PAPER Special Section on Trust, Security and Privacy for Pervasive Applications

# LOPP: A Location Privacy Protected Anonymous Routing Protocol for Disruption Tolerant Network

**Xiaofeng LU**[†a)], ***Member***, **Pan HUI**[††], **Don TOWSLEY**[†††], **Juhua PU**[†], ***and*** **Zhang XIONG**[†], ***Nonmembers***

**SUMMARY** In this paper, we propose an anonymous routing protocol, LOPP, to protect the originator's location privacy in Delay/Disruption Tolerant Network (DTN). The goals of our study are to minimize the originator's probability of being localized ($P_l$) and maximize the destination's probability of receiving the message ($P_r$). The idea of LOPP is to divide a sensitive message into $k$ segments and send each of them to $n$ different neighbors. Although message fragmentation could reduce the destination's probability to receive a complete message, LOPP can decrease the originator's $P_l$. We validate LOPP on a real-world human mobility dataset. The simulation results show that LOPP can decrease the originator's $P_l$ by over 54% with only 5.7% decrease in destination's $P_r$. We address the physical localization issue of DTN, which was not studied in the literature.

***key words:*** *location privacy, anonymous routing, anti-localization, security, DTN*

## 1. Introduction

An advantage of Mobile Ad Hoc Networks (MANET) is that it is not necessary to build the network infrastructure. However, if nodes move unpredictably at high speed, disconnections between nodes would be frequent and an end-to-end path between any node-pair may not be always possible. Such a kind of mobile ad hoc networks is referred to as a Disruption/Delay Tolerant Network (DTN) [1], [2]. Instead of pre-computing a routing path before sending, nodes can transmit a packet in a store-carry-forward fashion. They choose suitable encounter nodes as relays and when these relay nodes meet other nodes later, they forward the packet to the new relays. This packet delivery is analogous to the spread of infectious diseases [3], [4]. There could be many replicas of the packet in the network and if a copy of the packet reaches the destination node, the delivery is counted as successful [5]. Many routing protocols have been proposed for the delay tolerant network [6], [7] and partially connected MANETs [8], [9].

We focus on passive routing attacks that threat the security of mobile wireless networks. The nature of shared transmission media makes wireless networks very vulnerable to security threats. We expect to send messages without revealing the originator's location. For example, a law-enforcement team enters somewhere to find terrorists with mobile wireless networks to coordinate their motions. High-tech terrorists also eavesdrop the open-air wireless communication to detect wireless signals and trace the mobile nodes to launch the counterattack. Thus, the physical location privacy of the law-enforcement team is critical to the security of this law-enforcement team.

Some protocols can protect the location privacy at application layer, by which other users could not know a node's location from its connection request. However, if adversaries employ localization algorithm to explore the transmitter's location, they are able to know the transmitter's physical location without knowing the content of packets and launch a physical attack to destroy the transmitter which can bring serious destruction. Location privacy protected routing protocol in DTN is an open issue and has not been well studied yet. In this paper, we focus on assuring the originator to send sensitive messages with some delivery delay but not revealing the originator's physical location.

This paper is organized as follows. We review some related works about anonymous routing and secure routing protocols in Sect. 2 and introduce the threat model in Sect. 3. In Sect. 4, we introduce the transmission model and our anonymous routing protocol. We evaluate the routing protocol on human contact datasets in Sect. 5. Finally, we conclude our work in Sect. 6.

## 2. Related Work

Many protocols have been proposed to provide anonymity for Internet [10], [11] and MANET applications. However, few papers are about location anonymous routing in DTN.

Crowds [10] was designed to provide anonymity to users who want to access web pages. In Crowds, when a user wants to access a web server, he sends the web access request to other users before the request is sent to the web server. Other users will forward this request within them randomly before the request is sent to the web server. Thus, the web server cannot know which user originates the request, since it gets the request from a random member that is forwarding the message on behalf of the real originator.

Reed proposed onion routing in [11], [12]. The onion routing network allows the connection between the initiator and responder to remain anonymous. In onion routing, initiating applications make connections through a sequence of onion routers instead of making socket connections directly to the responding machine. In onion routing network,

Manuscript received July 3, 2009.
Manuscript revised October 9, 2009.

[†]The authors are with the School of Computer Science, Beijing University of Aeronautics and Astronautics, Beijing, China.
[††]The author is with the Deutsche Telekom Laboratories and TU-Berlin, Berlin, Germany.
[†††]The author is with the Dept. of Computer Science, University of Massachusetts, Amherst, U.S.A.
a) E-mail: luxf@cse.buaa.edu.cn

DOI: 10.1587/transinf.E93.D.503

messages are encapsulated with the keys of all intermediate nodes on the route to the destination. All nodes in the onion routing networks share a set of secret keys to peel off the encapsulated layers of an onion.

Some anonymous routing protocols are for ad hoc networks, such as MASK, ANODR, ASR. Zhang et. al proposed an anonymous on-demand routing protocol, MASK, for MANETs [13]. In MASK protocol, nodes authenticate their neighboring nodes without revealing their identities to establish pairwise secret keys in a neighborhood authentication process. By utilizing the secret keys, MASK achieves routing and forwarding without disclosing the identities of participating nodes. MASK provides identity privacy not location privacy. In MASK, adversaries may not identify the source from other nodes but they can compute the source's location.

ANODR is an anonymous protocol using on-demand routing for mobile ad hoc networks to provide route anonymity and location privacy [14]. For route anonymity, ANODR prevents adversaries from tracing a packet flow back to its source or destination; for location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitters. However, the location privacy ANODR provides is the identity of sender, not the physical location privacy.

Zhu proposed a secure routing protocol ASR for MANETs [15]. To realize anonymous data transmissions, the senders make sure that adversaries are not able to know the source and destination from data packets. Instead of encrypting the whole packet, they encrypt some small-size information and sent it together with the data packet. A relay node only needs to verify the encrypted small size information instead of the whole packet. ASR makes use of the shared secrets between any two consecutive nodes. The goal of ASR is to hide the source and destination information from data packets rather than protect the source's physical location privacy.

Most of anonymous routing protocols proposed for MANETs focus on ensuring that the receivers of packets are authenticated and cannot know the identify of the transmitter. Few of these protocols can protect the transmitter's physical location privacy.

## 3. Threat Model

### 3.1 Adversary Network

We suppose that adversaries are equipped with detection devices using omni-directional antennas to receive wireless signals. With radio detection devices, adversary can eavesdrop the wireless transmission within its communication range. Here, we assume an adversary's communication range to be fixed for the simplification reason and we assume all adversaries' communication ranges are the same. Two adversaries can send and receive packets only when they are within each other's communication range.

Eavesdropping leads to passive type of attack. Active attacks would like to start route disruption or "Denial of Service" attack. However, passive enemy will try to be as "invisible" as possible, until it starts to destroy the transmitter physically. This kind of passive attack is hard to be detected, so the passive attack is also a vital thread to MANETs [16].

An adversary saves received suspicious packets in its buffer and shares these suspicious packets with other adversaries when they meet. For example, a sensitive message is composed of $S_1$ and $S_2$. Adversary A received $S_1$ and adversary B received $S_2$ respectively. Both adversary A and B do not know $S_1$ and $S_2$ are segments of a sensitive message because they are not able to know the content of it before they have received both $S_1$ and $S_2$. When adversary A and B meet, they exchange $S_1$ and $S_2$ and both of them have $S_1$ and $S_2$ so as to know the content of the message.

### 3.2 Localization Algorithm: TDOA

Typically when an adversary node receives a sensitive message, it would like to know the identity and location of the transmitter. There are many localization algorithms such as TDOA (Time Difference Of Arrival), RSSI (Received Signal Strength Indicator) etc and most of them calculate a transmitter's location through triangle localization algorithm. Triangle localization algorithm needs at least 3 known nodes to compute an unknown node's location through the distance differences which can be acquired by differences in arrival time or differences in signals strength, etc.

One widely used localization algorithm is TDOA algorithm [17]. TDOA algorithm is as follows:

1. Assume a transmitter sends a packet at time $t = 0$, and $h$ adversaries receive it at different time $t_i (i = 1, 2, \ldots, h)$.

2. Adversaries share their time-of-arrivals (TD) and compute differences in the time-of-arrivals of this packet, $TD = t_i - t_j (i \neq j)$.

3. Then adversaries compute each corresponding spatial difference to the transmitter, $\triangle d_{i,j} = (t_i - t_j) \cdot C, (i, j = 1, 2, \ldots, h, i \neq j)$, where $C$ is the speed of light and $(i, j)$ is an enumeration of all pairs of receivers. Here, we assume each TD value is measured to a precision of about 10 nanoseconds which corresponds to about 3 meters.

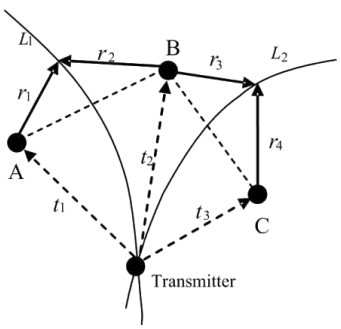



**Fig. 1** An illustration of TDOA localization algorithm, in which node A, B and C are three receivers of a packet from Transmitter.

4. With two adversaries, they can get a curve on which any point has the same $\triangle d$ to the transmitter.

5. At least three adversaries with known positions are required to find a 2D-position from two TDOAs as Fig. 1 shows.

## 4. Location Privacy Protected Routing Protocol

### 4.1 Transmission Model

Two nodes are called neighbors when they are within each other's transmission radius. Here, we assume that network nodes have the same transmission range $r$ and a node can only receive a packet when the sender of the packet is its neighbor. We assume a transmitter can send a packet to a specific receiver or broadcast a packet with the destination of this packet being a broadcast MAC address.

We assume the detection range of an adversary's detection system is larger than a node's communication range. Let the detection range of an adversary's detection system be $R$, $R = \beta r, \beta \geq 1$.

### 4.2 Formal Definition

It is dangerous to send a sensitive message in one packet to its neighbors directly because the originator does not know if there is any adversary in its neighborhood. The principle of our LOcation Privacy Protected routing protocol (LOPP) is to split the sensitive message into $k$ segments and send each segment to $n$ different neighbors.

Adversaries employ *TDOA* algorithm to locate the originator only when they know the content of a packet being sensitive. As other network nodes send and forward normal packets from time to time, there are lots of packets deliveries in the network. If adversaries compute each sender's location no matter whether this packet is a sensitive message or not, it would cost them much computing time and battery energy so as to the battery energy will be used up quickly.

Firstly, we introduce some assumptions for LOPP:

- Receivers including adversaries are able to know the content of a message only when they receive all segments.
- The relay nodes forward a packet only once to avoid broadcasting storm.
- In each packet, the source and destination's MAC addresses are assigned the broadcast MAC address.

Before sending a sensitive message, the originator assigns two specified values to $k$ and $n$ according to the network condition and divides the sensitive message into $k$ segments. It sends each segment to $n$ different neighbors. Table 1 lists all the notations we will use in our algorithm definition and the analysis later.

---

Algorithm: For the Originator

Originator's receiver-node set is $X_o$, $X_o$ is empty
**for** $i$=1 to $k$ **do**
  **if** $|Nb(originator)| \geq n$ and $Nb(originator) \notin X_o$ **then**
    Originator sends $S_i$
    $X_o \leftarrow Nb(originator)$
  **end if**
  move
**end for**

---

**Table 1** Notation and meaning.

| Notations | Meanings |
|---|---|
| $P_l$ | the probability of being localized |
| $P_r$ | the probability of transmission success |
| $S_j$ | segment $j$ |
| $Nb(node_i)$ | $node_i$'s neighboring nodes |
| $\|Nb(node_i)\|$ | The number of $node_i$'s neighboring nodes |
| $A$ | the transmitter's communication area |
| $\|A\|$ | the size of $A$ |
| $\|\|A\|\|$ | the number of adversaries in $A$ |
| $n$ | the number of neighbors |
| $k$ | the number of segments |
| $\lambda$ | the density of adversaries |
| $V$ | node's relative speed |
| $r$ | node's transmission range |
| $R$ | adversary's detection range, $R = \beta r$ |
| $p$ | the contact rate of nodes |
| $M$ | the number of normal nodes |
| $L$ | the length of experiment area |
| $N$ | the number of adversaries |

The algorithm for a relay node is different from that for the originator.

---

Algorithm: For a relay $node_j$

$node_j$'s receiver-node set is $X_j$, $X_j$ is empty
**loop**
  **if** $node_j$ receives a segment $S_i$ **then**
    $buffer \leftarrow S_i$
  **end if**
  **if** $|Nb(node_j)| \geq n$ and $Nb(node_j) \notin X_j$ **then**
    Get a segment $S$ from its $buffer$
    $node_j$ sends $S$
    Remove $S$ from its $buffer$
    $X_j \leftarrow Nb(node_j)$
  **end if**
  Listen to the network
**end loop**

---

The key step of LOPP protocol is to choose the appropriate value for parameters $k$ and $n$ according to the network environment. We choose the number of segments, k, from 2 and 3. We assign the value of $n$ to be the average number of a node's neighbors. The originator listens to the network every 10 minutes over $10 \times T$ minutes to get the total number of different neighbors $X$, then it computes the value of $n$ by $n = X/T$.

### 4.3 Localization Probability Model

#### 4.3.1 Without Fragmentation

If a sender sends a sensitive message in a packet without fragmentation, $P_l$ is the probability of there being at least three adversaries within the sender's transmission range according to TDOA algorithm. The probability of there being $k$ adversaries in $A$ can be calculated through Spatial Poisson Process [18].

$$Pr(\|A\| = k) = \frac{e^{-\lambda|A|}(\lambda|A|)^k}{k!} \tag{1}$$

$$\begin{aligned} P_l &= 1 - Pr(\textit{Not being localized}) \\ &= 1 - Pr(\|A\| < 3) = 1 - \sum_{k=0}^{2} \frac{e^{-\lambda|A|}(\lambda|A|)^k}{k!} \end{aligned} \tag{2}$$

#### 4.3.2 With Fragmentation

Assume that the originator divides a message into $k$ segments. When the originator sends the last segment, if there are more than two adversaries within its transmission range and these adversaries have received all the segments that the originator sends, they are able to know the content of this message when they receive the last segment, $S_k$. If this message is a sensitive message, they would employ TDOA localization algorithm to find the transmitter's position.

Let $N$ be the number of adversaries moving within a square area $L^2$ and $M$ be the number of normal nodes. According to [4], if the node's communication radius $r$ is largely smaller than the length of network area, say $r \ll L$, the rate $p$ at which a given node meets other nodes is

$$p = c\frac{Vr}{L^2} \tag{3}$$

where $c$ is a constant that depends on the mobility model used. We start from assuming the mobility model in our study to be random direction model or random direction, $c = 1$. Assume two nodes move at velocities $v_1$ and $v_2$, then the relative speed $V$ is computed by

$$V = c\frac{1}{\pi v_1 v_2}\int_{v_2-v_1}^{v_2+v_1}\left(\frac{x^2}{\sqrt{1-\left(\frac{v_1^2+v_2^2-x^2}{2v_1v_2}\right)^2}}\right)dx \tag{4}$$

Adversaries share their suspicious packets with each other when they meet, so the packets are delivered among adversaries according to epidemic routing [3], [4]. The authors of [4] derived the following estimation of the number of nodes that received a packet after time $t$:

$$I(t) = \frac{N}{1 + e^{-pNt}(N-1)} \tag{5}$$

where $I(t)$ represents the number of nodes that receive a segment, $p$ is the contact rate of the nodes and $t$ is the time duration from beginning till present.

Let $\lambda_j(S_i)$ represent the density of adversary nodes that have received $S_j$ when the transmitter sends $S_i$. We define $t_i - t_{i-1}$ to be the duration a node costs to move distance $R$ which is the detection device's detection range.

$$\lambda_1(S_2) = \frac{I(t_2 - t_1)}{L^2}, \ldots, \lambda_j(S_i) = \frac{I(t_i - t_j)}{L^2} \tag{6}$$

Let $\Lambda$ be the density of adversary nodes that have received all $S_i, i = 1, 2, \ldots, k-1$ when the originator sends $S_k$.

$$\Lambda = \prod_{i=1}^{k-1}\lambda_i(S_k) = \frac{\prod_{i=1}^{k-1} I(t_k - t_i)}{L^{2(k-1)}} \tag{7}$$

The probability of the originator being localized by adversaries is the probability that there are at least three adversaries which have received all the segment $S_1, \ldots S_{k-1}$ within the originator's transmission range when it sends the last segment $S_k$.

$$\begin{aligned} P_l &= Pr(\textit{being localized}) \\ &= 1 - \sum_{k=0}^{2} \frac{e^{-\Lambda\pi R^2}(\Lambda\pi R^2)^k}{k!} \\ \Lambda &= \frac{\prod_{i=1}^{k-1} I(t_k - t_i)}{L^{2(k-1)}} \end{aligned} \tag{8}$$

We did the simulation with parameters listed in Table 2. Figure 2 shows the increase of $P_l$ when sending packets with and without fragmentation. In this figure, x axis is the ratio of the adversary's detection range $R$ over the normal node's transmission range $r$, say $\beta = \frac{R}{r}$. Figure 2 shows that $P_l$

**Table 2** The values of parameters.

| Parameters | Values | Parameters | Values |
|---|---|---|---|
| $M$ | 100 | $L$ | 2000 m |
| $r$ | 30,50,70 m | $N$ | 25 |
| $v_1$ | 50 | $v_2$ | 50 |
| $k$ | 2 | $\beta$ | 1,2,...,7 |

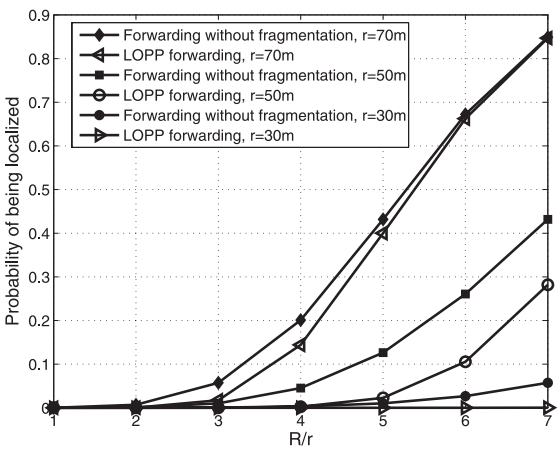



**Fig. 2** $P_l$ function of $\beta$ at different transmission ranges.

of sending packets with fragmentation is lower than that of sending packets without fragmentation in most conditions at given $r$ and $\beta$. This reveals our fragmentation sending is able to provide more location privacy for the originator. On the other hand, it also shows that both $P_l$ of routing packets with and without fragmentation increase with the increasing of $\beta$ at a given $r$. This is reasonable because if adversaries employ more advanced detection device, they have higher probability to detect legal node's signals so as to know its location. At a given value of $\beta$, $P_l$ increases with the increasing of node's transmission range. The larger a node's transmission range is, the more adversaries can receive its wireless signals and find the transmitter's location.

## 5. Simulation and Evaluation

### 5.1 Mobility Analysis

As human mobility plays a key role in packet routing in DTN [19], we need to check user mobility in real world. We evaluate LOPP on a real-world experiment dataset to determine the impacts of human mobility on the routing of packets. In this study, we use the experimental dataset gathered at the IEEE *Infocom* 2005 conference by the Haggle Project [20]. In the experiment, each participant carried a iMote device that logged the connection data. Each device has the same and limited transmission and reception range. Two nodes are considered to be neighboring nodes when they are within each other's transmission range.

Each device logged the begin time and end time of any connection with other nodes and that device's id. The format of this dataset is *(i, j, $t_b$, $t_e$)*, where $t_b$ is the begin time of a contact and $t_e$ is the end time of this contact. We define a variable *contact duration* to study the relative mobility between nodes, *contact duration* $= t_e - t_b$.

Figure 3 shows the distribution of the number of neighbors. We conclude that each node had at least one neighbor node with around 30 percent experiment time during the 4 days experiment time. This figure also shows a node did not have too many neighbors usually. It is almost zero probability that a node had more than 7 neighboring nodes at one moment in this experiment.

Figure 4 shows the contacts duration between nodes. The statistical results of these contacts show that more than 80 percent of the contacts are shorter than 10 minutes and more than 90 percent contacts are shorter than 20 minutes. This demonstrates that two nodes did not remain in contacted for a long time. This is the characteristic of disruption tolerant networks.

### 5.2 Simulation Results

We perform a packet routing simulation on the *Infocom* dataset to study the performance of LOPP. To get the average $P_l$ and $P_r$, we run the simulation program 100 times with each $n$. In each simulation, we randomly select two nodes as the originator and the destination node and randomly select some nodes as the adversary nodes. We assign the proportion of adversary nodes to be 50 percentage of all nodes to test the performance of our method in a highly risky network.

#### 5.2.1 Parameter Analysis: $k$

Figure 5 (a) shows the transmitter's $P_l$ at different number of segments, $k$. In this figure, the x-axis is the parameter $k$, where $k = 1$ corresponds to the no fragmentation case. The transmitter's average $P_l$ without message fragmentation is 0.256, but if we divide a message into two segments, the average $P_l$ is reduced to 0.116, which is about 54% improvement. The more segments we divide, the lower the value of $P_l$ becomes. This tells us that message fragmentation can significantly decrease $P_l$ of the originator.

However, with the increase of the number of segments, it would cost the originator longer time to send out all segments of a whole message and decrease the chance that the destination receives all segments. Figure 5 (b) shows that with the increase of $k$, $P_r$ decreases correspondingly. This reveals that the effect of minimizing the transmitter's $P_l$ and maximizing the destination's probability to receive a complete message $P_r$ are opposite. In order to resolve this, we

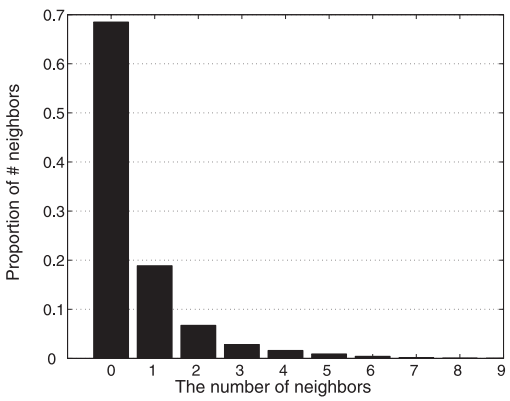



**Fig. 3** Distribution of the number of neighbors.

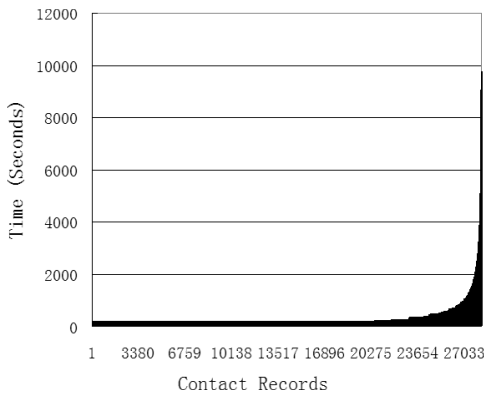
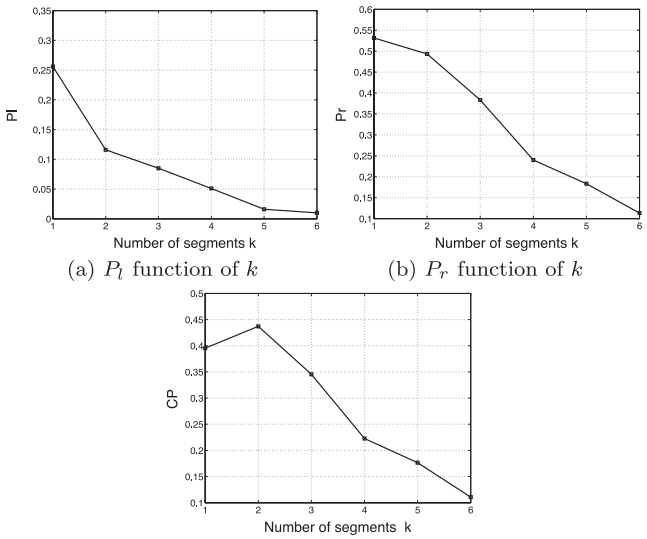


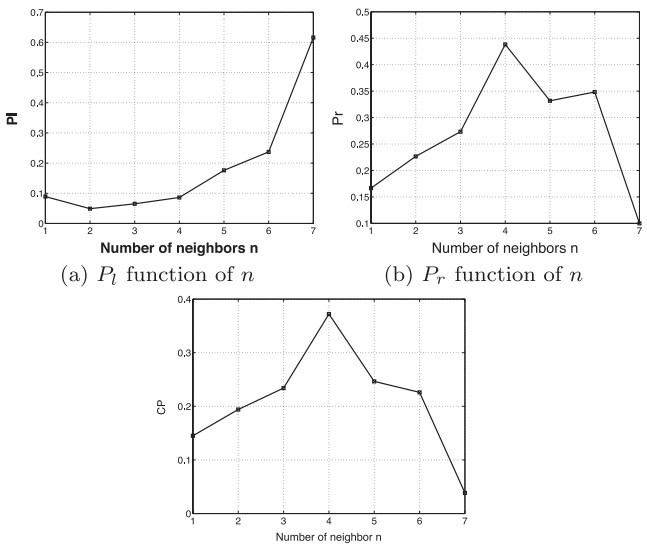

**Fig. 4** Contact durations between nodes. About 80% of the contacts are shorter than 10 minutes and more than 90% contacts are shorter than 20 minutes.




(a) $P_l$ function of $k$ (b) $P_r$ function of $k$

(c) $CP$ function of $k$

**Fig. 5** Impact of parameters $k$.




(a) $P_l$ function of $n$ (b) $P_r$ function of $n$

(c) $CP$ function of $n$

**Fig. 6** Impact of parameters $n$.

define a coalition probability $CP$ as the metric to determine $k$, where $CP = (1 - P_l) * P_r$, .

Figure 5 (c) shows that $CP$ reaches its maximum value when $k = 2$. Although we can get the smallest value of $P_l$ when $k = 6$, $P_r$ when $k = 6$ is smallest also. To get an overall optimized effect of LOPP protocol, we should not divide a message into too many segments. Hence, we suggest the number of segments to be 2 or 3.

### 5.2.2 Parameter Analysis: $n$

Figure 6 (a) shows the impact of $n$ on the originator's $P_l$. $P_l$ increases with the increase of the number of neighbors. If the originator sends segments when it has 1 or 2 neighbors, its $P_l$ is lower than 0.13, but $P_l$ is larger than 0.6 if it sends segments when it has more than 7 neighbors. The reason is if the originator sends segments when it has many neighbors, the probability of there being more than 2 adversaries in its communication range is high also.

Figure 6 (b) shows the destination node's $P_r$ with different $n$. We can see that the destination has about 45% probability to receive all segments of a complete message when $n$ is equal to 4. However, when $n$ is large, the probability of a node having so many neighbors becomes very small as Fig. 3 indicates. If a packet can not be spread out widely, the destination has low probability to receive it. This is the reason of the reduction of $P_r$ when $n$ is larger than 4.

Figure 6 (c) shows the coalition probability at different $n$. $CP$ reaches its maximum value 0.37 when $n$ is equal to 4. When $n$ is equal to 7, $CP$ is distinctly lower than other CPs. Our conclusion here is that the overall performance of LOPP protocol is highly related to the distribution of the number of neighbors. If we set the value of $n$ too low, segments can not be spread out widely and it will result in low $P_r$. If we set the value of $n$ too high, a node may only have very few chances of having so many neighbors at the same time and the segments can not be spread out, so it results in low $P_r$.

## 6. Conclusion

Location privacy is an important issue but has not been well touched in DTN. In this paper, we start looking at this issue by introducing a routing protocol, LOPP, which uses a series of *divide*, *forward*, and *move* procedures to increase node location privacy. We set up a mathematic model to compute the probability of the originator being localized by adversaries when it sends messages with fragmentation and without fragmentation. With the mathematic model, we prove LOPP can lower the originator's probability of being localized when it sends messages with fragmentation. Our simulation on a real-world mobility trace shows that LOPP protocol can decrease the originator's probability of being localized by over 54% without significant loss in delivery. We do not claim that we have found an optimum solution for location anonymous communication in DTN. It is a beginning instead of the end. We believe our work will trigger more researches in this area.

## Acknowledgment

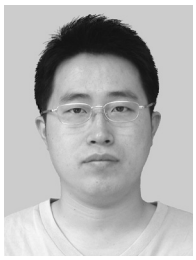
This work is supported by National Natural Science Foundation of China (60803120) and the P.h.D. Innovation Foundation of Beihang University

### References

[1] K. Fall, "A delay tolerant networking architecture for challenged internets," SIGCOMM '03: Proc. 2003 conference on Applications, technologies, architectures, and protocols for computer communications, pp.27–34, 2003.

[2] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K.

Scott, and H. Weiss, "Delay-tolerant networking: An approach to interplanetary internet," Communications Magazine, vol.41, pp.128–136, June 2004.
[3] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," Comput. Netw., vol.51, pp.2867–2891, 2006.
[4] T. Small and Z.J. Haas, "The shared wireless infostation model: A new ad hoc networking paradigm (or where there is a whale, there is a way)," MobiHoc '03: Proc. 4th ACM International Symposium on Mobile Ad Hoc Networking & Computing, pp.233–244, 2003.
[5] A. Panagakis, A. Vaios, and I. Stavrakakis, "On the effects of cooperation in dtns," Second IEEE/Create-Net/ICST International Conference on COMmunication System softWAre and MiddlewaRE (COMSWARE), 2007.
[6] T. Spyropoulos, K. Psounis, and C. Raghavendra, "Routing in intermittently connected mobile networks: The multi-copy case," IEEE/ACM Trans. Netw., vol.16, no.1, pp.77–90, Feb. 2008.
[7] W. Zhao, M. Ammar, and E. Zegura, "Controlling the mobility of multiple data transport ferries in a delay tolerant network," INFOCOM 2005, 24th Annual Joint Conference of the IEEE Computer and Communications Societies, 2005.
[8] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad-hoc networks," Tech. Rep, Duke CS-2000-06, Duke University, April 2000.
[9] W. Zhao, M. Ammar, and E. Zegura, "A message ferrying approach for data delivery in sparse mobile ad hoc networks," MobiHoc '04: Proc. 5th ACM international symposium on Mobile ad hoc networking and computing, pp.187–198, 2004.
[10] M.K. Reiter and A.D. Rubin, "Crowds: Anonymity for Web Transactions," Commun. ACM, vol.42, no.2, pp.32–48, 1999.
[11] M.G. Reed, P.F. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," IEEE J. Sel. Areas Commun., vol.16, no.4, pp.482–494, 1998.
[12] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing for anonymous and private internet connections," Commun. ACM, vol.42, no.2, pp.39–41, 1999.
[13] Y. Zhang, W. Liu, and W. Lou, "Anonymous communications in mobile ad hoc networks," IEEE INFOCOM 2005, 2005.
[14] J. Kong and X. Hong, "ANODR: ANonymous on demand routing with untraceable routes for mobile ad-hoc networks," ACM MOBIHOC '03, pp.291–302, 2003.
[15] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous secure routing in mobile ad-hoc networks," 29th Annual IEEE International Conference on Local Computer Network, LCNP '04, pp.102–108, 2004.
[16] X. Hong, J. Kong, and M. Gerla, "Mobility changes anonymity: New passive threats in mobile ad hoc networks: Research Articles," Wireless Communications & Mobile Computing, vol.6, no.3, pp.281–293, May 2006.
[17] F. Gustafsson, "Positioning using time-difference of arrival measurements," Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing., vol.6, pp.553–556, 2003.
[18] A. Kottas and B. Sans, Bayesian Mixture Modeling for Spatial Poisson Process Intensities, with Applications to Extreme Value Analysis, 2006
[19] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on the design of opportunistic forwarding algorithms," Proc. IEEE INFOCOM, pp.1–13, 2006.
[20] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE Rap: Social-based Forwarding in Delay Tolerant Networks," MobiHoc '08: Proc. 9th ACM International Symposium on Mobile Ad Hoc Networking & Computing, pp.241–250, 2008.



**Xiaofeng Lu** is currently a Ph.D. candidate in the Department of Computer Science of Beijing University of Aeronautics and Astronautics. He received his B.S. and M.S. degrees in computer science from North China University of Technology, in 1999 and 2005, respectively. He visited Computer Laboratory of University of Cambridge from 2007 to 2008. His research interests include wireless communication, Ad hoc networks security and anonymous communication in MANETs, etc.

**Pan Hui** is currently a senior research scientist in the Deutsche Telekom Laboratories and TU-Berlin after one year of postdoc in Cambridge on SOCIALNETs, ITA related projects. He received his B.S. and Mphil Degrees in 2001 and 2003 in computer science from University of Hong Kong. He received his Ph.D. in computer science from university in 2007. His research interests include social networks, and delay tolerant networks.

**Don Towsley** received the B.A. degree in physics and the Ph.D. degree in computer science, both from University of Texas University, in 1971 and 1975 respectively. He is currently a Distinguished University Professor in the Department of Computer Science at the University of Massachusetts - Amherst, where he co-directs the Networking Research Laboratory. He has been a Visiting Scientist at AT&T Labs - Research, IBM Research, INRIA, Microsoft Research Cambridge, and the University of Paris. He currently serves as Editor-in-Chief of the IEEE/ACM Transactions on Networking and on the editorial boards of Journal of the ACM and IEEE Journal of Selected Areas in Communications. He has twice received IBM Faculty Fellowship Awards, and is a Fellow of the IEEE and the ACM. Dr. Towsley's research interests include network measurement, modeling, and analysis.

**Juhua Pu** is currently an Associate Professor in the Department of Computer Science and Engineer of Beijing University of Aeronautics and Astronautics. She received her Ph.D. in computer science from Beijing University of Aeronautics and Astronautics in 2005. In 2004, Juhua Pu visited the Hongkong University of Science and Technology. Dr. Pu's current research interests include sensor networks and distributed multimedia, etc.

**Zhang Xiong** is currently a Professor in the school of Computer Science of Beijing University of Aeronautics and Astronautics. He received his M.S. degree in computer science from Beijing University of Aeronautics and Astronautics in 1984, and visited the Michigan State University from 1989 to 1992. Professor Xiong was awarded China National Golden Medal for Progress in Science and Technology in 1994. His current research interests include wireless sensor networks, multimedia, RFID, etc.