Providing Address Privacy and Communication Anonymity in Mobile Ad Hoc Networks
Yuguang Fang (UFL) and Yanchao Zhang (NJIT), http://web.njit.edu/~yczhang

Project Description

Network addresses of users are well-known in traditional mobile ad hoc networks. This enables attackers to easily locate, track, and launch targeted attacks on any interested user. Unprotected bare network addresses in packet headers also facilitate malicious traffic analysis to infer sensitive information such as network traffic patterns (e.g., who is talking to whom, and how often). This project aims to withstand such attacks by providing address privacy and communication anonymity.

Example 1: necessity for address privacy

Attackers in a military MANET can easily pinpoint commanding VIP users by overhearing and analyzing radio messages if knowing their addresses; attackers in a civilian MANET can track any user’s whereabouts after acquiring their network address.

Example 2: necessity for communication anonymity

Attackers in a military MANET can analyze network traffic patterns and/or traffic pattern changes. A significant change of traffic pattern may indicate a forthcoming action, a chain of commands, or a state change of network alertness.

Approach and Impact

<table>
<thead>
<tr>
<th>Approaches</th>
<th>Research Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use the <em>Middleman</em> approach to achieve controllable address privacy</td>
<td>• Controllable Address Privacy</td>
</tr>
<tr>
<td>• Manipulate cover traffic, packet rerouting, &amp; onion routing for strong communication anonymity</td>
<td>• Strong Communication Anonymity</td>
</tr>
<tr>
<td></td>
<td>• Overlay systems</td>
</tr>
</tbody>
</table>

Technical Details

Address privacy is achieved by hiding the network address of any user from all the others and enabling two users to communicate without knowing each other’s network address. Our approach is motivated by the scenario in spy movies where spies use middlemen to exchange information. Special measures are taken to balance the tradeoff between achievable address privacy and related communication and computation overhead. We formally model and quantify the achievable address privacy using an information-theoretic metric.

We achieve source anonymity, destination anonymity, and source-destination unlinkability via careful manipulation of cover traffic, packet rerouting, and onion routing. Different from previous work, our solution is an anonymous network overlay composed of nodes that anonymously communicate with one another atop the MANET substrate. Therefore, it can be built upon and nicely integrated with any (secure or insecure) MANET routing and MAC protocols. Formal analysis is used to evaluate the resulting communication anonymity under different attacker models.

Results: