E3PR: Efficient Privacy Preserving Prediction-based Routing in Mobile Delay Tolerant Networks

Jingwei Miao, Omar Hasan, Sonia Ben Mokhtar, Lionel Brunie

University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205, F-69621, France

{jingwei.miao, omar.hasan, sonia.benmokhtar, lionel.brunie}@insa-lyon.fr

Technical Report
University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205, F-69621, France

March 2014

E3PR: Efficient Privacy Preserving Prediction-based Routing in Mobile Delay Tolerant Networks

Jingwei Miao, Omar Hasan, Sonia Ben Mokhtar, Lionel Brunie

University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205, F-69621, France

Abstract

Message routing is one of the major challenges in Mobile Delay Tolerant Networks (MDTNs) due to frequent and long-term network partitions. A large number of routing protocols for MDTNs belong to the category of prediction-based routing protocols, which utilize the encounter probability of nodes to guide message forwarding. However, these prediction-based routing protocols compromise the privacy of the nodes by revealing their mobility patterns. In this paper, we propose a privacy preserving prediction-based routing protocol that forwards messages by comparing aggregated information about communities instead of individual nodes. Specifically, it compares the probability that at least one node in a community will encounter the destination node. We present theoretical security analyses as well as practical performance evaluations. Our simulations on a well established community-based mobility model demonstrate that our routing protocol has comparable performance to existing prediction-based protocols. Additionally, the community information is computed efficiently and independently of the routing protocol.

Keywords: delay tolerant networks, mobility, routing, privacy, community

1. Introduction

Mobile Delay Tolerant Networks (MDTNs) are constructed by the intermittent connection of co-located mobile devices, such as smart phones or sensor units. Contrary to Mobile Ad-hoc NETworks (MANETs) [1], a complete routing path between two nodes (i.e., mobile devices) that wish to communicate cannot be guaranteed in MDTNs [2]. The applications developed in these networks are often geo-localized with no critical time constraint, e.g., advertisement dissemination, recommendation of points of interest, and asynchronous communication. A number of networking scenarios have been categorized as MDTNs,

Email addresses: jingwei.miao@insa-lyon.fr (Jingwei Miao), omar.hasan@insa-lyon.fr (Omar Hasan), sonia.ben-mokhtar@liris.cnrs.fr (Sonia Ben Mokhtar), lionel.brunie@insa-lyon.fr (Lionel Brunie)

such as Vehicular Ad hoc NETworks (VANETs) [3], Pocket Switched Networks (PSNs) [4], etc.

In order to deal with the lack of end-to-end connectivity between nodes, message routing in MDTNs is often performed in a "store-carry-and-forward" manner [2], in which a node may store and carry a message for some time before forwarding it to another node [5]. In order to better choose intermediary nodes, a number of routing protocols [6, 7] forward a message from one intermediate node to another if the latter has higher probability of encountering the destination node. Such routing protocols are called prediction-based routing protocols. It has been shown that these protocols perform better than other protocols when nodes exhibit well-known mobility patterns. However, prediction-based routing protocols implicitly assume that nodes accept to reveal their mobility patterns to other nodes. However, in real-life, the disclosure of mobility patterns can result in the unwillingness of nodes to participate in MDTNs due to privacy concerns [8].

To the best of our knowledge, only our previous work (protocol 3PR [9]) has addressed the privacy issue of prediction-based routing protocols. In [9], message routing is guided by the maximum probability that nodes in a community will encounter a destination node. A community is defined as a set of nodes which frequently encounter each other (See Section 3). In order to compute the value of such maximum probability, the protocol in [9] needs to run $2+\beta$ (where $\beta \geq 7$) times of another protocol (named private_sum), which computes the sum of the probability that nodes in a community will encounter a destination node. In each run of the private_sum protocol, kN messages are exchanged among the nodes in a community, where N is the number of nodes in the community, k is a constant and $2 \leq k < N$. In this paper, we present an Efficient Privacy Preserving Prediction-based Routing protocol in MDTNs, named E3PR, which preserves the privacy of the node mobility patterns and is computationally efficient. In fact, E3PR has a running time of $1/(2+\beta)$ of that of the protocol presented in [9], where $\beta \geq 7$. Similarly to the protocol presented in [9], E3PR is intended for environments in which nodes belong to communities. Recent studies of real mobility traces have shown that this is the case for most nodes in real settings [10, 11, 12, 13].

We note that the performance of E3PR is similar to our previous protocol 3PR in terms of message routing. However, E3PR is more efficient in terms of computing the community information independently of the routing protocol. The 3PR protocol computes the maximum probability that nodes in a community will encounter a destination node, which, as described above, is an expensive operation. In contrast, the E3PR protocol computes the probability that at least one node in a community will encounter the destination node. In our performance evaluation of the protocols (Section 6), we observe that the delivery latency and delivery ratio of E3PR remain comparable to 3PR and other non-privacy preserving prediction-based routing protocols.

For routing a message, E3PR distinguishes the routing inside a community from the routing between communities. For disseminating a message inside a community, E3PR relies on the epidemic protocol [14], which by construction

preserves the privacy of nodes and is efficient as communities are small. The main challenge addressed by E3PR is thus the routing of a message between communities in a privacy preserving manner. To do so, each node in the network calculates the probability that at least one of the nodes in its community will encounter the destination. When two nodes from different communities encounter, instead of comparing their respective probabilities to encounter the destination node, they compare the aforementioned probabilities to determine the message forwarding decision. The probability that at least one node in a community will encounter a given node in the network is computed in a privacy preserving manner within the community using the MDTN-Private-Union protocol, also presented in this paper.

We evaluate E3PR both theoretically by providing a security analysis and practically through extensive simulations. We have conducted our simulations based on a well established community-based mobility model [15, 12]. We compare the performance evaluation of E3PR against four state-of-the-art protocols, i.e., the protocol in [9], epidemic [14], Direct [16], PRoPHET [17], and Bubble [10]. Epidemic and Direct are traditionally considered to achieve the upper and lower bounds of routing performance. PRoPHET and Bubble are representatives in prediction-based and social-based routing protocols respectively. Results show that E3PR has comparable performance to existing prediction-based protocols while preserving the privacy of nodes.

The remainder of this paper is structured as follows. Section 2 discusses related work on privacy preserving protocols in MDTNs. We then present our system model in Section 3. We describe the E3PR protocol in Section 4 followed by the MDTN-Private-Union protocol presented in Section 5. We further present our performance evaluation in Section 6 and the conclusion in Section 7.

2. Related Work

Recent years have seen considerable research addressing the issues of privacy in delay tolerant networks. The protocols in the literature are mainly concerned with preserving the privacy of one or more of the following sensitive user aspects: (1) identity, (2) location, (3) message content, and (4) relationships. In contrast, our protocol E3PR is a novel type of protocol, which has the specific goal of hiding the encounter probabilities of nodes. Therefore, E3PR differs fundamentally from other existing privacy preserving routing protocols for MDTNs due to the difference in objectives.

We note some recent protocols that attempt to hide the identity. Kate et al. [18] presented an anonymous communication architecture for MDTNs using Identity-Based Cryptography (IBC) [19]. This is one of the first anonymous communication solutions specifically for MDTNs. Kate et al. use a construct called MDTN gateways, which are entities assumed to be trusted and to be aware of user identities. In the routing process, a MDTN gateway replaces the identity of a source node with a pseudonym unlinkable to the identity. The advantage of the protocol is that there is not much overhead for routing.

However, the protocol relies on the assumption that trusted MDTN gateways are present, which is a strong assumption for MDTNs.

Le et al. [20] proposed a privacy preserving infrastructure called Privacy-Enhanced Opportunistic Networks (PEON) based on onion routing [21]. In PEON, nodes are clustered into groups. Nodes in the same group share public keys. Before sending a message, a source node determines the routing path, which contains a certain number of node groups. The message is then encrypted by the public keys of the destination node and the determined groups in an inverse order. Thus, each relay node can only be aware of the next hop (i.e., a node group) in the routing path and remains unaware of the identity of the source node. Compared to classic onion routing, the routing performance of PEON in terms of delivery ratio and delivery latency is enhanced due to the utilization of multicasting inside a group. However, node groups are randomly clustered, which may result in the inefficient dissemination of messages inside a group. In addition, the assumption of a Public Key Infrastructure (PKI) rarely holds in MDTNs [18].

Lu et al. [22] presented a social-based privacy-preserving packet forwarding protocol (named SPRING) for Vehicular DTNs. In SPRING, Road Side Units (RSUs) are assumed to be trusted and uncompromisable. RSUs are strategically deployed at some highly-social intersections to temporarily buffer the messages as relays. Due to the utilization of RSUs, an adversary cannot find out the identity of the source and the destination nodes. However, the private information of nodes is disclosed, if any RSU in the network is compromised. Additionally, all RSUs in SPRING are managed by a single management authority, which results in inflexibility.

In [23], Lu et al. proposed the Anti-Localization Anonymous Routing (ALAR) protocol for MDTNs. In ALAR, each message is divided into k segments and each segment is then encrypted and sent to n different neighbors. Therefore, an adversary may receive several copies of a segment at different times from different relay nodes. Even if the adversary collects these segments, they cannot localize the source node with high probability. The disadvantage is that the routing performance is influenced by the setting of the parameters k and n. Specifically, the routing performance in terms of delivery ratio and delivery latency is degraded as the two parameters increase.

Zakhary and Radenkovic [24] presented a location privacy protocol that is based on the utilization of social information of nodes. In this protocol, each node maintains a social profile, which includes n profile attributes. The social relationship between nodes are inferred by the matching of profile attributes. For each message, the forwarding is guided by the obfuscated attributes in the first k hops. After that, the message can be routed by any routing protocols. Therefore, an adversary cannot distinguish the location of the source node from the other k relay nodes. However, nodes that have strong social relationships are generally considered to be frequently co-located. Thus, the adversary can still detect the approximate location of the source node. Moreover, the routing performance is degraded, due to the extra k forwarding hops.

The following works protect the confidentiality of messages in DTNs. Jansen

and Beverly [25] proposed a Threshold Pivot Scheme (TPS) based on the technique of secret sharing. In TPS, a message, considered as the secret, is divided into multiple shares by the technique of secret sharing. The shares are delivered to the destination node via multiple independent paths. The content of a message is thus protected from individual intermediary nodes. At the destination node, the message can be reconstructed by the knowledge of any τ shares. The disadvantage of this protocol is that if an adversary succeeds in mounting a sybil attack, it can create multiple pseudonymous nodes and then intercept sufficient number of shares.

Shi and Luo [26] proposed an anonymous communication mechanism called ARDEN based on onion routing [21], multicast dissemination and Attribute-Based Encryption (ABE) [27]. In ARDEN, before sending a message, the source node determines a path of disjoint groups, one of which includes the destination node. The message is then encrypted by the keys of the destination node and the grouping keys. Compared with the traditional onion routing, the advantage of ARDEN is that it encrypts messages with the keys of groups rather than the keys of individual intermediate nodes. The performance in terms of delivery ratio and delivery latency can be improved, since all nodes in the same group can participate in message forwarding. On the other hand, the arbitrary group partitioning manner may result in performance degradation in terms of delivery ratio and delivery latency.

Parris and Henderson [28] presented the Privacy-enhanced Social-network Routing protocol. This protocol takes advantage of obfuscated social information rather than accurate social information to guide the message forwarding. The original social information of a node is obfuscated by the following two approaches: (1) modifying the friend list, i.e., adding or removing some items into or from the friend list, or (2) using a Bloom filter [29] to hash the friend list. The advantage of the protocol is that the presence of a public key infrastructure is not necessary. However, message routing may be guided erroneously due to the utilization of obfuscated social information. Moreover, in the case of modifying the friend list of a source node, an adversary can approximately determine the source node's friends by collecting the messages from the source node. In the second approach, the probability of false positives increases as the Bloom filter becomes more full, due to the characteristics of Bloom filter.

3. System Model

We consider a set V of mobile devices which can freely roam in a physical environment. Each mobile device is denoted as a node with a unique identifier. We assume that each node is equipped with a short-range radio interface (e.g., Bluetooth) for communication. For the sake of simplicity, we make the same assumption as in [30, 31, 32, 33] that the transmission range of all nodes is the same. Nodes are said to encounter (or contact) when they are in the transmission range of each other.

In general, the encounters between nodes can be characterized by the inter-meeting time (also known as inter-contact time) [30, 31], which is the time

interval between any two successive contacts of two given nodes. Karagiannis et al. in [34] demonstrated that under a large class of mobility scenarios in real life, the inter-meeting time follows a power-law in a finite range, and then exhibits an exponential decay. It is consistent with the suggestion made by Gonzalez et al. in [35] that a power law with an exponential decay is a very good approximation of human mobility patterns. Moreover, Chaintreau et al. in [36] pointed out that the exponential decay eliminates the issue of infinite message forwarding delay. Building on these previous studies, the inter-meeting time of nodes are assumed to be Independent and Identically Distributed (IID) with a given contact rate λ, which is the inverse of the expected inter-meeting time of any pair of nodes. It is a widely accepted assumption in MDTNs [30, 31, 32, 37].

Due to the nature of intermittent connectivity in MDTNs, message dissemination techniques are distinguished according to the connectivity of nodes. For the connected (i.e., encountering) nodes, messages are directly exchanged among them. We assume that the communication is unreliable, i.e., a message sent from a node to an encountering node may not arrive. However, we assume that the node knows whether the transmission of a message has been interrupted by a network failure or whether the message correctly reached the recipient (i.e., the encountering node).

For the disconnected nodes, a routing protocol is employed to deliver messages between them. The routing protocols that we address in this work are prediction-based routing protocols [6, 17, 12]. We generalize prediction-based routing protocols as follows: Consider a node a that has a message for a destination node d. When the node a encounters another node b, it forwards a copy of the message to the node b if the probability of b encountering d is higher than the probability of a encountering d. Thus the probability that a node with a copy of the message will encounter the destination node continues to rise until the message is delivered or the Time To Live (TTL) of the message expires.

As demonstrated in many studies [10, 38, 11] of real human mobility traces, we assume that nodes belong to communities [10] and each community has a unique identifier. We define a community C as a set of nodes such that $C \subset V$. We assume that the nodes in a community are frequently physically collocated and thus a high probability exists of successful message delivery from any source node in a community to any destination node in the community. A node l in each community is designated as the leader of the community. The leader node maintains the list of the nodes in the community. Let the set of nodes in a community $C = \{a_1, a_2, \ldots, a_n\}$, where $n = |C|$. We consider a community to comprise of at least three nodes, that is, $n \geq 3$.

Let an event $e_{a,d}$ denote that a node a has encountered a node d. Let $P(e_{a,d})$ be the probability that the event $e_{a,d}$ will happen. For simplicity, we omit the symbol of event e, that is, $P(e_{a,d}) \equiv P_{a,d}$. We note that our work focuses on preserving the privacy of this probability rather than its computation. The reader is referred to [17, 39] for details regarding the computation of such probability. We consider the probability that node a will encounter node d, that is $P_{a,d}$, as private information. Routing protocols can utilize such encounter probability to guide message forwarding. However, nodes require that their

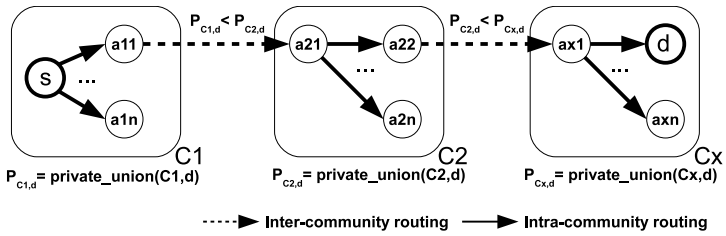


Figure 1: E3PR Protocol Overview

private information is not revealed to any other node in the network, which includes fellow nodes in a community.

In this paper, we consider the semi-honest adversarial model [40]. The nodes in this model always execute the protocol according to the specification. However, adversaries passively attempt to learn the private information of the nodes by using intermediate information gleaned during the execution of the protocol.

4. Privacy Preserving Prediction-based Routing

4.1. Protocol Description

In this section, we give an overview of E3PR, our Privacy Preserving Prediction-based Routing protocol. A routing example is depicted in Figure 1. This figure shows a number of nodes belonging to three communities C_1, C_2 and C_x. A source node s that belongs to the community C_1 wants to send a message to a node d that belongs to the community C_x.

In E3PR, we distinguish the routing inside a community (i.e., intra-community routing) from the routing between communities (i.e., inter-community routing). Specifically, when two nodes that belong to the same community encounter each other, they exchange all the messages they have. On the other hand, if two nodes a_{11} and a_{21} that belong to different communities C_1 and C_2 respectively encounter each other, node a_{11} forwards a message intended for a destination node d to node a_{21}, only if the probability that the nodes in community C_2 will encounter the destination node d is higher than the probability that the nodes in C_1 will encounter d. Let $P_{C_a,d} = union(C_a, d)$ be the probability that at least one node in community C_a will encounter the destination node d. In Figure 1, when node a_{11} encounters node a_{21}, node a_{11} forwards a copy of the message intended for d to node a_{21} because $P_{C_2,d} > P_{C_1,d}$.

Summarizing, to route a message from the source node s to the destination node d, the message is first disseminated in an epidemic manner inside the community of the source node. The message then moves from a community to another such that: (1) at each forwarding step, the probability that the message reaches the destination node is increased, (2) as soon as it reaches a community, the message is disseminated in an epidemic manner within the community.

A key characteristic of E3PR is that $P_{C_a,d} = union(C_a, d)$, the probability that at least one node in community C_a will encounter the destination node

d, is computed in a privacy preserving manner, that is without revealing the individual probabilities of the nodes in the community. $union(C_a, d)$ is therefore denoted as $private\_union(C_a, d)$ in Figure 1.

The E3PR protocol for privacy preserving prediction-based routing in MDTNs is specified in Figure 2. The computation of $private\_union(C_a, d)$ is performed using a decentralized protocol for privately computing the union of a set of probabilities in a delay tolerant network without revealing the individual values, i.e., MDTN-Private-Union further described in Section 5.

The probability $private\_union(C_a, d)$ is computed periodically in the community independently from the routing protocol. Hence, computing the probability has no direct impact on the performance of the routing protocol. Its only impact is on the recentness of the computed probabilities.

Protocol: MDTN-E3PR
Participants: Node a and node b.
Input: (1) m, a message carried by node a. (2) d, the destination node of message m. (3) C_a, the set of all nodes in the community of node a. (4) C_b. (5) $P_{C_a,d} = union(C_a, d)$, the probability that at least one node in community C_a will encounter node d. (6) $P_{C_b,d}$.
Output: Message m is delivered to node b if any one of the following conditions is met: (1) $b = d$, (2) $b \in C_a$, (3) $P_{C_b,d} > P_{C_a,d}$.
Setup: Node a has a message m whose destination is node d. Node b does not have message m.
Events and Associated Actions:

node a encounters a node b

```
1: if b = d then
2:     node a sends message m to node b
3: else
4:     if b ∈ C_a then
5:         node a sends a copy of message m to node b
6:     else
7:         if P_{C_b,d} > P_{C_a,d} then
8:             node a sends a copy of message m to node b
9:         end if
10:    end if
11: end if
```

Figure 2: Protocol: MDTN-E3PR

4.2. Security Analysis: Correctness

In order to increase the message delivery probability, the conventional prediction-based routing strategy forwards message copies to the nodes which have a higher probability of encountering the destination node than the current message carrier does. We consider our protocol E3PR to be correct if it achieves the same effect as the conventional prediction-based routing strategy.

In E3PR, a node a in community C_a sends message m to an encountering node b in another community C_b if $P_{C_b,d} > P_{C_a,d}$, i.e., if the nodes in community C_b have a higher probability of encountering the destination node d than the nodes in community C_a do (lines 7 and 8). Upon receiving message m, node b disseminates message m inside its community C_a in a flooding manner (lines 4 and 5). According to the definition of community in Section 3, the nodes which frequently co-exist in a common location comprise a community. Therefore, a high probability exists of successful message delivery from any node in a community to any other node in the same community. Considering this fact, message m reaches all nodes in community C_b with a high probability. Since the nodes in community C_b have a higher probability of encountering node d than the nodes in community C_a do, that is $P_{C_b,d} > P_{C_a,d}$, the protocol achieves a higher delivery probability by forwarding a copy of message m to node b.

4.3. Security Analysis: Privacy

In E3PR, a node a only reveals the probability that at least one node in its community C_a will encounter a given node to an outsider node. This probability is computed within the community in a privacy preserving manner using the MDTN-Private-Union protocol, thus individual probabilities of encountering the given node also remain confidential from the nodes inside the community.

One unavoidable side-effect of the protocol is that the adversary learns that node a's probability (i.e., $P_{a,d}$) of encountering the destination node d is no higher than $P_{C_a,d}$. Additionally, assume that node a achieves the maximum probability of encountering the destination node d in its community C. Therefore, the adversary also learns that the maximum probability of encountering node d is no higher than $P_{C_a,d}$. The reader may refer to Section 5 for the security analysis of the protocol MDTN-Private-Union.

5. Privacy Preserving Computation of Union

5.1. Protocol Description

Consider a community $C = \{a_1, a_2, \ldots, a_n\}$, where $n = |C|$. Let $P_{C,d}$ be the probability that at least one node in community C will encounter a given node d. In this section, we present a protocol for computing such probability $P_{C,d}$ in a privacy preserving manner. Let $e_{a,d}$ denote the event that a node a encounters node d, and $\overline{e_{a,d}}$ denote the opposite event of $e_{a,d}$. Let $P(e_{a,d})$ (denoted as $P_{a,d}$ in short) be the probability that event $e_{a,d}$ will happen. Therefore, the probability $P_{C,d}$ can be expressed as Equation (1).

$$\begin{aligned} P_{C,d} &= P(\textstyle\bigcup_{i=1}^{n} e_{a_i,d}) \\ &= 1 - P(\overline{\textstyle\bigcup_{i=1}^{n} e_{a_i,d}}) \\ &= 1 - P(\textstyle\bigcap_{i=1}^{n} \overline{e_{a_i,d}}) \\ &= 1 - \textstyle\prod_{i=1}^{n} P(\overline{e_{a_i,d}}) \\ &= 1 - \textstyle\prod_{i=1}^{n} (1 - P(e_{a_i,d})) \\ &= 1 - \textstyle\prod_{i=1}^{n} (1 - P_{i,d}) \end{aligned} \tag{1}$$

Each node in community C submits its individual probability of encountering node d, which is considered as a private information, to the protocol. After the computation of the protocol, each node learns the probability $P_{C,d}$ without disclosing its private information to other nodes. The protocol is specified in Figure 3.

The protocol is initiated by the leader node of the community C. The leader node floods an *init* message (Figure 3: protocol initiation: line 3) to all nodes in community C. Hereafter, we only concern about the nodes in community C. After receiving the *init* message, a node a can send the *init* message to any encountering node which has not received it yet (INIT: lines 7 and 8). After that, node a exchanges random numbers with each of the first K distinct encountered nodes (INIT: lines 10 and 11). K is a constant and its value is known to all nodes. Node a then mixes its σ_a (initially $\sigma_a = 1 - P_{a,d}$) with the sent and received random numbers (INIT: line 12). After encountering the first K distinct encountered nodes, node a sends the mixed private value to the leader node (INIT: line 14), when it encounters the leader node. The leader node maintains a product of the received mixed private values (PARTIAL: line 2). When the leader node receives all the mixed private values from the nodes in community C, the leader node computes the final result and floods it in its community (PARTIAL: line 4 and 5). The final result is the probability that at least one node in community C will encounter node d.

5.2. Protocol Setting

An interesting question is the relationship between the number of nodes in a community and the constant K, that is, what the value of the constant K should be. Recall the stated requirement with regard to the community size in Section 3: we consider a community C to comprise of at least three nodes. i.e., $n = |C| \geq 3$. Moreover, according to the mechanism of our protocol, a node at the most can exchange random numbers with all other nodes in its community. Therefore, the domain of the constant K should be $[2, n)$, i.e., $2 \leq K < n$.

In addition, when $K = 2$, whatever the value n is, these n nodes can always make a pair. Therefore, K can always be set as 2. When $2 < K < n$, according to the mechanism of our protocol, each node should exchange random numbers with K distinct nodes in its community. Hence, there are nK random numbers generated in each execution of our protocol. These nK random numbers should be divisible by $K+1$. That is $n(K+1-1) = n(K+1) - n$ is divisible by $K+1$. Therefore, the value of the constant K should meet the following requirement: $n\%(K+1) = 0$. An easy understanding example is that every $K+1$ nodes construct a clique.

Summarizing, the value of the constant K should meet the following two requirements: 1) $2 \leq K < n$ and 2) $K = 2$ or $n\%(K+1) = 0$.

5.3. Security Analysis: Correctness

The first challenge for the protocol is that the nodes a node will encounter are not known beforehand in MDTNs. To address this challenge, the protocol

Protocol: MDTN-Private-Union
Participants: Nodes in a community denoted by the set C. One node in C is the leader node denoted by l.
Input: Each node a_i has a private input $P_{i,d}$, that is the probability that node a_i will encounter node d.
Output: The nodes in C learn $\sigma_C = 1 - \prod_{a_i \in C} P_{i,d}$.
Setup: (l, g) uniquely identifies an instance of the protocol, where g is an integer. K is a constant such that $2 \leq K < n$ and $n\%(K+1) = 0$, where $n = |C|$. Nodes are not ordered, that is, a_i denotes any given node in C. ϵ is a sufficiently small number (i.e., 10^{-5}), which does not affect the accuracy of the computation.
Events and Associated Actions:

leader node l initiates the protocol

$R \leftarrow \phi$
$\sigma_C \leftarrow 1$
l floods $\langle \text{INIT}, l, g \rangle$ to all nodes in C

node $a_i \in C$ receives $\langle$INIT$, l, g\rangle$

$\sigma_i^0 \leftarrow 1 - P_{i,d}$
if $\sigma_i^0 = 0$ **then**
  $\sigma_i^0 \leftarrow \epsilon$
end if
for $j \leftarrow 1$ **to** K **do**
  a_i encounters node $a_j \in C$
  if a_j has not received $\langle \text{INIT}, l, g \rangle$ **then**
    a_i sends $\langle \text{INIT}, l, g \rangle$ to a_j
  end if
  a_i sends a random positive number r_{ij} to a_j
  a_i receives a random positive number r_{ji} from a_j
  $\sigma_i^j \leftarrow \sigma_i^{j-1} \times \frac{r_{ij}}{r_{ji}}$
end for
a_i sends $\langle \text{PARTIAL}, l, g, \sigma_i^K \rangle$ to l

leader node l receives $\langle$PARTIAL$, l, g, \sigma_i^K\rangle$ from a_i

$R \leftarrow R \cup \{a_i\}$
$\sigma_C \leftarrow \sigma_C \times \sigma_i^K$
if $R = C$ **then**
  $\sigma_C \leftarrow 1 - \sigma_C$
  l floods $\langle \text{FINAL}, l, g, \sigma_C \rangle$ to all nodes in C
end if

Figure 3: Protocol: MDTN-Private-Union

allows a node $a_i \in C$ to encounter any other K nodes in C (INIT: lines 5 and 6). The encountered nodes by node a_i are given as a_j, where $j \in \{1, 2, \ldots, K\}$.

Each node $a_i \in C$ exchanges random numbers (i.e., the sending random number r_{ij} and the receiving random number r_{ji}) with each of the first K encountered node a_j (INIT: lines 10 and 11). Node a_i multiplies its σ_i with the ratio of random numbers r_{ij} and r_{ji}, whereas node a_j multiplies its σ_j with the ratio of random numbers r_{ji} and r_{ij} (INIT: line 12). When the leader node computes $\sigma_C = \prod_{i=1}^{n} \sigma_i^K$, where $n = |C|$ (PARTIAL: line 2), the product σ_C is the required value $\prod_{i=1}^{n} \sigma_i^0$ because the product of $\prod_{i=1}^{n} \prod_{j=1}^{K} \frac{r_{ij}}{r_{ji}} \times \frac{r_{ji}}{r_{ij}}$ is 1 (PARTIAL: line 2).

Moreover, consider a special case that the σ_i^0 of node a_i is 0. In such a case, the σ_i^K is 0, whereas the exchanged random numbers are positive. Hence, when node a_i sends its σ_i^K to the leader node, the leader node can be aware that the σ_i^0 of node a_i is 0. In other words, the private information of node a_i is disclosed. In order to protect the private information for such kind of nodes. we modify the original σ_i^0 to be a small positive constant ϵ, if the original σ_i^0 is 0 (INIT: lines 2 – 3).

The result of σ_C (PARTIAL: line 2) will be influenced due to such modification. In order to investigate the impact of the modification on the original result, consider there are s, where $0 \leq s \leq n$, nodes whose original σ^0 are 0. Let σ_C is the result without the modification. Let $\sigma_C^{'}$ be the result with the modification. The value of $\sigma_C^{'}$ is $\epsilon^s \prod_{j=1}^{n-s} \sigma_j^0$. If $s = 0$, $\sigma_C^{'} = \sigma_C$; otherwise, the value of σ_C is then 0, and $\sigma_C^{'} - \sigma_C = \sigma_C^{'}$. However, the value of ϵ is so small that can be neglected. Hence, the value of $\sigma_C^{'} - \sigma_C = \sigma_C^{'}$ can be neglected.

The second set of related challenges of mobile delay tolerant network environments are as follows: connectivity is intermittent, messages may arrive after long and variable delays, and message transmission is asynchronous. Moreover, the MDTN-Private-Union protocol is based on community, while the community structure may change in the computation process of the protocol. For instance, some nodes in a community may leave the community, after the leader node initiates the computation of the protocol and before the computation is finished. Therefore, according to whether the community structure is changed or not during the computation of the protocol, we analyze the elements of the protocol that address this set of challenges in the following two cases.

In the case that the community structure does not change in the computation process, the following two elements of the protocol address the above set of challenges: (1) The *init* message reaches all nodes in community C with high probability and thus they all participate in the protocol. This is because that the nodes which frequently co-exist in a common location comprise a community. Therefore, a high probability exists of successful message delivery from any node in a community to any other node in the same community. (2) If a node $a_i \in C$ that has received the *init* message encounters a node $a_j \in C$ that has not yet received the *init* message then a_i sends a copy of the message to a_j to initiate it to the protocol (INIT: lines 7 and 8). Nodes consider an encounter successful only if they exchange all messages (i.e., a sending number and a

receiving number) according to the specification during their period of contact. Otherwise, they ignore any partial messages sent and received.

In the case that the community structure changes in the computation process, the above set of challenges are addressed by the following element of the protocol: the protocol is invoked periodically in a community independently from the routing protocol. Thus, even if the computation of MDTN-Private-Union cannot be finished due to the change of the community structure, the nodes in that community can still use the previous results of the protocol to guide the message forwarding police.

5.4. Security Analysis: Privacy

Without loss of generality, let's consider a node $a_i \in C$. In an ideal protocol, the node would submit its private value $P_{i,d}$ to a TTP. The TTP is considered trustworthy, therefore it would not disclose the private value $P_{i,d}$ of node a_i to any other party. It would only reveal the output of the protocol, which is the union of the private values received from all the nodes in community C.

In the MDTN-Private-Union protocol, node a_i discloses the following information: (1) a random positive number to each of the K nodes that it encounters after receiving the *init* message (INIT: line 10); (2) the value σ_i^K to the leader node l (INIT: line 14).

For the random positive numbers r_{ij}, where $1 \leq j \leq K$, since these numbers are independent of $P_{i,d}$, the encountered nodes do not learn any information about $P_{i,d}$.

With regard to $\sigma_i^K = \sigma_i^0 \times \gamma_i$, where $\gamma_i = \prod_{j=1}^{K} r_{ij}/r_{ji}$, let's assume that the interval of the random numbers is large compared to the interval of $P_{i,d}$ and that the random positive numbers are distributed uniformly. This implies that the interval of γ_i is also large and that it is distributed uniformly. Thus, the adversary can learn no information about $P_{i,d}$ from σ_i^K.

The adversary can learn $P_{i,d}$ if and only if it learns γ_i in addition to σ_i^K. To learn γ_i, the adversary must learn all values r_{ij} and r_{ji}. This is possible only if all K nodes a_j that encountered node a_i are dishonest and collude to reveal all of their individual r_{ij} and r_{ji} values and consequently the value of γ_i^K. The σ_i^K can be learned by the adversary, if the leader node is dishonest and colludes with the adversary (i.e., the K dishonest nodes).

After understanding the context where the private value of node a_i can be disclosed due to the collusion of dishonest nodes, an interesting question is the probability that such event happens. Let P_D denote the probability that the private value of a node a_i is disclosed by the collusion of dishonest nodes. According to the above analysis, we can see that $P_D = Prob\{\text{leader node } l \text{ is dishonest}\} \times Prob\{K \text{ encounters are dishonest}\}$. Hence, P_D depends on the number of nodes in community C, the value of K, and the number of dishonest nodes in community C. In order to identify P_D, we assume that the number of dishonest nodes excluding node a_i is known and denoted as m, where $0 \leq m \leq n-1$.

Let's assume that each node excluding node a_i in C has the same chance to be dishonest. Hence, $Prob\{\text{leader node } l \text{ is dishonest}\}$ can be expressed as Equation (2).

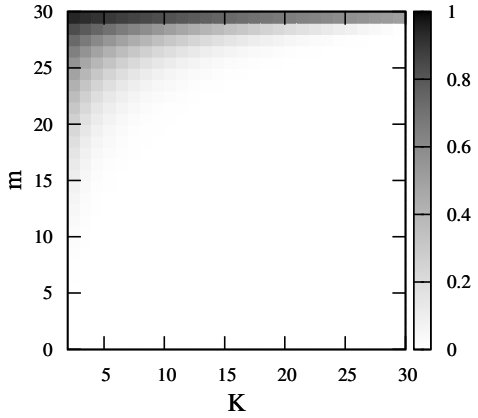


Figure 4: The impact of m and k on the privacy, where $n = 31$

$$Prob\{\text{leader node } l \text{ is dishonest}\} = \frac{m}{n-1} \tag{2}$$

Moreover, due to the random mobility model, we can probably assume that the encounters are random and cannot be scripted by the adversary. Hence,

$$Prob\{\text{K encounters are dishonest}\} = \begin{cases} 0, & \text{if } 0 \leq m < K \\ \frac{C_m^K}{C_{n-1}^K}, & \text{if } K \leq m \leq n-1 \end{cases} \tag{3}$$

Combining (2) and (3), the probability P_D can then be expressed as Equation (4).

$$P_D = \begin{cases} 0, & \text{if } 0 \leq m < K \\ \frac{m}{n-1} \times \frac{C_m^K}{C_{n-1}^K}, & \text{if } K \leq m \leq n-1 \end{cases} \tag{4}$$

The impact of m and K on the probability that the privacy of nodes is disclosed is illustrated in Figure 4. It can bee seen that (1) P_D decreases as K increases; (2) P_D increases as m increases. Moreover, we observe that P_D is high when m is chosen a big number.

In addition, one unavoidable side-effect of the protocol is that the adversary learns that node a_i's probability (i.e., $P_{i,d}$) of encountering the destination node d is not higher than $P_{C,d}$, since $P_{C,d} = P(\bigcup_{z=1}^{n} e_{z,d}) \geq P_{i,d}$, where $n = |C|$, $1 \leq i \leq n$. Furthermore, assume that node a_i achieves the maximum probability of encountering the destination node d in its community C. Therefore, the adversary also learns that the maximum probability of encountering node d is

not higher than $P_{C_a,d}$. However, the adversary can learn whether node a_i is the one who has the maximum probability of encountering node d, no better than a random guess with probability $1/(n-m)$. Moreover, the adversary can learn the exact value of the maximum probability of encountering node d, no better than a random guess with probability $\frac{1}{n-m}P_D$.

As in the ideal protocol, the output of the protocol is the union of the private values of all nodes in C. The MDTN-Private-Union protocol thus does not reveal any more information about the private value $P_{i,d}$ of node a_i than the ideal protocol if the following assumptions hold true: (1) the interval of the random numbers r_{ij} and r_{ji} is large compared to the interval of $P_{i,d}$ and the random numbers are distributed uniformly, and (2) at least one of the K nodes that encountered node a_i and the leader node is honest.

6. Experimental Evaluation

In this section, we present the performance evaluation of E3PR. We first present the simulation settings and the utilized mobility model in sections 6.1 and 6.2, respectively. We then introduce the routing protocols against which we compare the performance of E3PR and the performance metrics we used in sections 6.3 and 6.4, respectively. Finally, we present the results of our experiments in Section 6.5. As none of the algorithms against which we compare E3PR are privacy preserving, the objective of this performance evaluation is to assess the cost of introducing privacy preservation mechanisms in the routing process.

6.1. Simulation Settings

We have implemented E3PR as a module of the Opportunistic Network Environment simulator (ONE) [41]. We summarized the simulation parameters that we used.

We have used a simulation area of 2000 m $\times$ 1500 m. This area is equally divided into 12 regions as shown in Figure 5. In each region we initially deploy a varying number of nodes (from ten to fifty). Each node considers the region in which it has been deployed as its *local region*. According to the mobility model we used, further described below, a node is more likely to visit its local region than other places. Nodes associated to a region constitute a community. This simulation scenario is very similar to the one used in PRoPHET [17].

The communication between nodes is performed using the Bluetooth protocol since modern mobile devices are commonly equipped with this technology. Bluetooth has been often used in the evaluation of DTN protocols. For instance, the reality mining mobility traces [42], which have been used for the evaluation of many protocols, e.g., Habit [43], have been collected with mobile phones using Bluetooth. According to the specification of Bluetooth version 2.0 [41], the transmission range and bandwidth are set as 10 m and 2 Mb/s, respectively. Furthermore, the speed of nodes is set to 1.34 m/s, since this is an average human walking speed [44]. Each experiment we run approximately

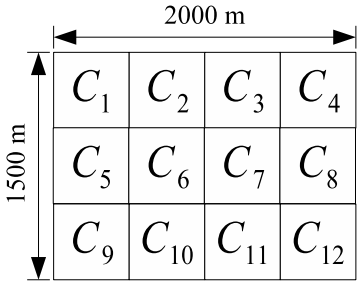


Figure 5: Community Model

Table 1: Parameter settings

Parameter Name	**Value**
Simulation area	2000 m × 1500 m
Transmission range	10 m
Simulation duration	13 hours + TTL
Warm-up period	1 hour
Message generation rate	1 message per 30 seconds
Number of communities	12
Number of nodes in a community	from 10 to 50
Node speed	1.34 m/s
p_l	0.8
p_r	0.2

lasts for thirteen hours (simulation time) among which one hour is a warm up period during which no message is generated. After this period, every thirty seconds, a random node sends a message to random destination node. We have considered only messages for which the source and the destination belong to different communities.

6.2. Mobility Model

In our evaluation, we adopt the community-based mobility model proposed in [15], which has been widely utilized for the evaluation of community-based routing protocols [31, 12]. In this mobility model, each community is associated with a geographical area. The movement of node i, which belongs to the community C_i consists of a sequence of *local* and *roaming* epochs. A local epoch is a random direction movement restricted inside the area associated with the community C_i. A roaming epoch is a random direction movement inside the entire network. If the previous epoch of a node i was a local one, the next epoch is a local one with probability p_l, or a roaming epoch with probability $1 - p_l$. Similarly, if the previous epoch of node i was a roaming one, the next epoch is a roaming one with probability p_r, or a local one with probability $1 - p_r$. The state transition between local and roaming epochs is shown in Figure 6. In our

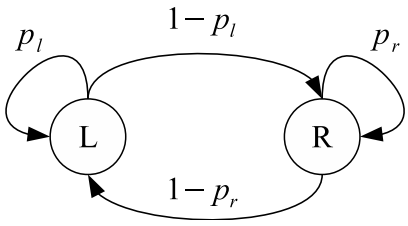


Figure 6: Community-based Mobility Model

simulations, we adopt the same values for p_l and p_r as in [17], i.e., p_l=0.8 and p_r=0.2.

6.3. Routing Protocols

We have compared the performance of E3PR against the following protocols:

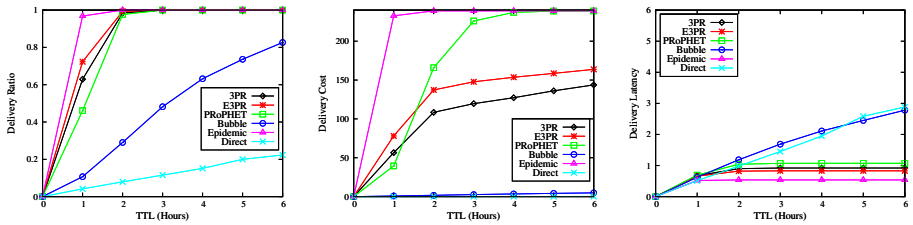
Epidemic: in this protocol, a node forwards a copy of each unexpired message it holds to every node it encounters, which does not already have a copy of the message. Epidemic routing achieves the upper bounds of delivery ratio and delivery cost, and achieves the lower bound of delivery latency.

Direct: in this protocol, the source node only forwards the message to the destination node. Contrary to Epidemic, Direct routing achieve the lower bounds of delivery ratio and delivery cost, and achieves the upper bound of delivery latency.

PRoPHET: in this protocol, a node forwards a copy of a message it holds to a node it encounters, only if the latter has a higher probability of encountering the destination node of the message. The parameters of the protocol are set as described in [17]. PRoPHET is a well known prediction-based routing protocol.

Bubble: this protocol utilizes social information about nodes, such as their centrality and the community to which they belong. There are two kinds of centrality in this protocol: local centrality and global centrality. The local (global) centrality value of a node indicates the number of its community members (nodes) that it encountered in time windows. In this protocol, a message is forwarded based on the values of the values of the global centrality of two encountering nodes, until it reaches a node in the same community as the destination node. After that, the message is forwarded based on the values of the local centrality of two encountering nodes, until it either reaches the destination node or expires. In our simulations, considering the TTLs of messages, the size of a time window is set to 1 hour. The centrality value of a node is accumulated in all time windows. Moreover, Bubble is a well known community-based routing protocol.

3PR: in this protocol, message forwarding decision is made by comparing information about communities of nodes instead of individual nodes. Specifically, it compares the maximum probability that a node in the community of a potential intermediate node will encounter the destination node. The parameters of the protocol are set as described in [9].



(a) Delivery Ratio (b) Delivery Cost (c) Delivery Latency

Figure 7: (a) delivery ratio, (b) delivery cost, and (c) delivery latency wrt the increasing TTL of messages.

We have compared the performance of E3PR against this set of algorithms for the following reasons. First, Epidemic and Direct are often used to show the upper and the lower bound in terms of performance, that can be reached in a given environment. Then, as E3PR is a prediction-, community-based algorithm, we used PRoPHET and Bubble as the representative algorithms for the categories of prediction-based and community-based algorithms, respectively.

6.4. Performance Metrics

To evaluate E3PR we used three well known metrics: the delivery ratio, the delivery cost and the delivery latency defined as follows.

Delivery ratio: is the proportion of messages that have been delivered out of the total unique messages created.

Delivery cost: is the total number of messages transmitted in the simulation. To normalize this, we divide it by the total number of unique messages created.

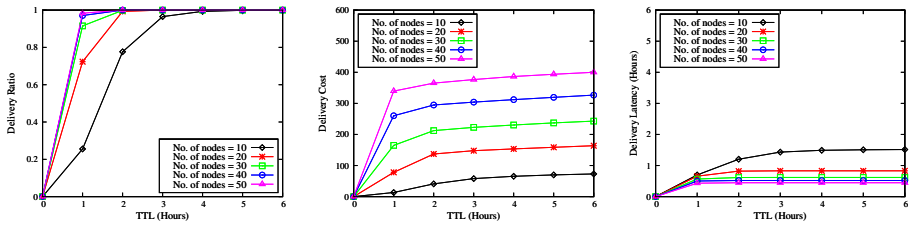
Delivery latency: is the average time needed to finish transmitting messages to their destinations.

6.5. Performance Results

We performed two experiments. First, we compared the performance of E3PR against the protocols introduced above, with respect to the above three performance metrics. We then analyze the impact of the community size on the performance of E3PR.

6.5.1. Performance Comparison of Routing Protocols

Figure 7 shows the delivery ratio of the compared protocols as a function of the Time-To-Live (TTL) of the generated messages. As expected, Epidemic and Direct achieve the best and worse delivery ratio, respectively, for all values of TTL. We also observe that E3PR achieves a better delivery ratio than PRoPHET and 3PR when the TTL is less then 2 hours, and achieves a similar delivery ratio to that of PRoPHET and 3PR when the TTL is greater than 2 hours. Finally, E3PR has a much higher delivery ratio than Bubble. The



(a) Delivery Ratio (b) Delivery Cost (c) Delivery Latency

Figure 8: (a) delivery ratio, (b) delivery cost, and (c) delivery latency wrt the increasing size of communities.

difference between the performance of the two protocols gets up to 70.29% for a TTL of 2 hours. This is because E3PR floods a message inside the communities which are on the path from the community of its source node to the community of its destination node.

Figure 7b, shows the delivery cost of the compared routing protocols. As expected, Epidemic and Direct have the highest and lowest delivery cost, respectively, whatever the value of TTL. Compared to the others, Bubble has a low delivery cost, which remains stable when the TTL increases. The delivery cost of E3PR is higher than that of Bubble and 3PR, but much lower than the one of PRoPHET.

Figure 7c shows the delivery latency of the compared routing protocols. Epidemic has the lowest delivery latency, whatever the TTL. Further, E3PR follows the same trend as Epidemic with higher latencies (around 0.29 hour). 3PR and PRoPHET achieve a little higher delivery latency than E3PR. The performance of Bubble and Direct increases linearly with the increase of the TTL.

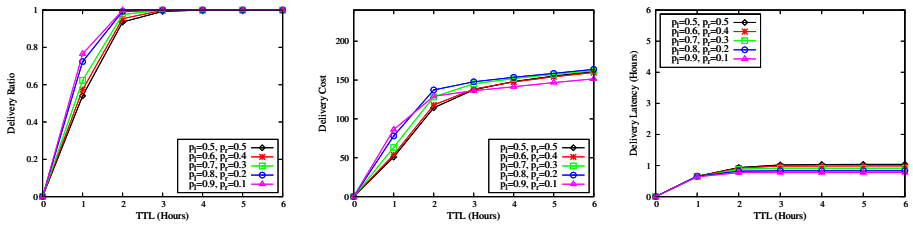
6.5.2. Influence of the Number of Nodes in a Community

In order to investigate the impact of the number of nodes in each community on the routing performance of our protocol, we run an experiment in which we vary the number of nodes in each community from 10 to 50.

Figure 8a, 8b and 8c show the impact of the increasing community size on the delivery ratio, the delivery cost and the delivery latency, respectively. Results show that the larger the communities, the higher the delivery ratio and cost and the lower the delivery latency. Since E3PR floods a message inside the community of the message carriers, the delivery cost increase as the communities become larger. However, more message copies increase the delivery probability and reduce the delivery latency.

6.5.3. Impact of the Settings of the Mobility Model

In this section, we investigate the impact of the settings of the adopted mobility model on the routing performance of E3PR. We run an experiment in



(a) Delivery Ratio (b) Delivery Cost (c) Delivery Latency

Figure 9: The impact of the settings of the mobility model on the (a) delivery ratio, (b) delivery cost, and (c) delivery latency of E3PR

which we vary the value of p_l from 0.5 to 0.9 with step by 0.1 and set the value of p_r as $1 - p_l$.

First, we look at the impact of the settings of the adopted mobility model on the delivery ratio. As shown in Figure 9a, we can observe that E3PR achieves similar results with different settings of p_l and p_r. The performance of delivery ratio increases as the increment of the value of p_l when the TTL is not greater than 3 hours. The performance of delivery ratio with different settings is the same, when the TTL is greater than 3 hours. Since E3PR floods messages inside a community, under the pre-condition that messages can be transferred among communities, the higher probability that a node stays inside its community, the higher probability that the node gets a message flooded inside its community.

Next, we compare the delivery cost of E3PR with different settings of the adopted mobility model. From the results illustrated in Figure 9b, we can observe that the performance of delivery cost increases as the value of p_l increases when the TTL is not greater than 3 hours. When the TTL is greater than 3 hours, the performance of delivery cost decreases as the increment of the value of p_l. This is because that the higher probability that a node stays inside its community, the higher probability that the node gets a message flooded inside its community. In our case, for a given message, most of nodes on the routing path from the community of its source node to the community of its destination node can get a copy of the message within 3 hours. Therefore, when the TTL is greater than 3 hours, the delivery cost increases slowly for the simulations with high values of p_l. This is consistent with the results of the delivery ratio.

At last, we investigate the results of delivery latency of (E3PR) with different settings of the adopted mobility model. As shown in Figure 9c, we can see that the delivery latency decreases as the increment of p_l. For each setting, the delivery latency increases as the TTL increases, when the TTL is less than 3 hours; the delivery latency keeps the same as the TTL increase, when the TTL is greater than 3 hours. For the case that the TTL is less than 3 hours, the messages that need more time can be delivered as the TTL increases. As for the case that the TTL is greater than 3 hours, the latency keeps the same, since the messages are delivered within 3 hours. Note that this is consistent with the results of the delivery ratio.

7. Conclusion

In this paper, we presented E3PR, a privacy-preserving prediction-based routing protocol for mobile delay tolerant networks. E3PR takes advantage of the mobility patterns of nodes to route messages, yet preserves the privacy of nodes by hiding their individual mobility patterns. The protocol requires that the nodes in a community compute the probability that at least one of the nodes in the community will encounter a destination node. We presented a protocol that computes this union in mobile delay tolerant networks in such a manner that the individual private values are not revealed even to the nodes inside the community. We evaluated E3PR both theoretically, with correctness and privacy analyses, and practically, through extensive simulations. Our simulations on a well established community-based mobility model, demonstrate that E3PR has comparable performance to existing prediction-based protocols, while preserving the privacy of nodes.

Acknowledgements

This work is supported in part by the China Scholarship Council (CSC) UT-INSA Ph.D. program, the MDPS German-French Doctoral College and the French National Research Agency (SocEDA, Grant ANR-10-SEGI-013).

References

[1] E. Royer, C. Toh, A review of current routing protocols for ad hoc mobile wireless networks, IEEE Personal Communications 6 (2) (1999) 46–55.

[2] K. Fall, A delay-tolerant network architecture for challenged internets, in: Proc. of the conf. on applications, technologies, architectures, and protocols for computer communications, 2003, pp. 27–34.

[3] T. Kosch, C. Adler, S. Eichler, C. Schroth, M. Strassberger, The scalability problem of vehicular ad hoc networks and how to solve it, IEEE Wireless Communications 13 (5) (2006) 22–28.

[4] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, C. Diot, Pocket switched networks and human mobility in conference environments, in: Proc. of ACM SIGCOMM workshop on Delay-tolerant networking, WDTN '05, ACM, New York, NY, USA, 2005, pp. 244–251.

[5] T. Spyropoulos, T. Turletti, K. Obraczka, Routing in delay-tolerant networks comprising heterogeneous node populations, IEEE Transaction on Mobile Computing 8 (8) (2009) 1132–1147.

[6] Q. Yuan, I. Cardei, J. Wu, An efficient prediction-based routing in disruption-tolerant networks, IEEE Transactions on Parallel and Distributed Systems 23 (1) (2012) 19–31.

[7] Z. Zhang, Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges, IEEE Communications Surveys and Tutorials 8 (1) (2006) 24–37.

[8] J. Miao, O. Hasan, S. Ben Mokhtar, L. Brunie, K. Yim, An investigation on the unwillingness of nodes to participate in mobile delay tolerant network routing, Int. J. Inform. Manage. 33 (2) (2013) 252–262.

[9] O. Hasan, J. Miao, S. Ben Mokhtar, L. Brunie, A privacy preserving prediction-based routing protocol for mobile delay tolerant networks, in: Proc. of the 27th IEEE International Conference on Advanced Information Networking and Applications, 2013, pp. 546–553.

[10] P. Hui, J. Crowcroft, E. Yoneki, Bubble rap: Social-based forwarding in delay-tolerant networks, IEEE Transactions on Mobile Computing 10 (11) (2011) 1576–1589.

[11] C. Boldrini, A. Passarella, Hcmm: Modelling spatial and temporal properties of human mobility driven by users' social relationships, Computer Communications 33 (9) (2010) 1056–1074.

[12] H. Dang, H. Wu, Clustering and cluster-based routing protocol for delay-tolerant mobile networks, IEEE Transactions on Wireless Communications 9 (6) (2010) 1874–1881.

[13] M. Boc, A. Fladenmuller, M. D. de Amorim, L. Galluccio, S. Palazzo, Price: Hybrid geographic and co-based forwarding in delay-tolerant networks, Computer Networks 55 (9) (2011) 2352–2360.

[14] A. Vahdat, D. Becker, Epidemic routing for partially connected ad hoc networks, Tech. rep., Citeseer (2000).

[15] T. Spyropoulos, K. Psounis, C. Raghavendra, Performance analysis of mobility-assisted routing, in: Proc. of the 7th ACM Intl. Symp. on Mobile ad hoc networking and computing, 2006, pp. 49–60.

[16] T. Spyropoulos, K. Psounis, C. S. Raghavendra, Efficient routing in intermittently connected mobile networks: The single-copy case, IEEE/ACM Transactions on Networking 16 (1) (2008) 63–76.

[17] A. Lindgren, A. Doria, O. Schelén, Probabilistic routing in intermittently connected networks, ACM SIGMOBILE Mobile Computing and Communications Review 7 (3) (2003) 19–20.

[18] A. Kate, G. Zaverucha, U. Hengartner, Anonymity and security in dtns, in: Proc. of SecureComm, 2007, pp. 504–513.

[19] A. Shamir, Identity-based cryptosystems and signature schemes, in: G. Blakley, D. Chaum (Eds.), Proc. of Advances in Cryptology, Vol. 196 of Lecture Notes in Computer Science, Springer Berlin / Heidelberg, 1985, pp. 47–53.

[20] Z. Le, G. Vakde, M. Wright, Peon: privacy-enhanced opportunistic networks with applications in assistive environments, in: Proc. of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments, PETRA '09, ACM, New York, NY, USA, 2009, pp. 76:1–76:8.

[21] M. Reed, P. Syverson, D. Goldschlag, Anonymous connections and onion routing, IEEE Journal on Selected Areas in Communications 16 (4) (1998) 482–494.

[22] R. Lu, X. Lin, X. Shen, Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks, in: Proc. of INFOCOM, 2010, pp. 1–9.

[23] X. Lu, P. Hui, D. Towsley, J. Pu, Z. Xiong, Anti-localization anonymous routing for delay tolerant network, Computer Networks 54 (11) (2010) 1899–1910.

[24] S. Zakhary, M. Radenkovic, Utilizing social links for location privacy in opportunistic delay-tolerant networks, the Proc IEEE ICC.

[25] R. Jansen, R. Beverly, Toward anonymity in dtns: Threshold pivot scheme, in: Proc. of MILCOM, 2010, pp. 587–592.

[26] C. Shi, X. Luo, P. Traynor, M. H. Ammar, E. W. Zegura, Arden: Anonymous networking in delay tolerant networks, Ad Hoc Networks 10 (6) (2012) 918–930.

[27] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proc. of the 13th ACM conference on Computer and communications security, CCS '06, ACM, New York, NY, USA, 2006, pp. 89–98.

[28] I. Parris, T. Henderson, Privacy-enhanced social-network routing, Computer Communications 35 (1) (2012) 62–74.

[29] B. H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM 13 (7) (1970) 422–426.

[30] E. Bulut, Z. Wang, B. K. Szymanski, Cost-effective multiperiod spraying for routing in delay-tolerant networks, IEEE/ACM Transactions on Networking 18 (2010) 1530–1543.

[31] K. . R. C. S. Spyropoulos, Thrasyvoulos; Psounis, Efficient routing in intermittently connected mobile networks: the multiple-copy case, IEEE/ACM Transactions on Networking 16 (1) (2008) 77–90.

[32] Y. Li, G. Su, D. Wu, D. Jin, L. Su, L. Zeng, The impact of node selfishness on multicasting in delay tolerant networks, IEEE Transactions on Vehicular Technology 60 (5) (2011) 2224–2238.

[33] Y. Li, G. Su, Z. Wang, Evaluating the effects of node cooperation on dtn routing, AEU - International Journal of Electronics and Communications 66 (1) (2012) 62–67.

[34] T. Karagiannis, J. Le Boudec, M. Vojnović, Power law and exponential decay of intercontact times between mobile devices, IEEE Transactions on Mobile Computing 9 (10) (2010) 1377–1390.

[35] M. Gonzalez, C. Hidalgo, A. Barabasi, Understanding individual human mobility patterns, Nature 453 (7196) (2008) 779–782.

[36] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, J. Scott, Impact of human mobility on opportunistic forwarding algorithms, IEEE Transactions on Mobile Computing 6 (6) (2007) 606–620.

[37] R. Groenevelt, P. Nain, G. Koole, The message delay in mobile ad hoc networks, Performance Evaluation 62 (1–4) (2005) 210–228.

[38] W. Hsu, T. Spyropoulos, K. Psounis, A. Helmy, Modeling spatial and temporal dependencies of user mobility in wireless mobile networks, IEEE/ACM Transactions on Networking 17 (5) (2009) 1564–1577.

[39] M. Musolesi, C. Mascolo, Car: context-aware adaptive routing for delay-tolerant mobile networks, IEEE Transactions on Mobile Computing 8 (2) (2009) 246–260.

[40] O. Goldreich, The Foundations of Cryptography - Volume 2, Cambridge University Press, 2004.

[41] A. Keränen, T. Kärkkäinen, J. Ott, Simulating mobility and dtns with the one, Journal of Communications 5 (2) (2010) 92–105.

[42] N. Eagle, A. Pentland, Reality mining: sensing complex social systems, Personal and Ubiquitous Computing 10 (4) (2006) 255–268.

[43] A. Mashhadi, S. Ben Mokhtar, L. Capra, Habit: Leveraging human mobility and social network for efficient content dissemination in delay tolerant networks, in: Proc. of WoWMoM, 2009, pp. 1–6.

[44] M. Kim, D. Kotz, S. Kim, Extracting a mobility model from real user traces, in: Proc. of INFOCOM, 2006, pp. 1–13.