information

MDPI

Article

A Privacy-Preserving Protocol for Utility-Based Routing in DTNs

Qingfeng Jiang [1], Kun Deng [2,*], Lei Zhang [3] and Chun Liu [4]

[1] College of Computer Science and Engineering, Changshu Institute of Technology, Changshu 225500, China; qingfeng_jiang@163.com
[2] College of Mathematics Physics and Information Engineering, Jiaxing University, Jiaxing 314001, China
[3] College of Information and Electronic Technology, Jiamusi University, Jiamusi 154007, China; 8213662@163.com
[4] College of Computer Science and Information Technology, Daqing Normal University, Daqing 163712, China; saralc@126.com
* Correspondence: dengkun@hrbeu.edu.cn

Received: 12 February 2019; Accepted: 31 March 2019; Published: 8 April 2019

Abstract: In the utility-based routing protocol of delay-tolerant networks (DTNs), nodes calculate routing utility value by encounter time, frequency, and so on, and then forward messages according to the utility. The privacy information of encounter time and frequency will be leaked when nodes communicate with real IDs. Node ID anonymity can protect the privacy information, but it also prevents nodes from collecting encounter information to calculate the real utility value. To solve the above problem, this paper proposes a privacy-preserving protocol for utility-based routing (PPUR) in DTNs. When node encounter occurs in PPUR, they anonymously generate and collect the encounter record information by pseudo-IDs. Then, nodes forward the information to a trusted authority (TA), which calculates the routing utility value and returns it to the nodes, so that nodes can protect the privacy information and obtain the real utility value at the same time. PPUR also protects the confidentiality and integrity of messages through hashing and digital signature. The experimental results show that PPUR can not only protect nodes' privacy information, but also effectively forward messages with real utility value.

Keywords: delay-tolerant networks (DTNs); privacy-preserving; utility-based; encounter information

1. Introduction

Delay-tolerant networks (DTNs) are networks without a stable end-to-end connection, and have the characteristics of long delay, intermittent interruption, small node buffer, and low computation capacity [1]. DTNs have been widely used in the fields of social networks, vehicular networks, disaster relief, environmental monitoring, and military strategy. Different from the traditional networks, DTNs lack guaranteed connectivity. Therefore, the message forwarding process in DTNs follows a "store-carry-and-forward" manner, i.e., messages are opportunistically routed toward the destination nodes. Many utility-based routing protocols [2–7] have been proposed to effectively deliver messages according to routing utility upon node encounter. In the utility-based routing protocol, nodes need to collect the encounter information, e.g., encounter time, the distance, visit frequency, geographic location, or contact history with real IDs, in order to deduce the routing utility. However, the privacy-sensitive encounter information will be leaked if nodes communicate with real IDs directly, and it will cause a significant security problem. Malicious nodes can attack by analyzing the information. For example, once an attacker intercepts the encounter time and location of a node, it may learn the node's mobility pattern.

At present, some node anonymity strategies [8,9] have been proposed to protect nodes' privacy information. However, when neighbor node anonymity is enforced, nodes cannot collect the encounter information to deduce the routing utility. Chen et al. [10] proposed FaceChange, a protocol which can support both anonymizing real IDs among neighbor nodes and collecting encounter information. However, the encounter information collected is real ID-based and will thus leak privacy information.

To solve the above problem, a privacy-preserving protocol for utility-based routing (PPUR) in DTNs is proposed in this paper. In PPUR, two encountering nodes collect encounter record information anonymously through pseudo-IDs. A node forwards encounter record information to a trusted authority (TA) when connecting the access point (AP). The TA calculates the node's routing utility value through encounter record information and then returns the value, so the node can protect privacy information and obtain the real utility value at the same time.

The main contributions of this paper are as follows:

1. We propose a privacy-preserving protocol for utility-based routing PPUR in DTNs. PPUR can protect nodes' privacy information and collect the encounter information to calculate the real utility value at the same time.
2. We achieve the confidentiality and integrity of messages through hashing and digital signature, and then analyze the security.
3. Extensive simulations are conducted to demonstrate the efficiency of the proposed routing protocol.

The rest of the paper is organized as follows. In Section 2, we review the related work. We present the system model in Section 3. We describe the system design of the privacy-preserving protocol, PPUR, in Section 4, and the simulation results of PPUR are given in Section 5. We make conclusions in Section 6.

2. Related Work

At present, the existing privacy-preserving routing protocols in DTNs are mainly classified into the following four categories: ID privacy [8–10], location privacy [11–13], message content privacy [14–18], and routing utility privacy [19–21].

Kate et al. [8] proposed the first anonymous communication solution for DTNs and introduced a new anonymous authentication protocol as a part of it. Furthermore, they presented a security infrastructure for DTNs to provide efficient secure communication based on ID-based cryptography. Lu et al. [9] proposed a social-based privacy-preserving packet forwarding protocol, called SPRING, for vehicular delay-tolerant networks. SPRING can achieve conditional privacy preservation and resist most attacks existing in vehicular delay-tolerant networks.

Lu et al. [12] proposed the antilocalization anonymous routing (ALAR) protocol for DTNs. ALAR can protect the sender's location privacy through message fragmentation and forwarding each segment to different receivers. Benslimane et al. [13] propose a novel fully distributed and collaborative k-anonymity protocol, called LPAF, to protect users' location information and ensure better privacy while forwarding messages.

Shi et al. [14] presented ARDEN, an anonymous communication mechanism for DTNs based on a modified onion routing architecture. ARDEN uses attribute-based encryption (ABE) to specify and manage groups that may decrypt and forward messages and enhances the anonymity of the underlying communications. Guo et al. [15] proposed PSaD: a privacy-preserving social-assisted content dissemination protocol in DTNs. PSaD applies users' verifiable attributes to establish their social relationships in terms of identical attributes in a privacy-preserving way. Besides, to provide the confidentiality of contents, PSaD enables users to encrypt contents before the dissemination process and only allows users who have particular attributes to decrypt them. Cai et al. [16] proposed a data sanitization method collectively manipulating user profile and friendship relations and employing collective methods to protect against inference attacks in social networks. Zhang et al. [17] proposed

an advanced framework for opportunistic routing protocols, providing the following properties: confidentiality of the nodes' routing metric, anonymous authentication, and efficient key agreement for pairwise communication. Bakiras et al. [18] proposed a novel message-forwarding algorithm that utilizes random walks to deliver messages to their destinations. By removing the requirement to list all the intermediate nodes on the end-to-end path, the method enhances the anonymity of the underlying communications.

Miao et al. [19] proposed a privacy-preserving probabilistic prediction-based pouting (4PR) protocol that forwards messages by comparing aggregated information about communities instead of individual nodes. Chen et al. [20] proposed a distributed strategy to protect the aforementioned private information in utility-based DTN routing algorithms while still guaranteeing the correctness of packet forwarding. Magaia et al. [21] proposed an enhanced privacy-preserving opportunistic routing protocol (ePRIVO) for vehicular delay-tolerant networks. ePRIVO addresses the problem of vehicles taking routing decisions while keeping their information private; i.e., vehicles calculate their similarity and/or compare their routing metrics in a private manner using the Paillier homomorphic encryption scheme.

The above privacy-preserving protocols have been proposed to protect the nodes' privacy information, but cannot collect encounter information to deduce the real utility of utility-based routing. Chen et al. [10] proposed a protocol named FaceChange that can support both anonymizing real IDs among neighbor nodes and collecting encounter information. For node anonymity, two encountering nodes communicate anonymously. When two nodes disconnect with each other, each node forwards an encrypted encounter evidence to the encountered node to enable encounter information collection to calculate the real utility. However, the encountering information collected is real ID-based and will thus leak privacy information. A malicious node can learn other node's mobility patterns from the real ID-based encountering information.

3. System Model

As shown in Figure 1, the components of the system network model are as follows:

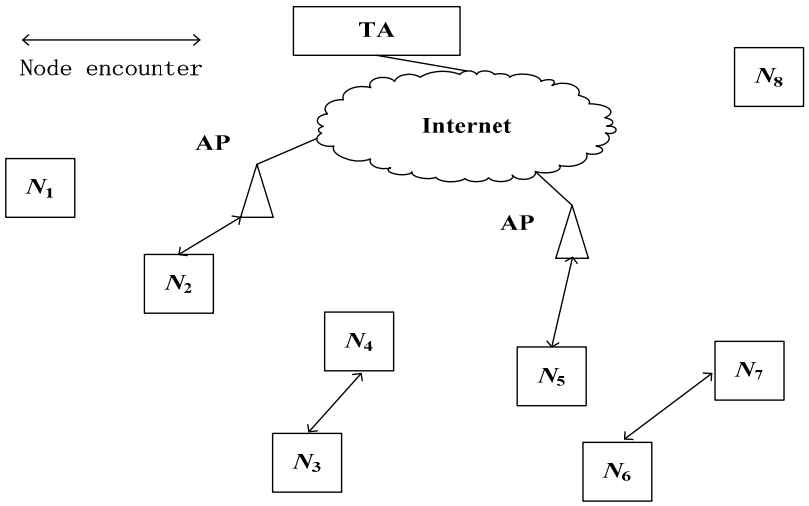

Figure 1. System model.

The trust authority (TA) has resourceful system resources and is trustable. As an authorization center, it is responsible for issuing public and private key certificates for each mobile node. In addition, it is also responsible for generating nodes' IDs and calculating routing utility value.

The fixed network, including the internet and AP (denoted by the triangle symbol in Figure 1), is responsible for connecting mobile nodes and the TA. DTN mobile nodes can obtain public and

private keys from the TA via the AP and internet. When encountering the AP, a node will send the encounter record information to the TA through the AP.

Mobile nodes N_1–N_8 denote pedestrians carrying equipment with short-distance wireless functions, such as Bluetooth and WiFi. A mobile node has one real and many pseudo-IDs. Mobile nodes acquire keys and IDs from the TA through the fixed network. They send node encounter information to the TA and obtain the routing utility value calculated by the TA.

Assuming that a utility-based routing protocol is adopted when forwarding messages, that is, when node N_i encounters another node N_j, if N_j has a higher probability to be the destination node, the message is sent to node N_j.

It is also assumed that DTN mobile nodes may launch some active attacks to modify or damage the received messages. They may also launch some passive attacks, such as eavesdropping on other nodes' IDs, routing utility, encounter time, location, and other privacy information.

4. System Design of PPUR

4.1. System Setup

TA firstly uses bilinear mapping technology to generate bilinear parameters (q, P, G_1, G_2, $\hat{e}$) with the security parameter k. G_1 and G_2 are groups of order q, P is generators, and $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ are nondegenerated bilinear mappings and can be effectively calculated. Then, the TA chooses a random number $s \in Z^*_q$ as the main key and $P_{pub} = sP$ as the public key. Finally, the TA chooses a symmetric encryption algorithm, Enc(), such as advanced encryption standard (AES), and the hash function H_1: $\{0,1\}^* \rightarrow G_1^*$, H_2: $G_2 \rightarrow \{0,1\}^n$ to publish system parameters (q, G_1, G_2, P, P_{pub}, $\hat{e}$, n, H_1, H_2, Enc()), where n is the length of the message to be encrypted.

When a mobile node N_i registers with the system, the TA generates a set of pseudo-IDs, $PID_i = [Pid_i^1, Pid_i^2, \ldots Pid_i^n]$, of N_i. A pseudo-ID, $Pid_i = Enc_s(N_i \| r)$, is generated by the symmetric encryption algorithm Enc(), master key s, and a random number r. Based on the pseudo-ID Pid_i and the node's public key $H_1(Pid_i)$, the TA generates the node's private key $sk_i = sH_1(Pid_i)$ by using the primary key s and hash function H_1 to sign the message. When communicating and signing messages, a node changes to using a different pseudo-ID after a certain period to hide its true ID. Because of having the master key s, the TA can obtain the real ID from a node's pseudo-ID and track the node to guarantee security.

4.2. Generation of Encounter Record Information for Anonymous Nodes

When forwarding messages, nodes need to calculate the utility value according to the number and time of node encounters. So, it is necessary to generate encounter record information for anonymous nodes. Assuming that two nodes N_i and N_j encounter, the encounter record information ET_{ij} will be generated as shown in Figure 2.

In the encounter record information, ET_{ij}, Pid_i, and Pid_j are the nodes' pseudo-IDs; $t_{ij}^1 \ldots t_{ij}^{n-1}$ and t_{ij}^n are the encounter time samples of nodes N_i and N_j (other information such as encounter location can be included when needed); Sig_{Pidi} and Sig_{Pidj} are the digital signatures of nodes N_i and N_j; E_{SKi} is the private key of node N_i; and H is the hash function used to generate the summary.

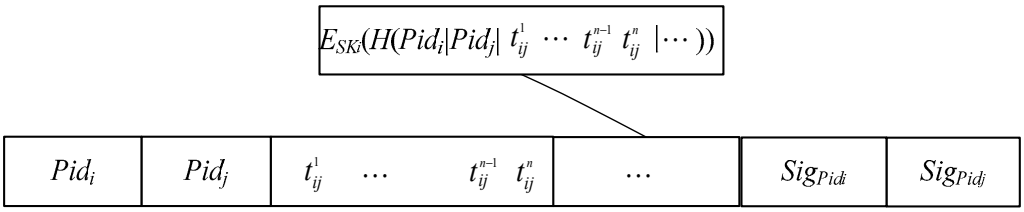

Figure 2. Encounter record information.

Nodes N_i and N_j generate the session key $\text{Key}_{ij} = \hat{e}\ (sk_i, H_1(Pid_j)) = \hat{e}\ (H_1(Pid_i), sk_j) = \hat{e}\ (H_1(Pid_i), H_1(Pid_j))^s$. Encounter record information is encrypted by the session key Key_{ij} to generate the encrypted encounter record $\text{ET}'_{ij} = E_{\text{Key}_{ij}}$ (ET) to ensure message confidentiality.

4.3. Collection of Encounter Record Information and Calculation of Real Utility Value

Nodes generate the encounter record information anonymously upon encounter. A node forwards encounter record information to the TA when connecting the AP. The TA receives the encounter record information, generates the session key, and then decrypts the information through its main key s. The TA obtains the node's real ID and then calculates the node's routing utility value according to Equation (1) in [2] (other routing utility value calculating methods can be adopted when needed):

$$U_{ij} = U_{ij(old)} + \left(1 - U_{ij(old)}\right) \times U_{init},\ 0 < U_{init} \leq 1, \tag{1}$$

where $0 \leq U_{ij} \leq 1$ denotes the new utility value of nodes N_i and N_j, $U_{ij(old)}$ is the utility value before update, and U_{init} is the initialization constant. The TA returns the utility value to the nodes. In this way, a node cannot get any privacy information except the real utility values.

If multiple pseudo-IDs only correspond to one real ID in the encounter record information sent to the TA, a malicious node can infer the corresponding relationship between the pseudo-IDs and real ID based on the returned utility value's changing result. To prevent the corresponding relationship from being inferred, TA will return the true utility value to a node only when the pseudo-IDs in encounter record information correspond to multiple real IDs. If there are k different pseudo-IDs, the probability that a node can infer other nodes' true ID from the utility value's changing result is only $1/k$.

4.4. Anonymous Message Forwarding of Encountering Nodes

Assuming that nodes N_i and N_j encounter, N_j plans to send a message m to N_i. The forwarding process of node N_i (the forwarding process of N_j is similar) is as follows:

1. For a message m, if N_i is not the destination node, it gets the utility value calculated by the TA, and then goes to step 3, or else goes to step 2.
2. Set the utility value to the max value of 1.
3. N_i compares the utility value with N_j by the solution for Yao's Millionaire Problem [22].
4. N_i receives message m if it has a higher utility value.

In step 3, N_i and N_j need to compare the utility values, but cannot know each other's real utility value. This can be solved by the solution for Yao's Millionaire Problem. Yao's Millionaire Problem is a secure multiparty computation (SMC) problem, which enables multiple participants with private data to collaborate on their private data without divulging their private information.

When N_i is the destination node of message m, if N_i receives m directly without comparing utility value, its real ID will be revealed. Therefore, in step 2, the utility value is set to the max value of 1, and the destination node N_i can receive message m anonymously by the comparing of values in step 3.

4.5. Security Analysis

We consider two types of attacks, namely passive and active attacks.

4.5.1. Passive Attack

A passive adversary (eavesdropper) may not interfere with the protocol, but instead monitors the underlying communications to get some relevant privacy information. PPUR can prevent malicious nodes from acquiring meaningful private information by overhearing the encounter record information. Firstly, the encounter record information ET_{ij} is encrypted by the session secret key Key_{ij} of nodes N_i and N_j, and the key can only be obtained by nodes N_i, N_j, and TA, so the eavesdropper cannot

understand the content in the transmitted encounter record information. Secondly, when receiving a message, if a node is not the destination node, it can anonymously compare utility values with the encountered node directly through the solution for "Yao's Millionaire Problem". If a node is the destination node, it sets the utility value to the max value of 1 and compares utility value with the solution for "Yao's Millionaire Problem", so the destination node can get the message and ensure anonymity at the same time. As a result, the eavesdropper cannot determine the ID of a node based on the messages it receives.

4.5.2. Active Attack

An active adversary may modify or damage the encounter record information. PPUR can prevent the active attack. Firstly, in PPUR, two encountering nodes generate the summary of encounter record information by the hash function, which can prevent information from being tampered with and forged, so the integrity is ensured. Secondly, the encounter record information is signed by the encountering nodes' private keys, so the signature ensures the nonrepudiation of the message.

5. Performance Evaluation

5.1. Simulation Setup

We implement PPUR on the Opportunistic Networking Environment simulator [23]. There are 40 mobile nodes in the simulation, which are divided into four groups on average. The node mobility model is a shortest path map-based movement model. In this mobile model, after choosing a destination, a node will select the path of shortest distance by which to move on the map through the Dijkstra single-source shortest-path algorithm. By default, the message generation interval is 4–8 s, message size is 100–200 KB, buffer size is 10 MB, TTL is 2 h, node movement speed is 2–5 m/s, data transmission speed is 250 KB/s, communication radius is 10 m, simulation area is 4500×3400 m^2, simulation time is 54,000 s, and warm-up time is 4000 s, assuming that there are a total of 4 APs with the locations (1795,1265), (1135,1545), (2573,1104), and (2957,2266), respectively.

5.2. Performance Comparison

PPUR is compared with the routing protocols of PROPHET [2] and FaceChange [10] to evaluate its performance. The PPUR has 1–4 APs denoted as PPUR1, PPUR2, PPUR3, PPUR4, respectively, to test the influence of the number of APs. We are interested in the following metrics for performance evaluation: message delivery ratio, average delivery delay, and overhead ratio. The delivery ratio is defined as the ratio of successfully delivered messages to total messages generated in the network. Delay is measured by the delay sum of all delivered messages divided by the number of delivered messages. Overhead ratio is defined as the ratio of the total number of forwarding to the number of delivered messages, which denotes how many times forwarding is needed to successfully deliver a message. We evaluate the influence of buffer size and TTL on performance.

5.2.1. Influence of Buffer Size

As shown in Figure 3, the delivery ratio increases as the buffer size increases for all the routing protocols. This is because nodes can carry more messages with larger buffer, and subsequently deliver more messages successfully. The delivery ratios of PPUR1, PPUR2, PPUR3, and FaceChange are smaller than PROPHET. This is because in PPUR, only when encountering the AP can nodes deliver encounter record information to TA and get the routing utility value. So, in PPUR, nodes cannot update the routing utility instantly, compared with PROPHET, leading to a slightly smaller delivery ratio. In FaceChange, as the nodes need some time to collect encounter evidence, the routing utility is not updated quickly enough to reflect the changes on meeting frequencies among nodes, leading to inaccurate guidance on routing and degraded success ratio. We also can see that PPUR4 has a similar delivery ratio to PROPHET. This is because when there are more APs, nodes have more chances to

deliver encounter record information to the TA and get the routing utility value quickly. When there are 4 APs, the delivery ratio of PPUR is almost the same or even larger than PROPHET if the buffer is more than 10 M. This is because in PROPHET, the routing utility is updated immediately after an encounter happens, which may cause it to deviate from the average utility value due to a burst on encountering nodes, leading to inaccurate message forwarding.

The impact of buffer size on delay is shown in Figure 4. It can be seen that delivery delay increases as buffer size increases for all routing protocols. This is because when buffer size increases, nodes can store and deliver more messages with longer delay, leading to the increase of average delivery delay. The average delivery delays of PPUR1, PPUR2, PPUR3, and FaceChange are smaller than PROPHET. This is because as seen in Figure 3, nodes in PPUR and FaceChange cannot update the routing utility instantly, so some messages with longer delay are not delivered. PPUR4 has a similar delay to PROPHET, and this is because nodes can update the routing utility value instantly when there are more APs and deliver more messages with larger delay.

The impact of buffer size on overhead ratio is shown in Figure 5. For all the protocols, the impact of buffer size has two aspects. On the one hand, as buffer size increases, nodes can get more forwarding chances, so the number of forwarding will increase, leading to the increase of overhead ratio. On the other hand, more messages are successfully delivered, leading to the decrease of overhead ratio. The impact of the latter outweighs that of the former, so the overhead ratio decreases. The overhead ratios of PPUR-AP1 and PPUR-AP4 are smaller than those of FaceChange and PROPHET because fewer messages are forwarded. The overhead ratios of PPUR-AP2 and PPUR-AP3 are larger than that of PROPHET because fewer messages are delivered.

From the above, we know that PPUR can achieve similar performance to PROPHET and achieve larger delivery ratio and smaller overhead ratio compared with FaceChange when having proper numbers of APs.

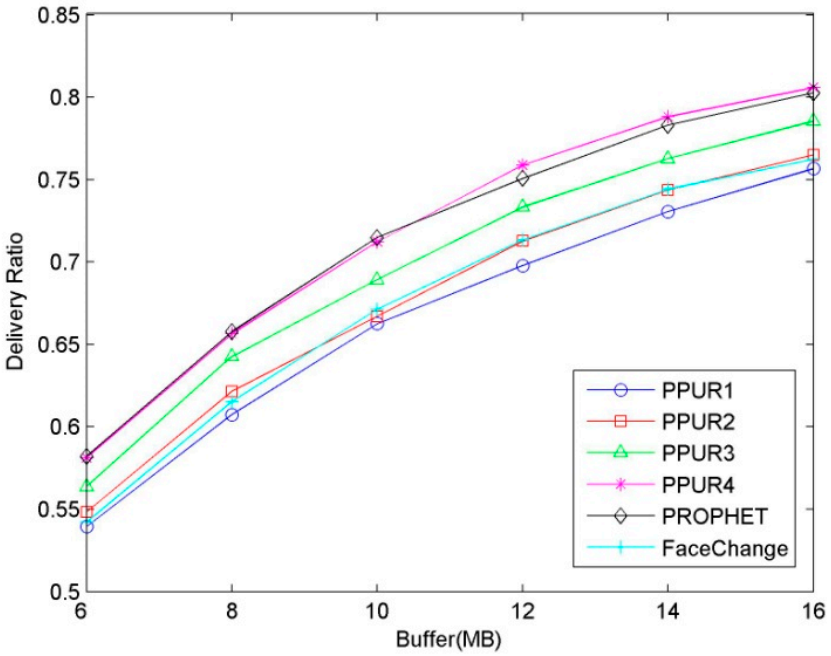

Figure 3. Delivery ratio for varying buffer size. PPUR1–4: APs 1–4 of the privacy-preserving protocol for utility-based routing (PPUR).

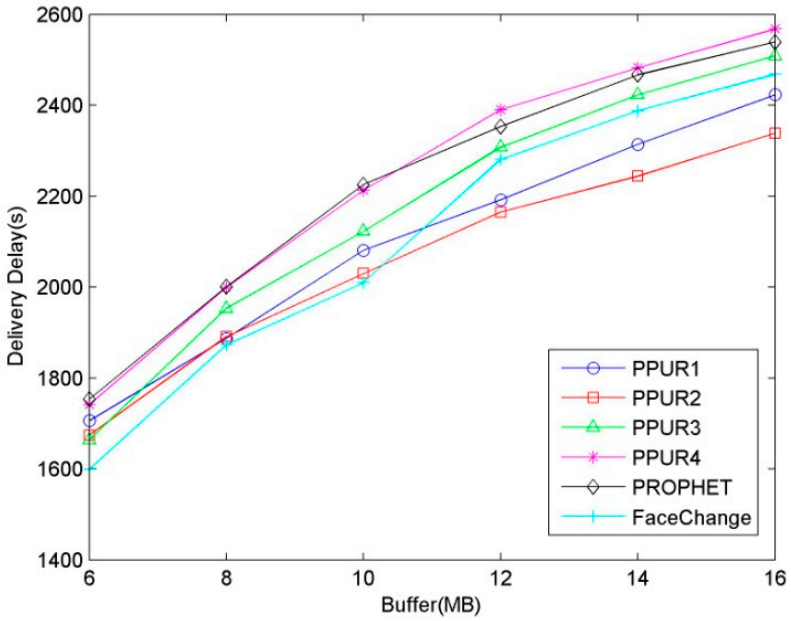

Figure 4. Delivery delay for varying buffer size.

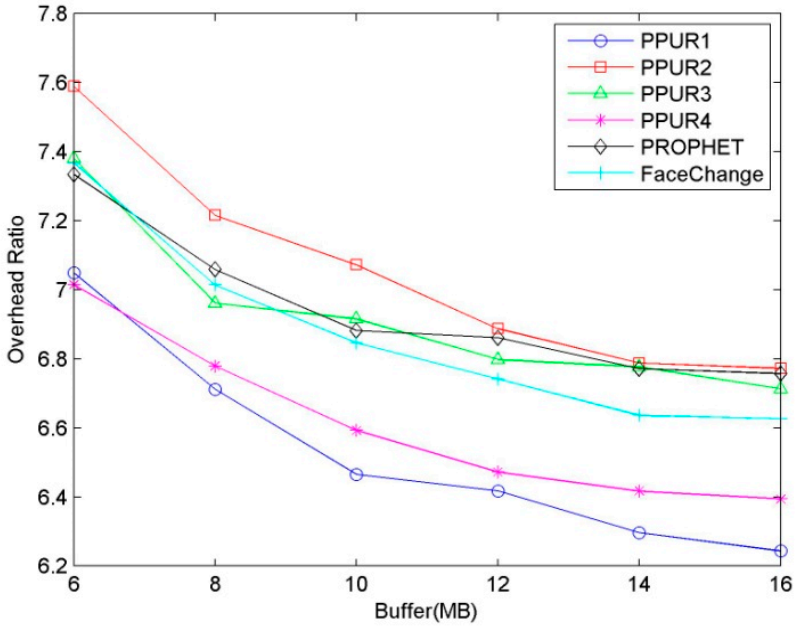

Figure 5. Overhead ratio for varying buffer size.

5.2.2. Influence of TTL

The impact of TTL on delivery ratio is shown in Figure 6. It can be seen that the delivery ratio increases as the TTL increases for all protocols; this is because the messages with larger TTL can stay longer in the buffer and have more chance to be delivered. The delivery ratios of PPUR1, PPUR2, PPUR3, and FaceChange are smaller than that of PROPHET, but the PPUR4 protocol has a similar delivery ratio to PROPHET because nodes can update the routing utility value only when encountering the TA.

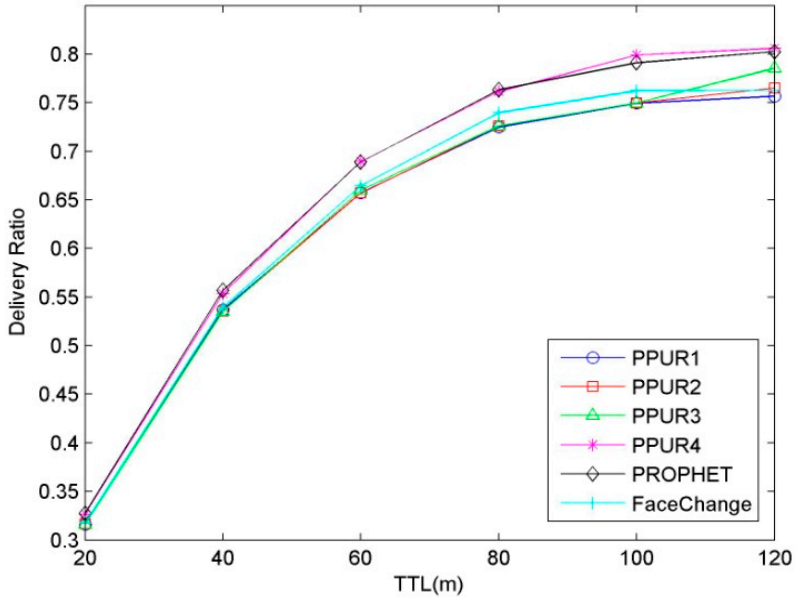

Figure 6. Delivery ratio for varying TTL.

Figure 7 shows the influence of TTL on delay. It can be seen that delivery delay increases as TTL increases for all protocols. This is because as the TTL increases, nodes can store and deliver more messages with longer delay. The delivery delay of PPUR4 is similar to that of PROPHET, and delays of PPUR1, PPUR2, PPUR3, and FaceChange are smaller than that of PROPHET.

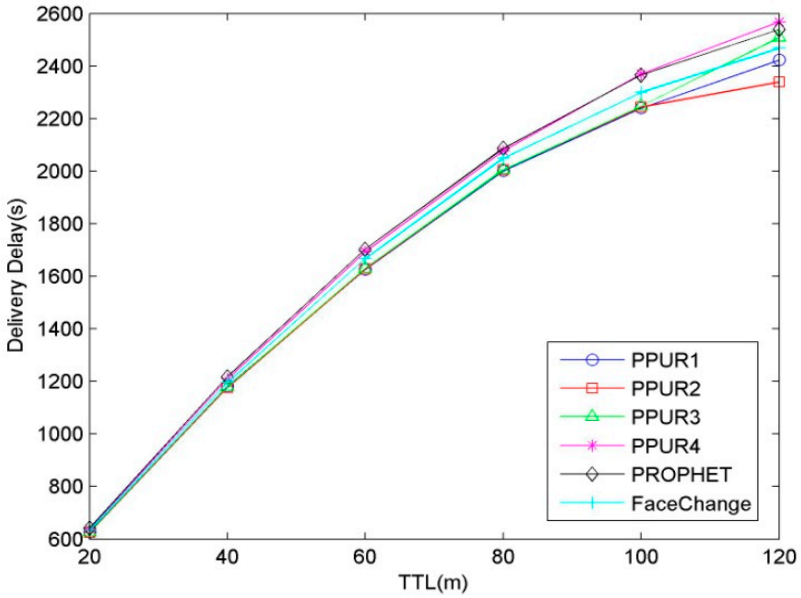

Figure 7. Delivery delay for varying TTL.

Figure 8 shows the impact of TTL on overhead ratio. For all the routing protocols, because more messages are successfully delivered as TTL increases, the overhead ratio will decrease. PPUR1, PPUR2, and PPUR3 have smaller overhead ratio than PROPHET. PPUR4 protocol has a similar overhead ratio to PROPHET and FaceChange.

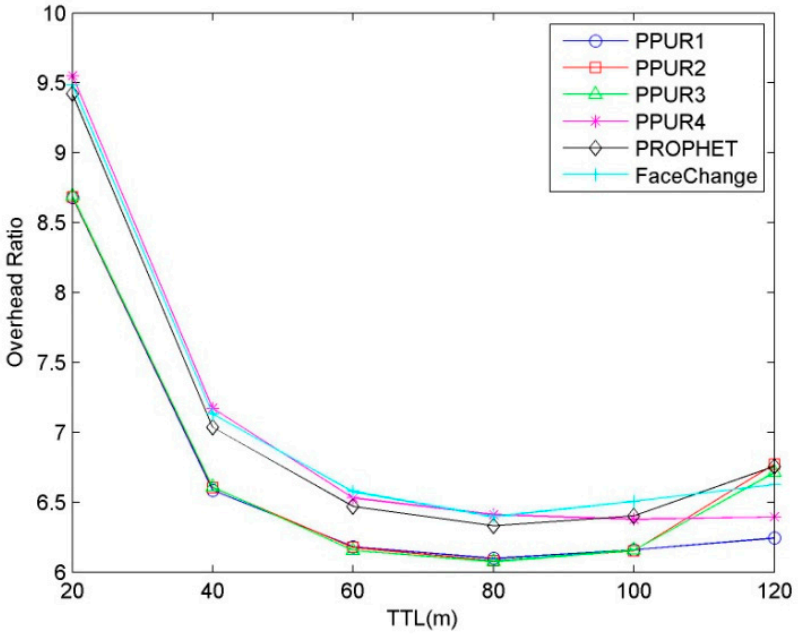

Figure 8. Overhead ratio for varying TTL.

6. Conclusions

In this paper, we have proposed a privacy-preserving protocol for utility-based routing PPUR in DTNs. PPUR can protect node privacy information and collect encounter record information to calculate the real utility value at the same time. In addition, the confidentiality and integrity of messages are ensured through hashing and digital signature. We have also verified the effectiveness of PPUR through extensive simulations. Now, this work just focuses on the privacy-preserving problem for utility-based routing without considering the selfish problem. So, our future direction is to explore a privacy-preserving incentive-aware DTN routing protocol that can stimulate nodes to cooperatively forward messages and protect node privacy at the same time.

Author Contributions: Conceptualization, methodology, Q.J.; writing—original draft preparation, K.D.; writing—review and editing, L.Z.; software, C.L.

Funding: This research was funded by the Humanity and Social Science Youth Foundation of Ministry of Education of China (grant numbers 18YJCZH068 and 17YJCZH033), The Natural Science Foundation of the Jiangsu Higher Education Institutions of China (grant number 18KJB520002), Research Start-up Fund Project of Changshu Institute of Technology (grant number KYZ2018005Q), and the Zhejiang Provincial Education Department Research Foundation of China (grant number Y201636127).

Conflicts of Interest: The authors declare no conflict of interest regarding the publication of this paper.

References

1. Fall, K. A delay-tolerant network architecture for challenged Internets. In Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03), Karlsruhe, Germany, 25–29 August 2003; pp. 27–34.
2. Lindgren, A.; Doria, A.; Schelen, O. Probabilistic routing in intermittently connected networks. *ACM SIGMOBILE Mob. Comput. Commun. Rev.* **2003**, *7*, 19–20. [CrossRef]
3. Burgess, J.; Gallagher, B.; Jensen, D. MaxProp: Routing for vehicle-based disruption-tolerant networking. In Proceedings of the INFOCOM 2006, Barcelona, Spain, 23–29 April 2006; pp. 1–11.
4. Balasubramanian, A.; Levine, B.N.; Venkataramani, A. DTN routing as a resource allocation problem. In Proceedings of the SIGCOMM 2007, Kyoto, Japan, 27–31 August 2007; pp. 373–384.
5. Hui, P.; Crowcroft, J.; Yoneki, E. Bubble Rap: Social-based forwarding in delay-tolerant networks. *IEEE Trans. Mob. Comput.* **2011**, *10*, 1576–1589. [CrossRef]

6. Elizabeth, M.; Haahr, M. Social network analysis for information flow in disconnected delay-tolerant MANETs. *IEEE Trans. Mob. Comput.* **2009**, *8*, 606–621.
7. Wu, J.X.; Huang, L.S. Homing spread: community home based multi-copy routing in mobile social networks. In Proceedings of the INFOCOM 2013, Turin, Italy, 14–19 April 2013; pp. 2319–2327.
8. Kate, A.; Zaverucha, G.; Hengartner, U. Anonymity and security in delay tolerant networks. In Proceedings of the IEEE SecureComm, Nice, France, 17–21 September 2007; pp. 504–513.
9. Lu, R.X.; Lin, X.D.; Shen, X.M. SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In Proceedings of the IEEE INFOCOM2010, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
10. Chen, K.; Shen, H.Y. FaceChange: Attaining neighbor node anonymity in mobile opportunistic social networks with fine-grained control. *IEEE/ACM Trans. Netw.* **2017**, *25*, 1176–1189. [CrossRef]
11. Zakharya, S.; Benslimane, A. On location-privacy in opportunistic mobile networks, a survey. *J. Netw. Comput. Appl.* **2018**, *103*, 157–170. [CrossRef]
12. Lu, X.; Hui, P.; Towsley, D. Anti-localization anonymous routing for delay tolerant network. *Comput. Netw.* **2010**, *54*, 1899–1910. [CrossRef]
13. Benslimane, A.; Radenkovic, M.; Zakhary, S. Efficient location privacy-aware forwarding in opportunistic mobile networks. *IEEE Trans. Veh. Technol.* **2014**, *63*, 893–906.
14. Shi, C.; Luo, X.; Traynor, P. Arden: Anonymous networking in delay tolerant networks. *Ad Hoc Networks* **2012**, *10*, 918–930. [CrossRef]
15. Guo, L.K.; Zhang, C.; Yue, H. PSaD: A privacy-preserving social assisted mobile content dissemination scheme in DTNs. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2903–2918. [CrossRef]
16. Cai, Z.P.; He, Z.B.; Guan, X. Collective data-sanitization for preventing sensitive information inference attacks in social networks. *IEEE Trans. Depend. Secure Comput.* **2018**, *15*, 577–590. [CrossRef]
17. Zhang, L.; Song, J.; Pan, J.P. A privacy-preserving and secure framework for opportunistic routing in DTNs. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7684–7697. [CrossRef]
18. Bakiras, S.; Troja, E.; Xu, X.H. An anonymous messaging system for delay tolerant networks. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–6.
19. Miao, J.W.; Hasan, O.; Mokhtar, S.B. 4PR: Privacy preserving routing in mobile delay tolerant networks. *Comput. Netw.* **2016**, *111*, 17–28. [CrossRef]
20. Chen, K.; Shen, H.Y. Distributed privacy-protecting routing in DTN: Concealing the information indispensable in routing. In Proceedings of the 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), San Diego, CA, USA, 12–14 June 2017; pp. 1–9.
21. Magaia, N.; Borrego, C.; Pereira, P. ePRIVO: An enhanced privacy-preserving opportunistic routing protocol for vehicular delay-tolerant networks. *IEEE Trans. Veh. Technol.* **2018**, *67*, 11154–11168. [CrossRef]
22. Yao, A.C. Protocols for secure computations. In Proceedings of the FOCS, Washington, DC, USA, 3–5 November 1982; pp. 160–164.
23. Keranen, A.; Ott, J.; Karkkainen, T. The ONE simulator for DTN protocol evaluation. In Proceedings of the 2nd International Conference on Simulation Tools and Techniques, Rome, Italy, 2–9 March 2009; pp. 1–10.