Cryptographic threat model for Hocnet

2017-01-07

1 Application

Public mesh network where each node is paid for the bandwidth they forward. Participants can be anyone with a WiFi device. Some nodes may employ dedicated hardware like directional antennas, IR bridges, or self run wires in an attempt to provide the fastest lowest cost route to a gateway (a node selling access into the internet).

From the perspective of users and applications the mesh will act like layer 2 switch although with significantly more happening behind the scenes.

Nodes have no chance to pre-exchange data and have either a normal consume router or medium tier networking equipment depending on how much effort they put into providing a good route.

2 Threat model

An attacker will be able to modify packets, advertise false routes, man in the middle a connection, flood the network with fake nodes in an attempt to either capture more traffic (and thus profit), or control some fraction of the network. Lets assume less than 10% for an organized attack.

Of course multiple attackers performing some combination of these is possible.

3 Security Properties

Integrity checking for all packets, encryption for data packets, persistent identity and strong encryption for adjacent nodes, session unique identity for all other nodes (we don't care if a node across the network is the same between sessions, we do care about adjacent nodes being the same).

Since routing metrics have a useful life on the order of minutes the security only needs to last that long. Making weaker methods more feasible. Payload encryption just needs to be infeasible to decrypt all traffic from a node long term. We need a very secure channel to adjacent nodes only for billing discussions.

The network is flooded with announce messages every second from every node, it needs to be feasible to verify all of these as well as to generate many since each node must update the routing metric on forwarding.

In an ideal world there would be some way to ensure that routing cost monotonically increases from the announcing node and transmission quality monotonically decreases. But that's not required.

4 Performance Constraints

Since the actual mesh is pretty light on CPU resources we can dedicate most of our processing to encryption, think 60% of a fast cell phone processor, memory is a bit tighter since we have to maintain a routing table of every node, so small keys are important think no more than 1GB ram for the routing table which minus crypto is a MAC address, transmission quality value (single precision FP), and gateway info. So 16 bytes per node without crypto, we need the routing table to be big enough for "the last mile", hard to define goal there without more research.

On the network traffic side overhead needs to be as low as is feasible, even at the cost of upgraded processor, ram, or dedicated hardware.