Anonymous Routing to Maximize Delivery Rates in DTNs

Kazuya Sakai*, Min-Te Sun†, Wei-Shinn Ku‡, and Jie Wu§
*Department of Info. and Commun. Systems, Tokyo Metropolitan University, 6-6 Asahigaoka, Hino, Tokyo 191-0065, Japan.
†Department of Computer Science and Information Engineering, National Central University, Taoyuan 320, Taiwan.
‡Department of Computer Science and Software Engineering, Auburn University, Auburn, Alabama 36849–5347.
§Department of Computer and Information Sciences, Temple University, 1925 N. 12th St. Philadelphia, PA 19122.
ksakai@tmu.ac.jp, msun@csie.ncu.edu.tw, weishinn@auburn.edu, and jiewu@temple.edu

***Abstract*—In this paper, we seek to address anonymous communications in delay tolerant networks (DTNs). While many different approaches for the internet and ad hoc networks, to the best of our knowledge, only variants of onion-based routing have been tailored for DTNs. Since each type of anonymous routing protocol has its advantages and drawbacks, there is no single anonymous routing protocol for DTNs that can adapt to the different levels of security requirements. In this paper, we first design a set of anonymous routing protocols for DTNs, called anonymous epidemic and zone-based anonymous routing, based on the original anonymous routing protocols for ad hoc networks. Then, we propose a framework of anonymous routing (FAR) for DTNs, which subsumes all the aforementioned protocols. By tuning its parameters, the proposed FAR is able to outperform onion-based, anonymous Epidemic, and zone-based routing.**

***Index Terms*—Delay tolerant networks, DTNs, anonymous routing.**

I. Introduction

Delay tolerant networks (DTNs) seek to address data communications within networks that lack continuous connectivity, such as people/pocket-switched networks, vehicular networks, battlefield communications, and so on. In this paper, we are interested in anonymous DTN communications that prevent adversaries from violating mobile users' privacy, e.g., deriving users' identities, locations, and routing paths, by traffic analyses.

A few anonymous routing protocols, which use the idea of onion groups [1] and the threshold [2], have been proposed for DTNs. However, the following research challenges that particularly arise in anonymous routing in DTNs are yet to be addressed. First, it is known that the use of a number of onions results in lower traceable rate. As a consequence, onion-based protocols [1] experience slow packet delivery. Second, the anonymous set of the source and destination nodes can be deduced, should the first and last onion relay be compromised. Third, although the zone-based approach improves node anonymity, neither Epidemi-like nor zone-based protocol has been proposed so far. One reason for this is the difficulty in defining a zone in DTNs where the network graph is constructed from the contact history, rather than from physical locations of nodes. At last, to the best of our knowledge, there is no work that balances the pros and cons of these different approaches. It is interesting to design an anonymous routing framework that subsumes all the aforementioned protocols and optimizes the anonymous DTN routing based on a number of metrics, e.g., delivery rate, anonymity, delay, and forwarding cost, by tunable parameters.

To address the above challenges, we propose the framework of anonymous routing for DTNs that subsume all the aforementioned protocols with tunable parameters.

II. Problem Formulation

A. Definitions and Assumptions

A DTN is represented by an undirected graph which is constructed from contact histories among nodes. Two nodes, say v_i and v_j, are connected in a graph if v_i and v_j have at least one contact in the past. The weight of a link between v_i and v_j is given by $\lambda_{i,j}$, where $1/\lambda_{i,j}$ is the expected inter-meeting time between v_i and v_j. It is known that the inter-meeting time between nodes in DTNs is modeled by the exponential distribution [3]. That is, the probability density function that v_i meets v_j at time t is obtained by $\lambda_{i,j}e^{-\lambda_{i,j}t}$. In addition, the probability that v_i meets v_j within T is computed by $1-e^{-\lambda_{i,j}T}$.

In onion-based routing, a message m travels a set of onions in the specified order by which each layer of an onion is to be peeled off. We denote R_i as the set of nodes for the i-th onion group by which m travels. The j-th node in R_i is labeled by $r_{i,j}$, and the size of R_i is G_i. In addition, the average group size is denoted by G.

For cryptographic operations, PK_i and SK_i are defined as the public and private keys of node v_i. In addition, GK_i represents the group key of onion group R_i. The encryption and decryption functions are denoted by $E(.)$ and $D(.)$.

B. The Attack Model

In this paper, we consider the compromise attack, where some nodes in a network are marked as being compromised and the message transmissions/receptions are monitored. Then, an adversary discovers possible routing paths based on the information disclosed from compromised nodes. Let $\{v_s, r_1, r_2, ..., r_K, v_d\}$ be a path with $K+1$ hops and the link between

two relays be $r_k \rightarrow r_{k+1}$. Then, we define the tracing attack as follow.

Attack 1 (The path tracing) *An adversary tries to discover links $v_s \rightarrow r_1$, $r_k \rightarrow r_{k+1}$ for $1 \leq k \leq K-1$, and $r_K \rightarrow v_d$ which constitutes a path as much as possible. Should r_k be compromised, an adversary will be able to find the next relay r_{k+1} by stalking r_k.*

C. Protocol Design

We propose a set of anonymous routing for DTNs based on ones primarily designed for ad hoc networks. Anonymous Epidemic (AE) routing is a flooding-like protocol. In AE, a message is encrypted by the destination's public key, and the encrypted message is forwarded at every contact. Restricted Epidemic Routing (RER) is an Epidemic variant, but the zone is defined to partially flood an encrypted message. Unlike the one for ad hoc networks, neither time-to-live nor physical location can be used for DTNs to define the partial flooding area. Thus, we introduce *zone deadline* by $t = -\frac{ln(1-\tau)}{\lambda}$. Here, λ is the average contact frequency and τ is the probability of the expected receiver receiving a message within t. Then, epidemic forwarding is conducted within the zone deadline. A zone-based anonymous DTN routing (ZBAR) can be constructed from Epidemic and spray-and-wait protocol, each of which is replaced with partial flooding and unicast routing (e.g., geographical routing). Between each pair of proxies, an anonymous spray-and-wait forwarding is used, which is basically the same as the one used between two intermediate relays in onion-based routing.

III. Framework of Anonymous Routing

In this section, we describe the high-level overview of the proposed FAR. Let v_s be the source node which wishes to deliver message m to destination v_d. The routing parameters, $\{K, L, G, F\}$, are selected by v_s, where K is the number of onion relays that m shall travel, L is the number of copies, G is the size of the onion group, and $F = \{f_1, f_2, ..., f_K\}$ is a set of forwarding modes. The forwarding mode can be either restricted epidemic RE or source spray-and-wait SW.

After initializing the routing parameters, v_s randomly selects a set of K onion groups ($K \geq 1$), along which m travels and creates an onion. How to forward m from one node to another differs, depending on the forwarding mode utilized. The forwarding mode for the i-th hop is determined by f_i. When a node, say r_j, in the next onion group R_{i+1} receives m, the outer layer of the onion is peeled off by the corresponding group key. Then, the forwarding process continues based on the forwarding mode specified in f_{i+1}. This process is repeated until the destination v_d receives m.

FAR subsumes epidemic, zone-based, and onion-based anonymous routing protocols. The parameters $(K = 0, null, null, S = \{RE\})$ indicate an AE protocol, in which epidemic is performed by hiding the source and destination nodes. In the case of $(K, L, G, \{f_1 = SW, f_2 = SW, ..., f_K = SW\})$, the protocol is reduced to onion-based routing. In addition, depending on G and L, the protocol can be onion ($G = 1$) or onion group ($G \geq 2$) routing with single/multi copies ($L = 1$ or $L \geq 2$) of the message. The configuration of $(K = 2, L = 1, G, \{f_1 = RE, f_2 = SW, ..., f_{K-1} = SW, f_K = RE\})$ serves as the ZBAR protocol.

IV. Performance Evaluation

We implement AE, ZBAR, and FAR along with OGR [1]. The simulations are conducted using the Infocom 2005 trace in CRAWDAD dataset [4]. The simulation methodology and configuration are basically the same as the ones in [1].

A. Results Using Real Traces

Figure 1 shows the delivery rate for different protocols with respect to the deadline. OGR always results in smaller delivery rate than the other protocols, and no significant difference between AE and FAR can be seen. ZBAR incurs a slightly longer delay than AE and FAR, as it uses the onion-based forwarding between source and destination proxies.

Figure 2 presents the traceable rate with respect to the percentage of compromised nodes. Note that traceable rate is independent of the inter-meeting time among nodes. As can be seen in the figure, the traceable rate of FAR is at least half of AE, ZBAR, and OGR when 50% of the nodes are compromised.

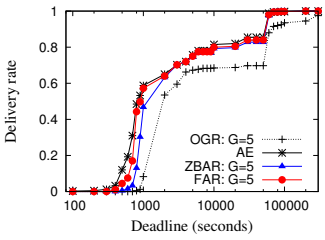

Fig. 1. The delivery rate.

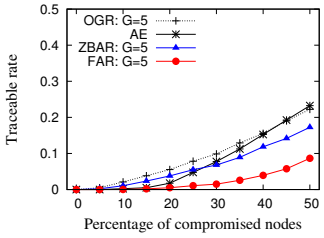

Fig. 2. The traceable rate.

V. Conclusion

In this paper, we first construct AE, RER, and ZBAR for DTNs by porting the existing solutions designed for ad hoc networks. Then, we design a framework for anonymous routing (FAR) that subsumes these protocols. By tuning parameters, the proposed FAR enjoys the advantages of these protocols, but at the same time offsets disadvantages. With this design, FAR accommodates compatibility problems among DTNs with different routing policies, and thus, it can be deployed to DTNs with different security and anonymous requirements with ease. The simulation using real mobility traces demonstrates that FAR outperforms the existing solutions.

References

[1] K. Sakai, M.-T. Sun, W.-S. Ku, J. Wu, and F. S. Alanazi, "An Analysis of Onion-Based Anonymous Routing for Delay Tolerant Networks," in *ICDCS*, 2016, pp. 609–618.

[2] R. Jansen and R. Beverly, "Toward Anonymity in Delay Tolerant Networks: Threshold Pivot Scheme," in *MILCOM*, 2010, pp. 587–592.

[3] W. Gao, G. Cao, A. Iyengar, and M. Srivatsa, "Supporting Cooperative Caching in Disruption Tolerant Networks," in *ICDCS*, 2011, pp. 151–161.

[4] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "CRAWDAD dataset cambridge/haggle (v. 2009-05-29)," Downloaded from http://crawdad.org/cambridge/haggle/20090529, May 2009.