Ad Hoc Network Secure Protocol Simulator

Wui Cheong Wong

Advised by: Wei Yu, Johannes Thorsteinsson, Yan Lindsay Sun, Prof. K.J. Ray Liu

Motivation:

1) Simulator can compare the security performance of different protocols
2) Ad hoc network can be established without help from a fixed infrastructure
3) Security is a critical issue since military work may be involved

Types of attacks:

1)Resource consumption attacks (waste bandwidth)
2)Routing disruption attacks (drop routing packets)

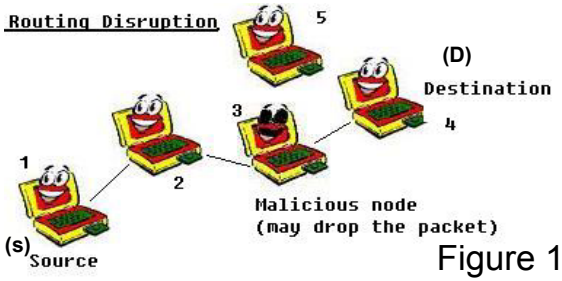
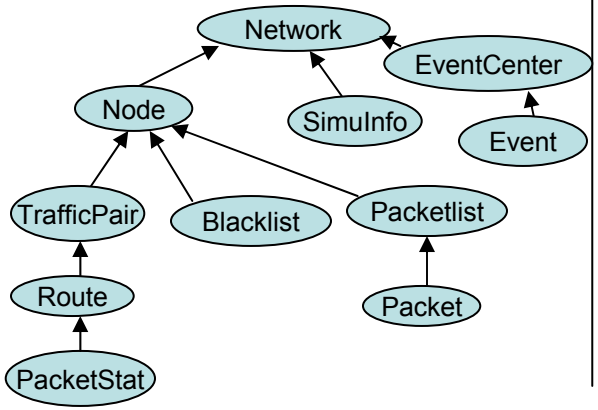


Figure 1

Simulator using C++:

-Object-oriented
-Easy to add more components or easy to change the scenario

Program Structure:



- **Network**

-Controls all other objects
-Contains nodes and graphs to simulate an ad hoc network
-Processes the events get from EventCenter

- **Event**

-Types of events: generate packet, forward packet, update graph

- **EventCenter**

-Registers events to an array, sort the event order by priority
-Network class processes events from here

- **SimuInfo**

-Contains all simulation information: good node #, bad node # area of network, transmission range of each node

- **Node**


Good node – never lies **Bad node** – may lie to frame others

-Contains position of itself, moving speed, moving direction, pause time between each move, power level, status of itself, packetlist
-Most important: contains Blacklist, TrafficPair

- **Packetlist**

-linked list of packets

- **Packet**

-Can be data packet, route request packet, route reply packet
-Knows sender & receiver
-Since DSR is the routing protocol, route is sent along with the packet

Most important in term of security issue:

- **TrafficPair**

-Knows it's sender and receiver
-A list of valid routes for this traffic pair

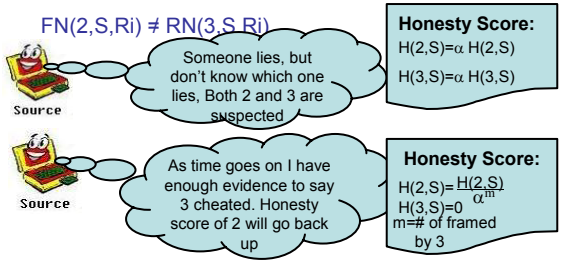
- **PacketStat**

-RN(A,S,Ri), number of packets received by hop A for S via Ri route
-FN(A,S,Ri), number of packets forward by hop A for S via Ri route
-P (A,S,Ri)= $\frac{FN(A,S,Ri)}{RN(A,S,Ri)}$ packet delivery ratio of hop A for S via Ri route

Example: In figure 1, node 2 claims it has forwarded all packets to node 3(malicious). But node 3 has not forwarded all packets to node 4
Result: P(2,S,Ri) = 1 & 0<P(3,S,Ri) <1

- **Blacklist**

-It contains the honesty score of other nodes
Honesty score: start with a 1 for every node. Score will go down if a node is suspected cheating
Example:
In figure 1, node 2 claims it has forwarded all packets to node 3(malicious). Node 3 tries to frame node 2, claims it receives none



Evaluation of routes:

$$Q(R_i)=\prod_{A\in R_i} P(A,S) * H(A,S) - \lambda * L_i$$

According to the information from PacketStat and Blacklist, we can determine which route is more secure
Li=number of hops in a route
λ=determine how important is the number of hops
**if the traffic is already heavy, shorter route preferred, we weigh Li more

Future work:

1) Finish the implementation
2) Additional routing protocol classes