
  – Auditing, logging, check-pointing, monitoring, intrusion detection, denial of service.

• Adaptability:
  – Adapt to timing, duration, severity, type of attack.

• Election Protocols – selection of back-up base station.
Objective

- To provide uninterrupted secure service to the mobile hosts when base station moves or fails.

Research focus

- Fault-tolerant Authentication
- Group Key Management
- Adaptable, Re-configurable Software
- Experiments
Fundamental Security Services

• Authentication
  – Provides assurance of a host’s identity.
  – Provides a means to counter masquerade and replay attacks.
  – Can be applied to several aspects of multicast (ex: registration process).
Problem Description

• To ensure security and theft of resources (like bandwidth), all the packets originating inside the network should be authenticated.

• Typically, a Mobile Host sends a packet to its Home Agent along with the authentication information.
Problem Description (continued)

- If the Authentication is successful, Home Agent forwards the packet. Otherwise, packet is dropped.

Diagram:
- Mobile cellular user
- Authentication and Forwarding Services
- Home Agent
- Internet
Proxy-Based Solution

Source cell

BS1

Arbitrary Network

Foreign Network

Destination cell

Arbitrary Network

BS
Proposed Schemes

- We propose two schemes to solve the problem.
  - Virtual Home Agent
  - Hierarchical Authentication
- They differ in the architecture and the responsibilities that the Mobile Hosts and Base Stations (Agents) hold.
Virtual Home Agent Scheme

VHA ID = IP ADDRESS
Master Home Agent (MHA)

Database Server

Shared Secrets Database

Backup Home Agents

Other hosts in the network
Advantages of the Proposed Scheme

• Has only 3 states and hence the overhead of state maintenance is negligible.
• Very few tasks need to be performed in each state (outlined in the tech report).
• Flexible – there could be multiple VHAs in the same LAN and a MHA could be a BHA for another VHA, a BHA could be a BHA for more than one VHA at the same time.  [Bhargava et al, International Conference on Internet Computing, 00]
Disadvantages of Virtual HA Solution

• Not scalable if every packet has to be authenticated
  – Ex: huge audio or video data
• BHA (Backup Home Agents) are idle most of the time (they just listen to MHA’s advertisements.
• Central Database is still a single point of failure.
Hierarchical Authentication Scheme

- Multiple Home Agents in a LAN are organized in a hierarchy (like a tree data structure).
- A Mobile Host shares a key with each of the Agents above it in the tree (Multiple Keys).
- At any time, highest priority key is used for sending packets or obtaining any other kind of service.
Hierarchical Authentication Scheme

- K2
- A
- B
- Database
- D
- E
- F
- G

(K1, P1)
(K2, P2)
Hierarchical Authentication Scheme

Key Priority depends on several factors and computed as cumulative sum of weighted priorities of each factors:

Example Factors:
- Communication Delays
- Processing Speed of the Agents
- Key Usage
- Life Time of the Key
Clusters to Achieve Scalable Fault Tolerant Authentication

- Front-End is the MHA.
- Back-Ends are BHAs.
- Each packet is digitally signed by the Mobile Host.
- Packets are forwarded to the MHA.
- Back-Ends verify the signatures.
Example: Cellular Aided Mobile Ad hoc (CAMA) Network (In progress)

• Goal:
  – Integrating Ad hoc networks with current cellular system and building a topology that has advantages from both architectures
  – Overcome the traditional security weakness in ad hoc networks caused by lack of central control and slow information distribution
Advantages

• Reliable information distribution
  - Information for intrusion detection need not go through un-known intermediate hosts

• Fast information distribution
  - One hop uplink and downlink cellular channel takes place of multi-hop ad hoc channel

• Global positioning routing
  - Robustness of positioning routing can prevent Ad hoc network from attacks on routing discovery
Conclusion

- Service violation exists in all networks and puts severe threats to network security and performance
- Distributed monitoring and joint response among entities in the networks are essential to the detection of service violation
- Designed mechanisms must provide assurance on accuracy and efficiency of detection