Anonymous DTN routing protocol

Routing in a mobile delay-tolerant network (DTN) is extremely challenging, in part because data cannot simply go to where the destination is now; it must go to where the destination will be. Efficient solutions typically come at the cost of divulging users privacy - they require all participants to advertise where they are, where they have been, and where they intend to go - and therefore are not suitable for deployment among privacy-conscious users or hostile environments.

In this project, we propose a routing protocol which provides *identity anonymity* and *location anonymity* against untrusted participants in DTN. By the definition of identity anonimity, an identity of a packet sender or destination is not revealed to any other nodes whom the sender or destination doesn't trust. Location anonymity implies that the geographic location of a node cannot be tracked by other nodes whom the node doesn't trust. In addition, the proposed protocol would show reasonable efficiency in terms of packet delivery rate, bandwidth and packet delivery latency.

As a first order principle in this line of work, we assume that each participant uses ephemeral addresses - concretely, each node locally changes its address at the end of loosely synchronized epochs. To make this problem more concrete, we assume that each node has a set of other nodes whom it trusts: If Alice trusts Bob, then Bob is able to generate her ephemeral address at any time and map an ephemeral address back to her. Conversely, anyone Alice does not trust cannot link her to any of her ephemeral addresses. Within this trust model, the goal is for some node S to transmit a message to node D, without resorting to flooding the entire network, and without having to divulge any more than their ephemeral addresses to any nodes they do not trust. A strawman solution is to only forward messages through trusted nodes; but in a DTN, the set of trusted nodes may not form a path from S to D.

The key abstraction we seek to develop would allow trusted nodes to compute the address schedule of the destination. Each node maintains an ephemeral addresse during the pre-defined time frame, e.g., "epoch". Given the permanent address of Alice and epoch, Bob can generate the current ephemeral address of Alice. With this abstraction, we envision the following scheme: Senders initiate messages with the current ephemeral address of the destination. On contacting other node, the sender (or an intermediate node with packets to forward) gives a digest of packets that it wants to forward. Given the digest of packets, the next-hop node first pulls the packets whose destination nodes are either trusted by the next-hop node or included in the neighbor node list of the next-hop node. If the transmission of pulled packets is done, the sender may transmit unpulled packets to the intermediate node. If a message reaches an intermediate node trusted by the destination, the intermediate node regenerate the message with a new ephemeral address of the destination at the end of an epoch. Any untrusted node holding a message whose destination address has expired cannot determine where to route it, and so the node drops the data. This would ensure that messages that cannot be forwarded would eventually be garbage-collected.

The proposed protocol has several encouraging properties that are readily apparent. It maintain

anonymity even in the face of an eclipse attack wherein all of a victims neighbors are colluding attackers. Moreover, because untrusted nodes do not know a given users permanent or epehemral address at any point in time, attackers cannot launch a targeted denial of service attack. We have designed the proposed anonymous DTN routing protocol and are implementing the protocol using *ONE* simulator. ONE simulator supports a few existing DTN routing protocols such as epidemic, MaxProp and Prophet. Through the experiment, we will show the performance of our protocol compared to those existing DTN routing protocols.