On the effectiveness of monitoring for intrusion detection in mobile ad hoc networks

Rajendra V. Boppana and Xu Su
Intrusion Detection System

• Monitoring-based IDT
  • Some or all nodes monitor transmission activities of other nodes
  • IDT in MANET: Noise and interference *false positive*

![Diagram](image-url)
Outline

• 3 nodes testbed experiment
• Analytical Model
• Noise modeling
• Effectiveness Analysis in MANET
• Conclusion
3 Nodes Experiment
Intrusion Detection Monitoring

- Fixed Window

- Sliding Window

- Threshold
  - $T, L = WT$
Testbed Setting

- 3 nodes setting: Linksys wrt54g Wi-Fi router
  - Linear chain in a long corridor with 20’ apart
  - From 2:00 am to 5:00 am

Transmit every packet

A 200 Kbps B C

Fifty 500 byte packets per second

- Every node records the packet ID it receives, transmits, or overhear
Test result with $W=150$

- Though the testbed is small, it can show some interesting result.
Analytical Model

- **Notions**
  - $t_i, r_i, o_i$
    - e.g. in 3 nodes setting
    - $r_1 = o_2 = o_3 = t_3 = 0$
    - $t_1 \geq r_2 \geq t_2$ and $o_1 \leq t_2$
  - $q = \frac{r_2 - o_1}{r_2}$

- **Sliding window size monitoring**
  - Discrete Markov Chain
Sliding Window Size Monitoring

- Discrete Markov Chain

- \( p_{i,i-1} = \)
  \[
  P \left[ \begin{array}{c}
  \text{The oldest packet in current window is not overheared} \\
  \cap \text{The newest packet in next window is overheared}
  \end{array} \right] | \text{current state} = s_i = \frac{i}{W} (1 - q)
  
  \]

- \( p_{i,i+1} = \)
  \[
  P \left[ \begin{array}{c}
  \text{The oldest packet in current window is overheared} \\
  \cap \text{The newest packet in next window is not overheared}
  \end{array} \right] | \text{current state} = s_i = (1 - \frac{i}{W}) q
  
  \]
The purpose of Markov Chain is to estimate the time for a node to suspect the next node. It can be partitioned into

\[
P = \begin{pmatrix}
p_{0,0} & p_{0,1} & 0 & \cdots & \cdots & 0 & 0 \\
p_{1,0} & p_{1,1} & 0 & \cdots & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\
0 & \cdots & \cdots & 0 & p_{L-1,L-2} & p_{L-1,L-1} & p_{L-1,L} \\
0 & \cdots & \cdots & \cdots & 0 & 0 & 1
\end{pmatrix}
\]

\[
p_{i,i} = \begin{cases} 
1 - p_{i,i-1} - p_{i,i+1} & \text{if } 0 < i < L \\
1 - \frac{i}{W} (1 - q) - (1 - \frac{i}{W}) q & \\
1 - q - \frac{i(1-2q)}{W} & \\
1 - q & \text{if } i = 0 \\
1 & \text{if } i = L.
\end{cases}
\]

It can be partitioned into \( P = \begin{pmatrix} Q & C \\ 0 & 1 \end{pmatrix} \), so after \( n \) steps, the transition probability has the form \( P^n = \begin{pmatrix} Q^n & C' \\ 0 & 1 \end{pmatrix} \).

\( T_0 \) is the number of packets that node 1 transmit before it suspect node 2 is malicious.
Fixed Window Size Monitoring

- Model as Binomial Distribution
  - Number of not-overheard packets in window. \( W \) is the window size, \( q \) is the overall not-overhear rate
    \[
    \mathcal{P}[X = i] = \binom{W}{i} q^i (1-q)^{W-i}.
    \]
  - The probability that less than \( L \) (suspicion threshold) packets are not overheard
    \[
    \mathcal{P}[X < L] = \sum_{i=0}^{L-1} \binom{W}{i} q^i (1-q)^{W-i}.
    \]
  - The average number of fixed windows that need to be check before a fixed window has \( L \) or more not-overheard packets
    \[
    N = \frac{1}{1 - \mathcal{P}[X < L]} = \frac{1}{1 - \sum_{i=0}^{L-1} \binom{W}{i} q^i (1-q)^{W-i}}.
    \]
Model
The time can be calculated by \( ((N - 1) \cdot W + R_{fw})/\lambda \).
Noise Modeling
Background Noise Measure

- Testbed
  - 8 wrt54g Wi-Fi router
  - Each router provides noise level every 100ms

- Notice that: the noise level is much higher than the default ambient noise levels used in current simulators.
Matlab Model
GEV Noise Model

- RMSE

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Fixed window</th>
<th>Sliding window</th>
</tr>
</thead>
<tbody>
<tr>
<td>5%</td>
<td>0.2647</td>
<td>0.0002</td>
</tr>
<tr>
<td>10%</td>
<td>0.2193</td>
<td>0.0279</td>
</tr>
<tr>
<td>15%</td>
<td>1.8623</td>
<td>2.8541</td>
</tr>
</tbody>
</table>
Why GEV?

- GEV is a simple parametric noise model
  - Easily adjust to simulate different background noise
- GEV is not computationally expensive
  - Compare to CPM
- GEV has reasonable accuracy
IDT Effectiveness in MANET
Simulation of MANET

- **Performance Metrics**
  - Number of nodes suspected
  - False positive
  - Network throughput

- **Simulation Setting**
  - High density 1500*300
  - Low density 2200*440
  - Sliding window with default
  - Sliding window with GEV

---

<table>
<thead>
<tr>
<th>Number of Nodes</th>
<th>50</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Speed</td>
<td>[1-19] m/s</td>
</tr>
<tr>
<td>Node Mobility</td>
<td>Modified Random Waypoint</td>
</tr>
<tr>
<td>Pause Time</td>
<td>0 second</td>
</tr>
<tr>
<td>Field Size</td>
<td>1500 m x 300 m</td>
</tr>
<tr>
<td></td>
<td>2200 m x 440 m</td>
</tr>
<tr>
<td>Warmup time</td>
<td>200 sec.</td>
</tr>
<tr>
<td>Total simulation time</td>
<td>1800 sec.</td>
</tr>
<tr>
<td>Attack start time</td>
<td>600 sec. (if used)</td>
</tr>
<tr>
<td>Radio Range</td>
<td>250 m</td>
</tr>
<tr>
<td>MAC</td>
<td>802.11</td>
</tr>
<tr>
<td>Number of Traffic Pairs</td>
<td>10</td>
</tr>
<tr>
<td>Traffic Load</td>
<td>100 Kbps (CBR/UDP)</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>DSR</td>
</tr>
<tr>
<td>Data Packet Payload</td>
<td>500 bytes</td>
</tr>
<tr>
<td>Link BW</td>
<td>2 Mbps</td>
</tr>
<tr>
<td>Noise Models: Glomosim default</td>
<td>-100.97 dBm (constant)</td>
</tr>
<tr>
<td>GEV noise model:</td>
<td>-93.768 dBm</td>
</tr>
<tr>
<td>$\mu$</td>
<td>1.579</td>
</tr>
<tr>
<td>$\sigma$</td>
<td>0.179</td>
</tr>
<tr>
<td>$\xi$</td>
<td>-</td>
</tr>
<tr>
<td>Monitoring:</td>
<td>10%</td>
</tr>
<tr>
<td>Threshold, $T$</td>
<td>Sliding and fixed</td>
</tr>
<tr>
<td>Window type</td>
<td>150</td>
</tr>
<tr>
<td>Window size, $W$</td>
<td></td>
</tr>
</tbody>
</table>
IDT Setting

- Watch Dog Intrusion Detection
  - Monitoring-based Scheme
- Three Components:
  - Watch-dog
    - Send alarm to source if next hop is suspected
    - Clear monitoring window if the path breaks
  - Path rater
    - Node is rated based on observed behavior
    - Route rate is the sum of node along the path
    - Source always chooses highest rate path
  - Route request
    - New route discovery is initiated when all paths have negative rate
Simulation Result & Discussion: no malicious node

Threshold 10%

Number of nodes suspected

Total false positives

Throughput (kbps)

Time (s)
Simulation Result & Discussion: 10 malicious nodes
Conclusion & Discussion

- Monitoring based IDT is not accurate in ad hoc network due to the noise and other inference
- Default noise model in simulation is not good for ad hoc network
- Based on simulation of large ad hoc network, monitoring-based IDT may
  - Reduce performance of a normal network
  - May not improve the network throughput

- Questions?
Thank You