Leveraging Social Contacts for Message Confidentiality in Delay Tolerant Networks [*]

Karim El Defrawy, John Solis and Gene Tsudik
Donald Bren School of Information and Computer Science, UCI
{keldefra,jsolis,gts}@ics.uci.edu

Abstract

Delay and disruption tolerant networks (DTNs) can bring much-needed networking capabilities to developing countries and rural areas. DTN features such as high node mobility and infrequent interconnectivity make it challenging to obtain security services for messages exchanged between users. In particular, it is hard to pre-fetch credentials of peer users. Furthermore, multi-round protocols are difficult to implement due to unbounded delivery times. In this paper we present schemes where users leverage social contact information to establish shared cryptographic keys, thus facilitating secure messaging in DTNs.

1. Motivation and Problem Formulation

Delay and disruption tolerant networks (DTNs) are characterized by highly mobile nodes, intermittent connectivity and frequent disruptions. Disruption can occur because of wireless radio range, sparsity of nodes, resources, or attacks. DTNs are an attractive solution for networking in rural areas and countries that lack communication infrastructures. Several DTNs are already currently in use [3, 4].

Low connectivity results in slow message propagation and unstable, non real time end-to-end paths. This complicates confidential and authenticated messaging. Since DTNs are applicable to a broad range of scenarios, we cannot assume the availability of traditional public key infrastructures (PKIs). Even if a PKI is available, we cannot assume that each node can retrieve the public key certificate of the destination or that queries to the PKI are returned in a timely fashion.

Problem Formulation:

Given above issues, how can a user *(S)* send a confidential message to user *(D)* through a DTN if *S* does not share a secret key with *D*, or know *D*'s public key (if it exists)?

We propose a scheme where *S* leverages social information, such as workplace affiliation or common social contacts, to send a confidential message to *D*. *S* will route the confidential message using secrets shared with affiliated intermediate nodes to ultimately deliver the message to D.

2. Network Model and Assumptions

We follow the language and definitions of the DTNRG Delay-Tolerant Networking Architecture [5]:

Network Model: We assume a generic network model with multiple operating regions defined by geographic boundaries (e.g., city or county). Regions are interconnected with fixed nodes, called gateways, that are part of a larger limited infrastructure. We envision a setting where each city is a region and gateways are placed at the entry/exit points of bus routes to the city. As buses travel between cities, crossing these gateways, messages are transferred to and from buses. We assume that nodes travel predominately within their home region, yet may periodically travel to other regions.

Node Assumptions: Nodes are uniquely identified by endpoint identifiers (EIDs) and the DTN has an underlying addressing scheme that allows nodes to exchange messages. To make our solution broadly applicable, we assume heterogeneous nodes and allow each region to use a different routing protocol. Nodes entering a new region are notified of the current routing protocol. Multiple gateways may be present at region boundaries. Gateways act as an overlay network inter-connecting regions.

3. Intra-region Messaging

The basic idea behind intra-region messaging is that it might be impossible for each user to retrieve (or store) the public key of all other users it communicates with. Instead, users can leverage social information to send confidential messages. We assume that each user shares a secret (or public) key with its friends and associated organizations/entities. If a user and destination have a mutual organi-

[*] Detailed project information can be found online at: http://sprout.ics.uci.edu/projects/dtn/

zation/entity or friend, the mutual entity can use the known public key or shared secret key of the destination to forward a message. With as few as two entities/friends in common, a user can *confidentially* send a message to a destination inside the same region. The sender adds two layers of encryption using the keys of the mutual entities and a source route that contains these entities. Upon receiving the message each entity removes its corresponding encryption layer and adds another that only the final destination can remove. A stream cipher (e.g., RC4) or an encryption scheme such as [1] can be used to achieve this. An added benefit of this technique is that nodes can verify that a message came from trusted friends or an affiliated entity.

However, it is possible that the sender cannot identify common friends or link the destination to any organization. In this case the sender generates a random key and encrypts the message with it. The key and the message are sent to the destination at different times. The problem with this approach is that any intermediate node who receives both messages can easily recover the confidential message. One can increase the number of encryption keys used and thus decrease the probability that a single node will capture all keys. However, this increases latency since all keys must be received before the destination can decrypt the message.

We show, by simulation, the probability of capturing a message and its corresponding key in a certain region and across different regions in the honest-but-curious adversary model[1]. While this probability can be zero (delay between messages exceeds message time-to-live (TTL)), we look at the more interesting case where the delay is less than the TTL. This balances total delivery time with probability of capture. Initial results show that a delay of 4 hours and an 8 hour TTL gives a 15% chance of capture.

4. Inter-region Messaging

Inter-region messaging occurs primarily between gateway nodes and is based on high-speed link access and gateway capabilities. If the source and destination gateways both have access to a high-speed link (e.g., 3G, WiFi or WiMax), the two gateways can use a multi-round protocol to establish a secure channel and trivially forward messages to each other. If both gateways are capable of public-key operations, then they can establish a secure channel. If not, then symmetric key solutions must be used. Since the number of gateways, and their locations, is constant we can employ existing schemes from MANETs and ad-hoc networks (e.g., probabilistic key exchange protocols[2], bipartite key agreement[6], interleaved encryption[1]).

We focus on interleaved encryption [1] as the underlying idea is similar to the one proposed for intra-region routing. Interleaved encryption works by establishing keys with each direct neighbor and with the direct neighbors of the direct neighbors. i.e, with all nodes one and two hops away. Keys of the one hop neighbors are not known to the set of nodes that are two hops away. To send messages a node encrypts using the keys of the next two nodes on the path to the destination. Upon receiving a message, a node removes its layer of encryption and adds the layer for the node two hops away. Interleaved encryption allows for confidential messaging if no two adjacent nodes collude.

Inter-region routing works by using the known local gateway as one social affiliation in the path to the destination. When a user *(S)* identifies the destination *(D)* as belonging to a different region (based on the EID) he encrypts the message under the keys of the local gateway and one common affiliation *(CA)*.

If CA and S are in the same region, CA receives the message, removes its layer of encryption, adds a layer using the key of *D*, and forwards to the local gateway. The gateway removes its layer of encryption and uses interleaved encryption as a black box to securely route messages to the destination region. The message is forwarded to *D* who removes the final layer of encryption to recover the message.

If CA and S are not in the same region, the gateway receives the messages, adds a layer using the key of the destination region gateway, and forwards to CA (regardless of its region). CA receives the message, removes its layer of encryption, adds a layer using the key of *D*, and forwards to the gateway of the destination region. The destination region gateway removes its layer of encryption and forwards it to *D* who removes the final layer of encryption.

Interleaved encryption combined with inter and intra-region routing enables confidential and authenticated messaging across the entire network.

References

[1] C. Castelluccia. Securing very dynamic groups and data aggregation in wireless sensor networks. *IEEE MASS*, pages 1–9, Oct. 2007.

[2] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *ACM CCS'02*.

[3] A. Pentland et al. Daknet: Rethinking connectivity in developing nations. *IEEE Computer*, 37(1):78–83, January 2004.

[4] J. Burgess et al. Maxprop: Routing for vehicle-based disruption-tolerant networks. *IEEE INFOCOM*, pages 1–11, April 2006.

[5] V. Cerf et al. Delay-tolerant network architecture. *IETF RFC 4838*, April 2007.

[6] N. Mittal. Space-efficient keying in wireless communication networks. *IEEE WiMOB*, pages 75–75, Oct. 2007.

[1] Nodes are not actively malicious (e.g., modify, drop or inject messages) but may read (or snoop on) messages being carried.