Efficient Routing Over Ephemeral Addresses: Anonymity within a DTN

Dave Levin, Bobby Bhattacharjee, Elaine Shi, and Neil Spring

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. This work investigates whether it is possible to achieve efficient routing within a DTN without requiring mobile participants to be trackable. 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. Although this renders tracking nearly impossible, it also runs contrary to virtually all efficient routing protocols—how can Alice send a message to Bob if she (or anyone, for that matter) does not know Bob's address at any point in time?

To make this problem more concrete, we consider the following trust model. (1) We assume that each node has a set of other nodes whom it trusts: more specifically, if Alice trusts Bob, then Bob is able to map any address Alice uses back to her (conversely, anyone Alice does not trust cannot link her to any of her addresses). (2) We also assume that all participants are *honest but curious*—they will follow the protocol as prescribed, but seek to extract as much information as possible (without violating the protocol). (We believe this second assumption be necessary for convergence, but not for correctness.)

Within this trust model, the goal is for some node S to transmit a message to D, without resorting to flooding the entire network (the system should be efficient), and without having to divulge any more than their ephemeral addresses to any nodes they do not trust (the system should respect users' policies). A strawman solution is to only forward messages through trusted nodes, but in a DTN, the set of trusted nodes may not (or indeed, never) form a path from S to D. Any solution that divulges D's long-term identity compromises anonymity and is not suitable.

The key abstraction we seek to develop would allow trusted nodes to compute the address schedule of the destination. Specifically, trusted nodes would be able to know what address the destination is using now, the addresses it will use later, and the time frames ("epochs") during which it maintains a given address. With this abstraction, we envision the following scheme: Senders initiate messages with the correct (current) address. If a message reaches an intermediate trusted node, the trusted node re-generates the message with a new destination address at the end of an epoch. Nodes distribute digests containing their neighbors' current addresses. Given a message and a digest, a node (whether it is trusted or not) can determine if a neighbor has a path to the message's destination. Any untrusted node holding a message whose destination address has expired cannot determine where to route it, and so the node drops the data—to an untrusted node, it is as if the destination has ceased to exist (even if they came in contact with the destination, they would not realize it). This would ensure that messages that cannot be forwarded would eventually be garbage-collected.

While many details of this protocol and the underlying abstractions remain, it has several encouraging properties that are readily apparent. It maintain anonymity even in the face of an eclipse attack (wherein all of a victim's neighbors are colluding attackers). Moreover, because untrusted nodes do not know a given user's address at any point in time, attackers cannot launch a (targeted) denial of service attack.

We propose to develop the basic cryptography that would enable secure construction, aggregation, and dissemination of address digests, and develop a formal understanding of the security provided by our routing protocol. We also propose to study the convergence properties of this protocol. In particular, we wish to prove

that the protocol will find an end-to-end path securely if a path exists “often enough.” In conjunction, we propose to implement this protocol and study end-to-end performance over different deployments, both in simulations and over any available testbed.

Trimmed text from above

First, it maintains anonymity even if a node only has untrusted, colluding nodes as its neighbors—messages are delivered (assuming untrusted nodes forward), and that they are not able to map any ephemeral address to a long term identity. Second, because untrusted nodes do not know a given user’s address at any point in time, attackers cannot launch a (targeted) denial of service attack. In this sense, address digests serve as a form of communication capability—unlike prior work which filters all traffic that does not come with a valid capability, our proposed system “filters” traffic by virtue of the fact that no one but capable nodes have the ability to determine who the destination is.