future internet

MDPI

Article

Efficient Privacy-Aware Forwarding for Enhanced Communication Privacy in Opportunistic Mobile Social Networks

Azizah Assiri and Hassen Sallay *

Department of Computer Engineering and Networks, College of Computing, Umm Al-Qura University, P.O. Box 715, Makkah 24382, Saudi Arabia; st43780105@st.uqu.edu.sa
* Correspondence: hmsallay@uqu.edu.sa

Abstract: Opportunistic mobile social networks (OMSNs) have become increasingly popular in recent years due to the rise of social media and smartphones. However, message forwarding and sharing social information through intermediary nodes on OMSNs raises privacy concerns as personal data and activities become more exposed. Therefore, maintaining privacy without limiting efficient social interaction is a challenging task. This paper addresses this specific problem of safeguarding user privacy during message forwarding by integrating a privacy layer on the state-of-the-art OMSN routing decision models that empowers users to control their message dissemination. Mainly, we present three user-centric privacy-aware forwarding modes guiding the selection of the next hop in the forwarding path based on social metrics such as common friends and exchanged messages between OMSN nodes. More specifically, we define different social relationship strengths approximating real-world scenarios (familiar, weak tie, stranger) and trust thresholds to give users choices on trust levels for different social contexts and guide the routing decisions. We evaluate the privacy enhancement and network performance through extensive simulations using ONE simulator for several routing schemes (Epidemic, Prophet, and Spray and Wait) and different movement models (random way, bus, and working day). We demonstrate that our modes can enhance privacy by up to 45% in various network scenarios, as measured by the reduction in the likelihood of unintended message propagation, while keeping the message-delivery process effective and efficient.

Keywords: privacy; OMSN; trust; routing; selection mode; one simulator; efficiency

Citation: Assiri, A.; Sallay, H. Efficient Privacy-Aware Forwarding for Enhanced Communication Privacy in Opportunistic Mobile Social Networks. *Future Internet* **2024**, *16*, 48. https://doi.org/10.3390/fi16020048

Academic Editor: Guan Gui

Received: 14 December 2023
Revised: 18 January 2024
Accepted: 29 January 2024
Published: 31 January 2024

1. Introduction

Mobile social networks (MSNs) facilitate communication anytime and anywhere. However, mobile devices typically connect via mobile networks, which can struggle with coverage and capacity, leading to connectivity issues [1–3]. Opportunistic networks have emerged as a solution, allowing devices to communicate ad hoc through a store-carry-forward method. Messages are held until a suitable opportunity for delivery arises, relying on the cooperation of passing devices to transport and deliver messages [4]. These developments have fostered the creation of opportunistic MSNs (OMSNs), which are deeply integrated into social life by enabling new forms of social interaction via features like texting and photo sharing. However, this convenience comes at the cost of privacy. As messages are forwarded through intermediary nodes within these networks, personal data and user activities become increasingly vulnerable to exposure [5–8]. Therefore, OMSN privacy implications must be balanced with their benefits [7,9].

The challenge lies in preserving privacy without impeding the efficiency of social interactions. Traditional routing models in OMSNs prioritize metrics such as delivery rate, latency, and network overhead, often overlooking the critical aspect of security and privacy.

Recently, there has been a great tendency to take advantage of social relationships in routing design to achieve more reliable message delivery by efficiently selecting the next

hop of message forwarding [10,11]. However, using social metrics to enhance privacy in OMSNs poses some challenges. The primary challenge is developing a system model that intelligently decides which nodes to trust with message forwarding. This involves quantifying trust using social metrics, which can be complex due to these networks' dynamic and decentralized nature. Trust can be asymmetric and context-dependent, further complicating the decision-making process. Additionally, integrating a privacy-aware solution with the legacy protocols poses the risk of altering the fundamental path construction logic, potentially affecting the network's overall efficiency. Moreover, extensive simulation and analysis are required to validate the effectiveness of privacy-preserving methods in diverse and realistic network scenarios.

In response to these challenges, the paper introduces the following contributions. Firstly, it presents a privacy layer that can be integrated into existing routing decision models, empowering users to control the dissemination of their messages. This layer is designed to be lightweight and flexible, ensuring that the core logic of path construction remains intact. Secondly, the paper proposes three user-centric privacy-aware forwarding modes that leverage social metrics to guide the selection of intermediary nodes in the message-forwarding path. These modes are tailored to approximate real-world social relationship strengths, categorized as familiar, weak tie, or stranger. They are complemented by trust thresholds that users can adjust according to social contexts. Thirdly, the paper thoroughly evaluates the privacy enhancement and network performance implications of these modes through extensive simulations using the ONE simulator. The simulations cover a range of routing schemes and movement models, comprehensively assessing the proposed solutions. The results demonstrate that the proposed privacy-aware modes can significantly enhance user privacy by up to 45% in various network scenarios, striking a balance between privacy and network performance. These contributions collectively address the pressing need for privacy preservation in OMSNs and pave the way for more secure social networking experiences.

The remainder of this paper is organized as follows. Section 2 surveys the related works. Section 3 presents our system model and methodology. Section 4 presents the proposed privacy-aware forwarding selection modes. Section 5 presents the simulation parameters and measurement metrics. Section 6 thoroughly shows the results and performance study. Finally, Section 7 discusses the results, and Section 8 concludes the paper.

2. Related Work

The key human behavior properties in mobile social networks were thoroughly identified in [12]. Social ties measure relationship strength through interaction frequency, contact time, social homogeneity (preference similarity), or social neighborhood for nodes with significant ties, while community structure represents clustered nodes linked by relationships and interests measured by a clustering coefficient describing community interconnectedness, centrality categories node importance via the number of ties, information spread speed, and location/tie importance. Bubble Rap protocol uses a community structure of social networks and forwards via central nodes having high social interaction in their communities, showing better delivery performance than the classical Prophet protocol [13]. SimBet protocol is based on nodes' similarities, the strength of ties, and the betweenness of nodes, which is the node's ability to connect nodes [14]. Dlife, a more realistic social-aware routing algorithm, monitors real social interactions of users in their daily lives by using the dynamic nodes' behavior and strength of social ties measured by contact duration between nodes for the selection of the message-forwarding carrier [15]. SocialCast routing exploits social interaction metrics using users' interests, relations strength, and mobility patterns [16]. Authors in [17] use social relations analysis to identify which data to disseminate to whom and what will be more cooperative and reliable to transmit. In [18], a social preference-aware forwarding scheme based on social information and contact probability and a buffer replacement policy for the message preferences shows a good performance with acceptable delay. Ref. [19] presents a friendship-based routing that utilizes users'

features and relationships by presenting a social pressure metric that measures friendship between nodes by their long and frequent contact during periods, ensuring a better message-delivery rate.

On the other hand, to prevent nodes' selfishness when nodes behave selfishly, i.e., to exploit the network with little or without participation in the delivery process, trustworthiness became a critical factor of each node before sharing information and establishing new relationships. In that context, ref. [20] introduced trustworthiness between nodes based on node and path trust levels to improve reliability and performance. Trust measurement uses intimacy and cooperation social metrics, along with a sliding window, to track the recent behavior of nodes and eliminate long ones in the decision of routing and message forwarding to ensure a reliable route for data dissemination. They achieved high packet delivery and transmission delay but lost the advantage when the network topology changed and became bigger. Ref. [21] improved routing adaptability and handled network selfishness by using trust degree and threshold concepts, where nodes with greater social relationships will be selected as the next hop candidate to transfer data. The trust thresholds adjust the delivery ability and deal with various network selfishness. Ref. [22] improved packet delivery based on thresholds of a composite trust, including QoS trust (connectivity and energy metrics) and social trust (cooperation degree), for next-hop message selection. This composite trust approach achieves high delivery with acceptable delay and overhead. Ref. [23] measured contact time, frequency, and regularity, so better frequent and longer contact will be more trustworthy in the delivery process. The solution achieves a better delivery ratio and delay than the classical Bubble Rap protocol.

The authors in [24] presented a trusted routing based on social similarity to deal with selfish and malicious nodes using a threshold-based approach. At the same time, ref. [25] handled misbehaving nodes using social relations to establish a trusted node list used later in routing, along with identity trust enforced by a distributed key management scheme. Ref. [26] fully utilized geographic, social, and interest features to identify optimal relay nodes for efficient data propagation. The proposed Geo-Social-Interest protocol outperforms others by selecting relays based on spatial contact patterns, social characteristics, and user interests. Ref. [27] proposed an activity-based message-forwarding algorithm that selects relay nodes and optimal paths to improve delivery ratios and reduce delays and overhead compared to opportunistic routing algorithms. Ref. [28] focused on protecting location privacy when accessing location-based services in opportunistic mobile social networks. Two obfuscation protocols that utilize social ties to anonymize user identities and locations were proposed for that purpose. Despite the proposed protocols' efficiency with higher query success ratios than existing methods by facilitating multi-hop routing through social contacts, ref. [29] tackled the problem of privacy leaks, enabling external adversaries to infer user demographics from exposed location profiles and match shared locations to real mobility traces and points of interest. The authors proposed a context-based, system-level privacy protection solution that automatically learns user preferences and provides transparent control over location sharing to address this. The two last works are limited only to the location-based service's privacy, limiting their use.

Although these works contributed greatly to the OMSN routing field, most focus on ensuring a high delivery rate with low latency and acceptable network overhead without considering security and privacy. It is also worth noting that research works explicitly tackling the privacy issues in OMSN at the routing level are rare. Therefore, privacy preservation in OMSNs constitutes a challenging issue. This paper presents lightweight privacy-aware routing schemes for OMSN by adding a privacy layer to the state-of-the-art OMSN routing decision models. This layer approximates real-world scenarios and provides user-centric message delivery according to user incentives and requirements. The proposed privacy-aware forwarding modes minimize privacy misuse while keeping the message-delivery process effective and efficient.

3. System Model and Methodology

We aim to empower users to communicate efficiently while maintaining control over their personal information, thereby fostering trust and privacy in OMSNs. Trust and privacy are indeed closely related but distinct concepts. Trust is a measure of confidence in an entity's behavior based on past interactions and social relationships. It is context-dependent and can vary across different spheres of interaction, such as personal, professional, or social. In OMSNs, trust is quantified using social metrics that help to establish the likelihood that a node will reliably forward a message without compromising the sender's intentions. Trust can be asymmetric; for example, node A may trust node B more than node B trusts node A, depending on their interaction history.

On the other hand, privacy concerns the control over the dissemination of personal information and the ability to communicate without exposing sensitive data to unintended parties. Therefore, privacy-aware routing protocols aim to ensure that messages are forwarded in a manner that respects the sender's privacy preferences, which may include restricting the visibility of messages to certain nodes based on trust levels.

Our approach considers contextual trust differentiation by using trust thresholds and relationship scores to determine the next hop for message forwarding. For example, trusting a friend socially but not professionally illustrates this concept of contextual trust. This would mean trust metrics could differ for various contexts (e.g., work, social, family). Thus, if a node is trusted in a social context but not a professional one, the trust metrics can be adjusted accordingly to prevent message propagation through that node in a work-related context. Consequently, we propose that the privacy-aware forwarding modes consider the context of the network and the relationships between nodes. This implies introducing an overarching context layer that sets parameters for different scenarios, such as work or home. Users could define their privacy preferences for various contexts, and the system would use these settings to make routing decisions that align with the desired level of privacy.

Figure 1 presents our system model to empower privacy in OMSNs. For example, if you are part of a professional network and another social network, you might set higher trust thresholds for message forwarding within your professional network. This would ensure that only nodes (colleagues) with a strong professional trust relationship with you would be selected to forward sensitive work-related messages. Conversely, you might opt for a lower trust threshold for social messages, allowing more nodes (friends) to participate in forwarding nonsensitive messages.

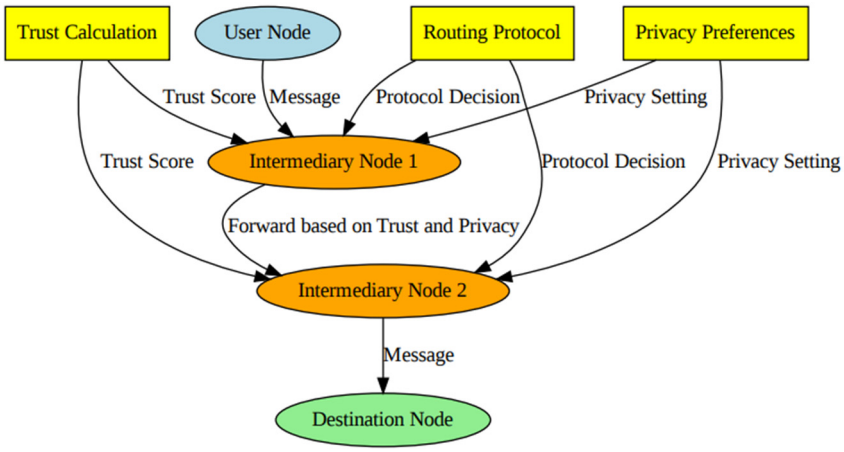

Figure 1. System model overview.

For efficiency purposes, the proposed privacy-aware solution is integrated into existing routing algorithms without affecting the overall path construction logic; thereby, users have the flexibility to define their privacy needs in various social contexts, which would be respected during the message-forwarding process.

To implement this model-enhancing privacy in OMSNs, the methodology shall provide a comprehensive approach from conceptualization to validation. Therefore, our methodology can be distilled into three clear steps: (1) privacy-aware mode development, (2) simulation and implementation, and (3) evaluation and performance study. The first phase involves the creation of a theoretical framework that defines the privacy challenges and formulates the privacy-aware forwarding strategies. It includes developing trust models and algorithms that will enable nodes within the network to make informed decisions about message forwarding based on predefined privacy preferences.

The formulated strategies are translated into practical algorithms and implemented within a simulated OMSN environment in the second phase. This step is critical for testing the feasibility and effectiveness of the privacy-aware forwarding strategies under controlled conditions. It involves setting up simulations that mimic real-world user mobility and interaction patterns, allowing for data collection on how the strategies perform across various network scenarios.

The third and final phase focuses on analyzing the collected data to assess the performance of the privacy-aware forwarding strategies. This phase thoroughly examines the strategies' impact on privacy preservation and network efficiency. This final phase ensures that the methodology addresses the theoretical aspects of privacy in OMSNs and stands up to practical scrutiny.

4. Privacy-Aware Selection Modes

In real situations, people need to meet each other to communicate directly and privately with whom they trust. They will pass by a third party to deliver their messages if there is no way to meet. Therefore, they must conveniently select the intermediates to ensure reliability and privacy. Therefore, selecting the next hop considers a trust factor in the forwarding decision and chooses nodes with the highest trustworthiness. Thus, adding a privacy layer integrating dedicated policies in the routing decision process will prioritize the selection of trusted intermediary nodes in the routing path and enhance privacy from source to destination. We propose three different selection methods for that layer, enhancing message privacy on the top of the routing schemes. Mainly, the nodes run the common, well-known routing of any OMSN algorithms that optimize reliability and efficiency. When it decides to pass a message, it checks the privacy required conditions according to the proposed modes. The following section details the trust model and the three routing selection modes.

4.1. Trust Model

The social relationships between mobile users are the main element that defines the meaning of privacy; they can vary from weak to strong ties depending on the context or the location of the opportunistic network. Variant social metrics can determine this relationship, including profiling similarity, number of encounters, number of common friends, distance count less than six in the six-degree theory, centrality, etc. Considering n common countable social metrics between two nodes A and B, we calculate the trust between two nodes A and B by the following weighted equation:

$$Trust(A,B) = \sum_{i=1}^{n} \left(\alpha_i \frac{\text{Metric}_i(A,B)}{\max(\text{Metric}_i(A,*))} \right) where \sum_{i=1}^{n} \alpha_i = 1 \quad (1)$$

Equation (1) states that the trust score is calculated with n social metrics; for each metric and node, we evaluate this metric for its neighbors ($*$ nodes) (depending on the node coverage zone). When the node has no relation regarding that metric, the metric will not be considered. The node with the maximum value will take a full trust value and constitute the reference node for that metric. Accordingly, any node will be rated according to that reference node for that specific metric. The total score will be weighted by α_i to combine the metrics and tune their impact on the trust score.

In this paper, we experiment with the trust score for two metrics:

1. Number of Common Friends (NCF)—counts how many common friends two nodes have. Higher NCF indicates a stronger social tie. The value ranges from 0 (no common friends) to (network size—2) (maximum possible common friends).
2. Number of Exchanged Messages (NEM)—counts previous messages between two nodes. Higher NEM indicates a better relationship. Value is 0 for no prior exchanges or a positive number x for x messages exchanged in the past.

Then, the trust scores using only the *NCF* metric, only the *NEM* metric, or the *NCF* and *NEM* metrics jointly between two nodes *A* and *B* are calculated, respectively:

$$Trust(A,B) = \frac{NCF(A,B)}{max(NCF(A,*))} \tag{2}$$

$$Trust(A,B) = \frac{NEM(A,B)}{max(NEM(A,*))} \tag{3}$$

$$Trust(A,B) = \alpha_1 \frac{NCF(A,B)}{max(NCF(A,*))} + \alpha_2 \frac{NEM(A,B)}{max(NEM(A,*))} \tag{4}$$

α_1 and α_2 are weights in [0–1] to tune metric impacts, $\alpha_1 + \alpha_2 = 1$, and the trust score range is [0–1].

The calculated score represents the tie strength between two nodes. We note firstly that the trust scores are directional—node A's score for B may differ from B's score for A. Secondly, a higher score indicates stronger trust/familiarity, and thirdly, thresholds are defined to classify relationships as stranger/weak tie/familiar. When we use one single metric approach, we simplify the trust calculation, while the combined metrics provide more fine-grained scoring to distinguish different relationship strengths. Both help nodes determine social trust with peers during routing. Using this score, we define three relationship strength levels using thresholds: (1) stranger, (2) weak tie (acquaintance), and (3) familiar. Therefore, a higher score means stronger social ties and higher trust between nodes and vice versa. The thresholds help qualify trust levels like strangers, acquaintances, and close friends. Each node stores NCF and NEM values for every other node locally and updates them continually. This information is used during message forwarding to pick trusted next hops and enable private routing.

4.2. Privacy-Aware Selection Modes

Based on the previous trust model, we propose three different next-hop selection methods to allow routers to better preserve message privacy during forwarding. These selection modes are integrated into existing routing algorithms without affecting overall path construction logic. Before passing a message copy to neighbors, the privacy process checks if nodes meet the defined familiarity/trust conditions and prioritizes them in the selection process. By proceeding so, we support diverse privacy needs in social contexts.

4.2.1. Trust Threshold-Based Selection Mode

This next-hop selection mode is based on defined trust thresholds. Nodes prioritize neighbors above a configured minimum trust level to forward to (see Figure 2a). Indeed, each node calculates a relationship score (e.g., using the number of common friends metric) with each neighbor. This score represents the strength of social ties. Trust thresholds are then defined to determine whether a neighbor is sufficiently trusted to relay messages. A node selects the next hop during message forwarding if its relationship score exceeds the defined trust threshold—a high threshold like 0.8 means picking strongly tied nodes across the entire message path for high privacy. A lower threshold like 0.3 allows the selection of even weak tie neighbors, improving message spread but reducing privacy. The threshold can be tuned based on different social contexts and privacy needs—from allowing only the most trusted friends to relay messages to allowing even strangers to do so. This flexibility helps address diverse real-world scenarios. A simplified trust evaluation using just a single

defined threshold to classify neighbors as "trusted" or "not trusted" allows us to address different social privacy requirements.

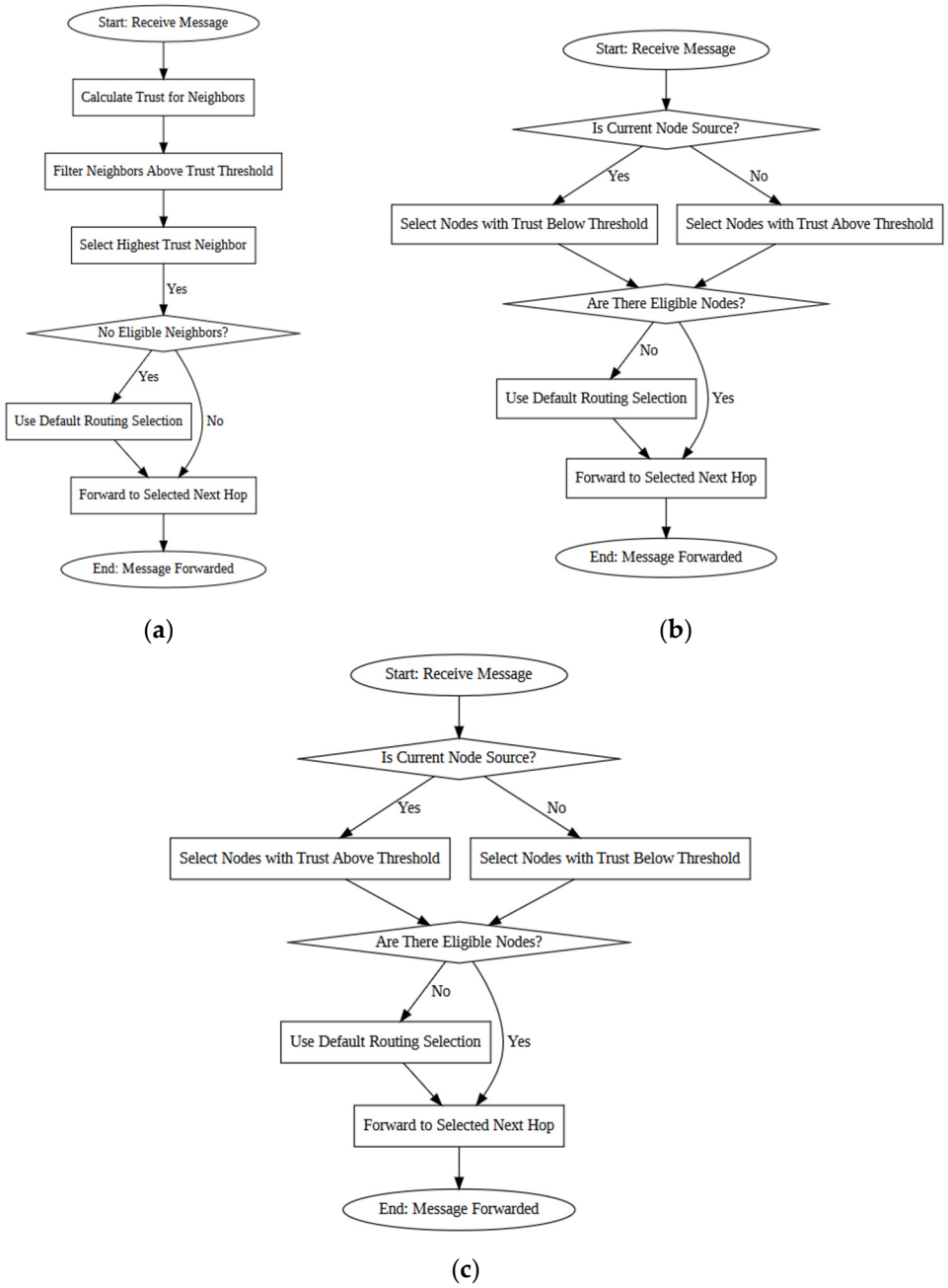

Figure 2. Privacy modes' flowcharts (**a**) for the trust threshold-based mode, (**b**) for stranger then familiar selection mode, and (**c**) for familiar then stranger selection mode.

4.2.2. Stranger Then Familiar Selection Mode

This next-hop selection mode addresses complex social situations where privacy needs vary. Nodes forward to least familiar/trusted neighbors to maximize anonymity (see Figure 2b). Indeed, the selection is based on categorizing node relationships as "stranger", "weak tie", or "familiar" by user-preferred thresholds based on NCF and NEM metrics. Multimetric scoring allows for the handling of more complex privacy needs than binary trust thresholds. The "stranger then familiar" method acts as follows:

1. The source node selects initial hops that are strangers or weak ties to maximize anonymity.

2. Subsequent intermediary nodes prioritize familiar, well-connected neighbors to relay messages.

This mode ensures the originator can hide messages from known people by routing through strangers first, and the intermediaries protect privacy by passing them to trusted parties later, who will probably be strongly unfamiliar to the sender since they are familiar with the chosen stranger node. Therefore, this approach suits social contexts where sources want privacy without involving familiars, while intermediaries only rely on trusted parties. Moreover, it is suitable when sources want to hide messages from familiars but do not mind strangers receiving copies.

4.2.3. Familiar Then Stranger Selection Mode

The "familiar then stranger" next-hop selection mode acts as follows:

1. The source node first selects a familiar, well-trusted neighbor to start message forwarding.
2. Subsequent intermediary nodes prioritize strangers to relay messages to further restrict propagation.

This approach suits contexts where sources want to limit spread beyond the community. To limit sender recognition, the user will choose a trusted node to forward, and this one chooses a stranger from his neighbors to maximize the probability of not being familiar to the sender but to any relay node in the path (see Figure 2c). This mode can be applied in a context where the sender is a well-known person and has an important number of social bonds. He wants the nodes carrying his information to be strangers to each other to avoid their discussion or disclosure. As before, relationship scores are calculated using two metrics—the number of common friends and exchanged messages. The scores divide nodes into stranger/weak ties/familiar ranges. This method limits propagation by leveraging the source's trusted ties while intermediaries route through strangers. It prevents messages from spreading among the source's trusted contacts. The multi-metric scoring and thresholds support more complex notions of familiarity and trust than binary selections.

In all modes, the existing routing logic stays unchanged. Only the final next-hop selection decision is modified to enforce privacy policies by prioritizing nodes satisfying the mode to be selected. Indeed, when the node cannot find relay nodes satisfying the selection mode criteria, its common routing strategy proceeds to balance the message privacy preservation and delivery time. Proceeding like so allows privacy preservation integration without affecting the overall routing. The selection modes support diverse social situations and privacy needs—from high confidentiality to anonymous transmission and restricted propagation. The next section evaluates these modes through simulations for different sample scenarios.

5. Simulation Characterization

In this section, we contextualize our simulations. We present the simulator used. The OMSN used routing algorithms and movement models. We then define our metrics for privacy and introduce the performance metrics used in this analysis. Finally, we present the simulation parameters and their values.

5.1. Simulation Context

We used the opportunistic network simulator ONE to evaluate proposed approaches and their performances, their impact on network efficiency, and the improvement of user privacy [30]. It is a well-known simulator designed to evaluate OMSNs and delay-tolerant networks in general. The simulator integrates principal opportunistic routing schemes and movement models, making network scenarios more realistic. We selected three routing algorithms (Epidemic, Prophet, and Spray and Wait) and three movement models (random way, bus, and working day) for the simulation scenarios.

5.1.1. Routing Algorithms

The Epidemic routing approach [31] is one of the first schemes and is commonly used as a benchmark for most routing protocols in opportunistic mobile social networks (OMSNs). It relies on continuous flooding where all nodes can act as first senders or re-layers of messages. When nodes encounter each other, they exchange message vectors to identify new messages to exchange copies of. This achieves high message-delivery rates when node buffers are unlimited, but performance deteriorates when buffers are limited, as messages are dumped due to insufficient memory. To control the flooding, some variations set conditions before transferring messages, like n-epidemic, which requires a node to have at least n neighbors before relaying.

Prophet is a prediction-based routing approach that relies on two main metrics: predictability of message delivery and transitivity in forwarding decisions [32]. It uses delivery probability to indicate how likely node A is to deliver a message to a destination node B when encountering each other. Nodes that meet more frequently have higher delivery probabilities. When nodes do not meet for a while, the probability decreases. It also uses transitivity—if A meets B and B meets C, then C is a more forwardable node. When two nodes meet, they exchange message lists and identify new messages. The message is copied and transferred if the new encounter has a better delivery prediction for a destination. This ensures efficient overhead and resource usage by intelligently calculating delivery predictability.

The Spray and Wait routing [33] approach limits flooding by controlling the number of copies per message, similar to Epidemic routing but with two phases to balance flooding with directed propagation: a spray phase, where a source node spreads L message copies to the first L distinct nodes encountered, and nodes with copies can further spread to other nodes without copies, and a wait phase, where once a node only has one copy left, it switches to direct transmission, only forwarding the copy to the destination when encountered. Its main advantages are simplicity, low latency, and overhead, while disadvantages include a lower delivery ratio than other flooding protocols.

5.1.2. Movement Models

Movement models are defined in ONE simulator to emulate different kinds of travel. We applied the random waypoint, bus movement, and working day models to the simulation. The random waypoint movement model defines random positions and destinations for different hosts. Then, each node will move straight from its current position to the next one. In the bus-based model, users should travel together in a bus with a predefined line of movement and a fixed number of stations. The bus travels from the beginning of its line and stops regularly at each station until it reaches the end of the line. Each host's random probability is generated to define when it can board or alight the bus. The last model is the "working day". It represents a typical daily routine. People start at home, walk to work offices, or drive cars. At offices, they can be stationary and later move in the same "building" from one position to another to simulate their habitual walking between offices. Coffee breaks are also generated randomly. At the end of the working shift, people can go home directly or decide to go shopping or to any entertainment places. During different periods of the day, many encounters can happen. A single person can meet his coworkers in the office and later some friends to have a drink.

5.2. Simulation Metrics

5.2.1. Privacy Metrics

We define the privacy awareness ratio (PAR) metric that rates the number of privacy-aware nodes in the forwarding path for any message between source A and destination B. By privacy-aware node, we mean a node that uses one of the three proposed routing selection modes previously defined. This contrasts the privacy-unaware node, which proceeds in its default routing selection setting (Epidemic, Prophet, and Spray and Wait) without involving the three proposed selection modes. We stated that in the privacy-aware

routing, we enforce privacy policies by prioritizing nodes satisfying the node policy to be selected. When the node cannot find relay nodes satisfying the selection mode criteria, it proceeds with its common routing strategy to balance message privacy preservation and delivery time. Let n be the total number of selected privacy-aware nodes in the path between A and B and N be the total number of nodes constituting that path; then, PAR is calculated by:

$$PAR_{policy}(A, B) = \frac{n}{N} \quad (5)$$

PAR equals 1 when all intermediary hops successfully enforce the privacy-aware selection policy on all the path nodes. When we use routing algorithms without privacy policy enforcement, we can determine that the PAR can be 0 or greater than 0 since it can unintentionally select trust nodes when constructing the path between A and B. Therefore, we compute the privacy enhancement ratio (PER):

$$PER = \frac{PAR_{with-privacy} - PAR_{without-privacy}}{PAR_{without-privacy}} \quad (6)$$

5.2.2. Performance Metrics

For the performance evaluation, we used the following metrics:

- Energy Consumption: the consumed energy ratio during running time for routing with and without the defined privacy-aware modes. We aim to compare needed energy in privacy-aware routing versus privacy-unaware routing schemes. We set energy model parameters in the ONE simulator to initial energy = 72,500 (equivalent to typical mobile phone battery capacity), scan energy = 1, transmit energy = 1, and scan response energy = 1.
- Packet Delivery Ratio (PDR): the ratio of total packets delivered to the total packets transmitted across from source to destination nodes. It measures the rate of delivered messages in the whole network. It will show if privacy enhancement positively or negatively affects the number of successfully delivered messages.
- Average Transmission Time (ATT): measuring the average time needed to transfer a message to a destination. We will compare privacy-aware routing to normal routing to measure the possible delay introduced.
- Packet overhead: measures how many packets are used in the whole running time to identify the impact of privacy modes on message delivery.

5.3. Simulation Parameters

Table 1 presents the common parameters for all our experiments. First, we vary network size from 40 to 300 hosts to simulate small to large groups of network users with random walk and bus movement models. We vary node numbers from 120 to 200 hosts for the working day model. Each host is equipped with two mobile interfaces: Bluetooth and Wi-Fi. This configuration accurately depicts people using their mobile devices during their daily routines. Simulated space is defined in two different ways. The first case (1000 m, 1000 m) represents a small to medium city square or campus building where people gather or move for different purposes like social events, meetings, daily routines, or attending conferences. We simulated the amount of 1-h networking usage with this type of zone. The second case (10,000 m, 8000 m) outlines a large movement zone like a whole city or a village. It is suitable to simulate people during an entire working day. They will be moving from home to work/office to entertainment places or shops and back to their homes at the end of the day. Thus, with this kind of space, we set the duration of the simulation scenario to 10 h. To simulate host communication, we use a random uniform generator. It chooses randomly based on a uniform distribution couple (source, destination) and exchange events. So messages will be sent from sources to destinations during the whole scenario duration and covering the entire simulated zone.

Table 1. Simulation parameters and values.

Simulation Parameter	Value
Simulation Time	1 h, 10 h
Simulation Space	1000 m × 1000 m, 10,000 m × 8000 m
No. of Nodes	Variable from 40 to 300 nodes
Interfaces	Wi-Fi + Bluetooth
Bluetooth Interface	10 m with 250 k
Wi-Fi Interface	1500 k, 2500 k, 4500 k, 6000 k, 6750 k
Node Buffer Size	5 MB
Size of Message	500 KB–1 MB
Message TTL	300 min
Routing Protocol	Epidemic, Prophet, Spray and Wait
Mobility Model	Random Way, Bus, Working Day

6. Results

In this section, we detail the results of each approach and compare recorded enhancement in different routing algorithms. We then discuss those results and their impact on privacy preservation and performance.

6.1. Trust Threshold-Based Selection Mode

In this experiment, we use three routing algorithms (Epidemic, Prophet, and Spray and Wait), three movement models (random way, bus movement, and working day), and three defined trust threshold values (30, 50, and 80). The combination of those parameters generates different cases. We experiment with 27 scenarios. For each case, we also run its equivalent using the normal routing version to compare them. We organize the presentation of simulation results based on trust thresholds, movement models, and routing protocols.

6.1.1. Results Using Trust Threshold 30%

- Random waypoint movement model

Figure 3 shows that the privacy enhancement rate provided by the mode on the routing is almost the same.

Using a low score limit of 30% allows the routers to select a large number of next hops as a relation score with the origin. More specifically, the Prophet and Epidemic routing show the same improvement. In the Epidemic, privacy preservation has been improved by 45% with different network sizes. It means that the intermediary routers can choose the next hop with stronger ties than the normal version in the privacy-aware version of the Epidemic protocol. In Prophet, the results are the same as the experiment with the Epidemic routing. A lower restriction in the selection method leads to modest privacy enhancement. Then, "Spray and Wait" maintains a stable rate, while other protocols show a small degradation until reaching 10% with a larger network. The "Spray and Wait" protocol controls the number of allowed copies of the transmitted message. Thus, even if the threshold is low and the network becomes more crowded, the routing decision keeps a high enhancement rate for the origin sender.

For network efficiency values, the packet delivery ratio (PDR) and the average transmission time (ATT) vary according to the routing scheme, while the energy consumption is not affected. The remarkable difference is due to the specification of each algorithm. Spray and Wait limits the forwarding copies and surveys the reception by destination, resulting in a better delivery ratio and longer transmission time. The Prophet protocol is an enhanced version of the Epidemic protocol. It uses its predefined probabilities to improve forwarding, providing better PDR but not reducing the transmission time. Epidemic shows a small difference in the measurement of ATT between the two routing versions. Adding the selection in the forwarding process forces the routers to apply the privacy mode and check for candidates. Therefore, the average transmission time will be greater than the time in the normal version.

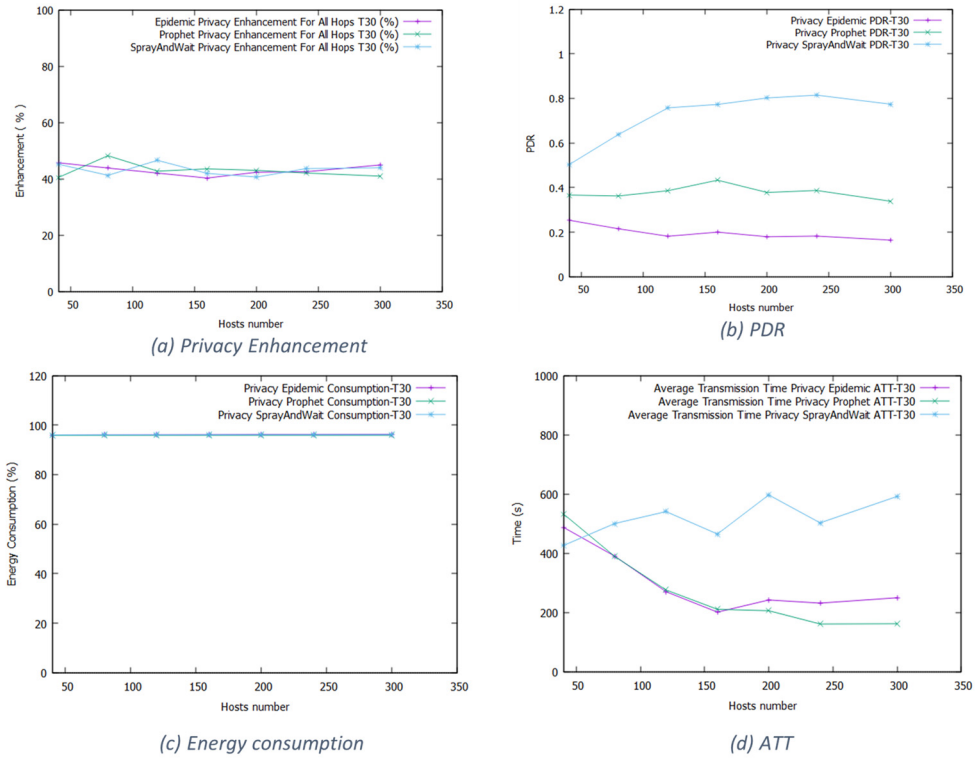

Figure 3. The result of trust threshold 30% and random way movement model.

- Bus movement model

Figure 4 shows the results using the bus movement. It confirms the previous outcomes. In Epidemic and Prophet, the privacy improvement reaches 45% for all hops, while in Spray and Wait, it reaches 55%. The enhancement is larger for the Spray and Wait protocol than the two other protocols because Spray and Wait controls the number of allowed copies of the transmitted message (i.e., is more selective), and then even if the network becomes more crowded, the routing decision keeps a high enhancement rate for the origin sender. For network efficiency parameters, we can see Spray and Wait routing generates a better rate for PDR and even provides very low packet overhead while having the highest ATT metric values. All three protocols maintain the same energy level consumption and improvement rate for intermediary nodes. The study confirms again that the privacy enhancement depends on the threshold value without affecting the network stability.

- Working day movement model

This model emulates larger space (10,000 m, 8000 m) and longer time (10 h) than the two previous models. Figure 5 shows the result for the working day movement model. The specifications of this model, with long duration and wide space, mean that the opportunity to meet new mobile nodes is very low. Thus, it is harder for routers to find various forwarding possibilities. Consequently, despite the routing scheme, the results will be the same. Epidemic shows that privacy-aware routing versions generate 40% with a small network size. It reaches 60% with medium size, then slows down with larger size. We explain this behavior by the large space and longer amount of time used by the working day model. Thus, it will be more difficult to find candidates' nodes able to fulfill the selection method for privacy preservation.

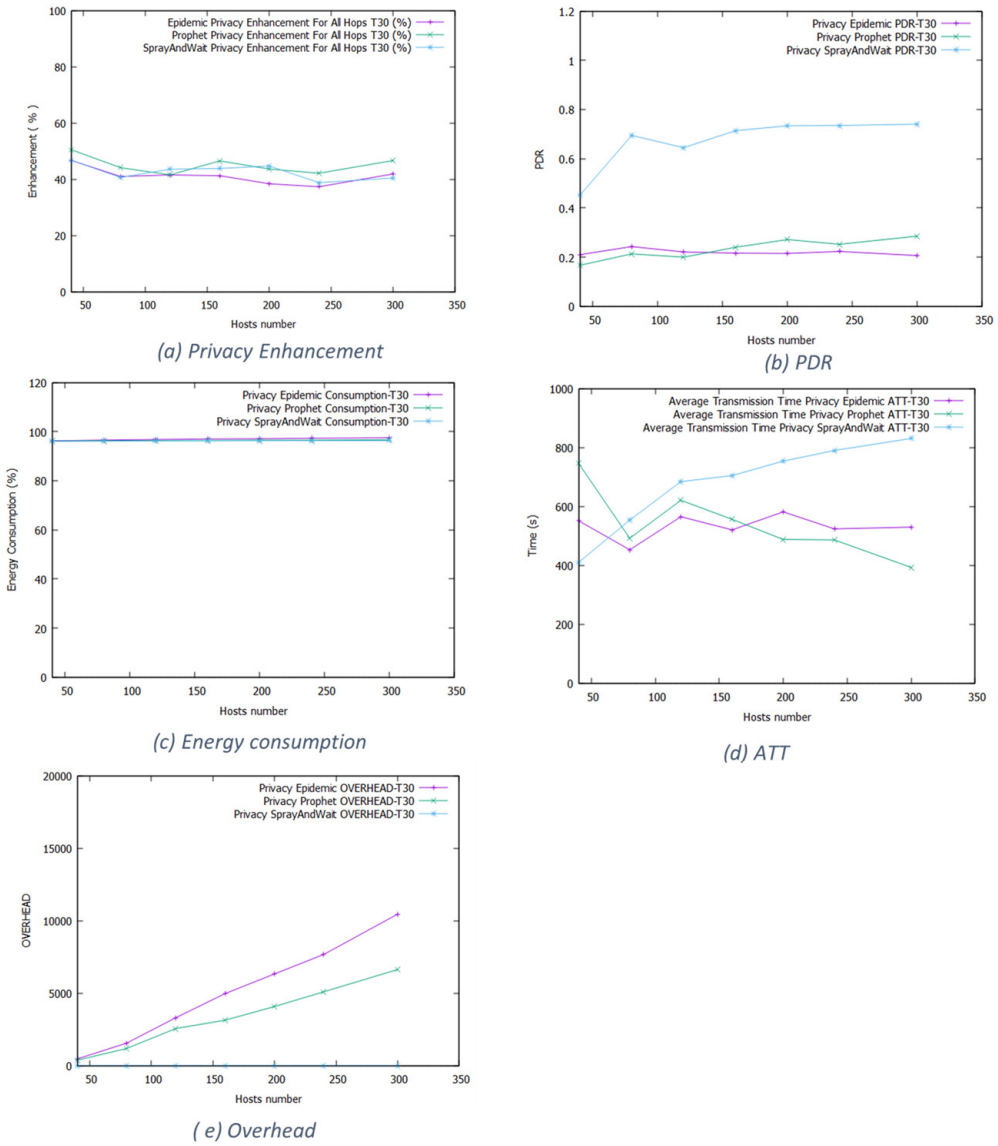

Figure 4. The result of trust threshold 30% and the bus movement model.

The enhancement increases with medium-sized networks (65% for 160-sized networks), but when the number of hosts overpasses 160 nodes and a threshold (30%), intermediary routers select more hosts with low relation scores, which decreases privacy enhancement. This is also true for Prophet and Spray and Wait protocols. For all of them, the network efficiency is lightly affected.

6.1.2. Results Using Trust Threshold 50%

- Random waypoint movement model

Figure 6 presents the result with the random way model. The routing schemes maintain the same behavior. More specifically, using a threshold of 50% forces mobile nodes to select closer hosts, resulting in better privacy preservation. A larger network means more opportunities for message forwarding. Therefore, the probability of meeting good candidates who satisfy the privacy preservation criteria increases with the number of hosts in the network. We observe a 100% enhancement in privacy with minor degradation in the network performance except for the transmission time for Epidemic and Prophet, which slightly increased due to the restriction about relaying nodes. Spray and Wait gives the best packet delivery rate with a distinct weakness in its delivery time.

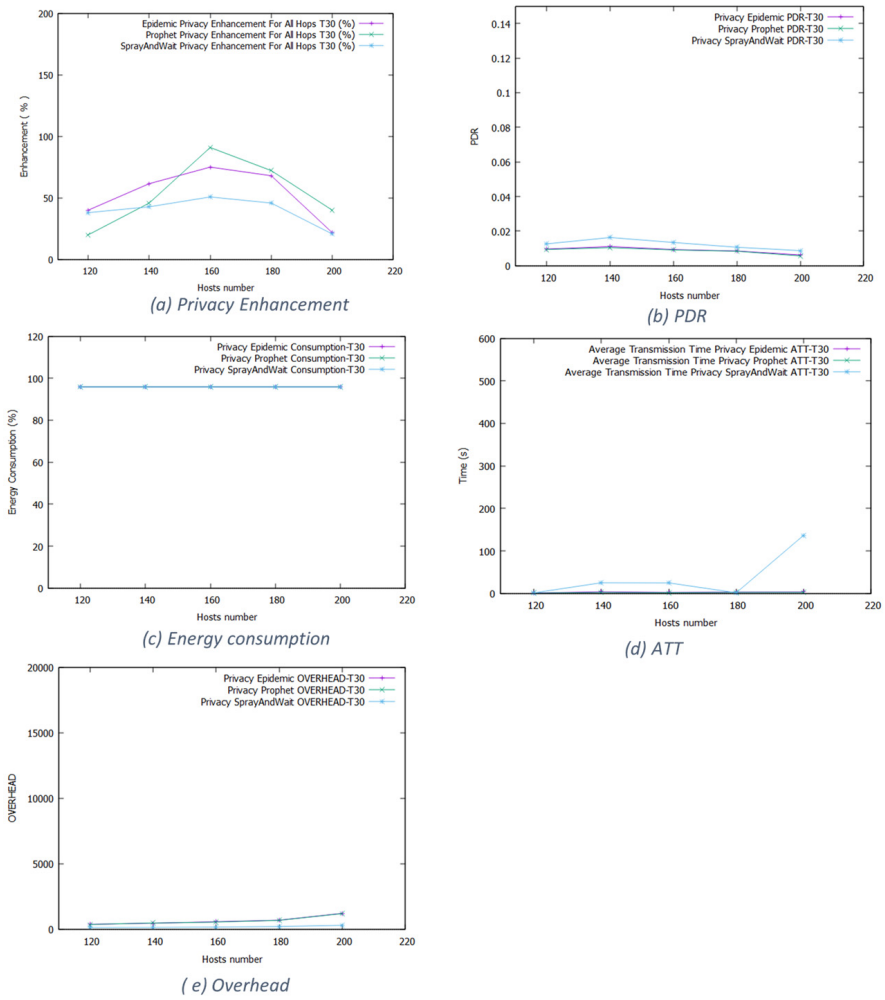

Figure 5. The result of trust thresholds 30% and working day movement model.

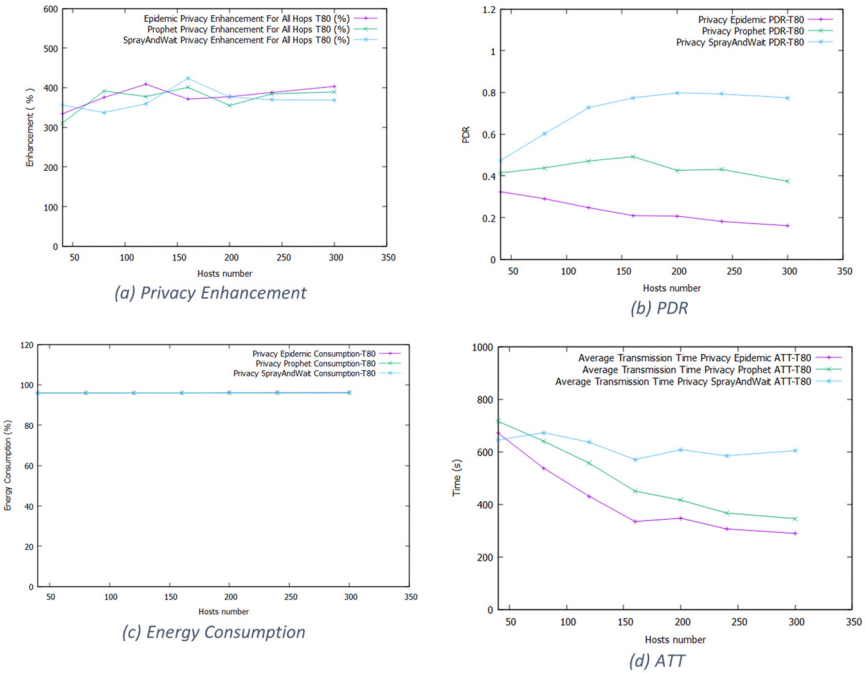

Figure 6. The results of thresholds 50% and random way model.

- Bus movement model

Figure 7 shows the results for the movement bus model. Prophet and Epidemic behave the same, while the Spray and Wait protocol keeps the highest performance. They gain 100% privacy preservation with minor degradation of network performance. Spray and Wait gives the best packet delivery rate with a distinct weakness in delivery time, while Epidemic has a high overhead with a larger network.

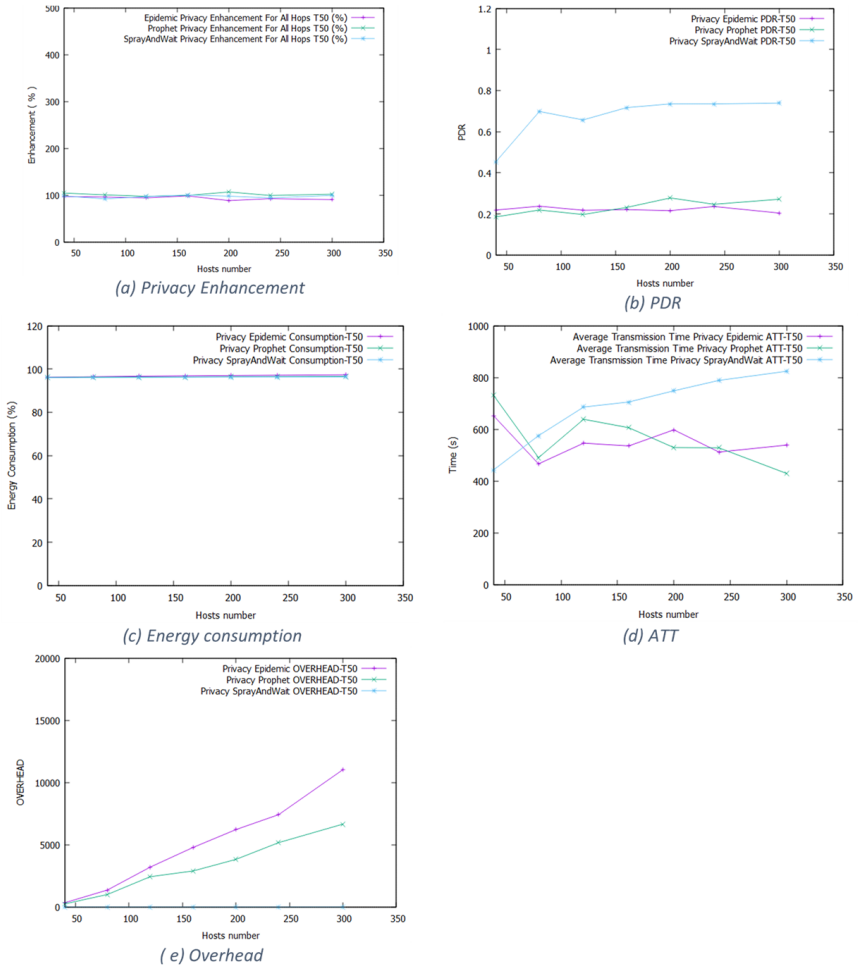

Figure 7. The result of thresholds 50 and bus model.

- Working day movement model

Figure 8 shows the results for the working day movement model. We observe that Epidemic's privacy is improved by 140% with a small-size network and goes down to 50% with a medium size. Then, it rises again with a larger network. The large space and longer time scenario narrows the opportunities to encounter new mobile nodes when the network contains few users. Also, the high threshold hardens the next hop choice. While the Prophet protocol has low improvement with a small network, it becomes better with medium sizes. The three protocols become closer to each other when the network overpasses 180 with acceptable network performance. The higher threshold combined with the Prophet probabilities of success increases the privacy protection rate.

6.1.3. Results Using Trust Threshold 80%

- Random way movement model

Figure 9 shows that the higher the relationship score threshold, the better the privacy enhancement rate will be. For all the algorithms, there is a very good enhancement in

privacy. Still, as expected, with a degradation in network performance metrics, mainly the ATT transmission time, a high threshold prevents the intermediary routers from choosing bad-quality hops, which leads to a longer forwarding time.

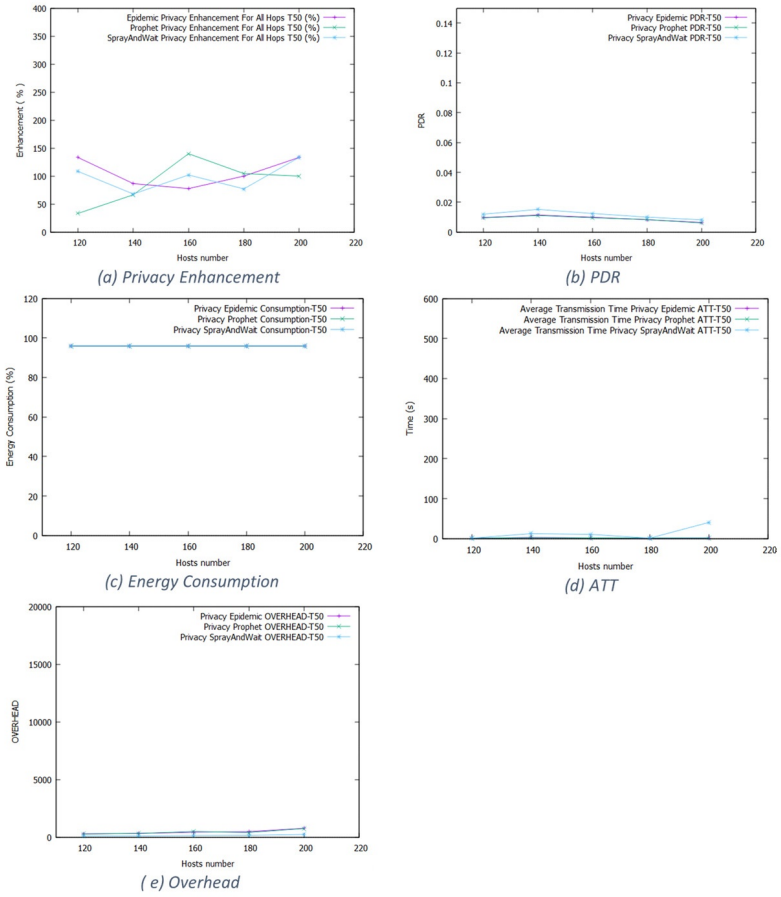

Figure 8. The result of thresholds 50 and working day.

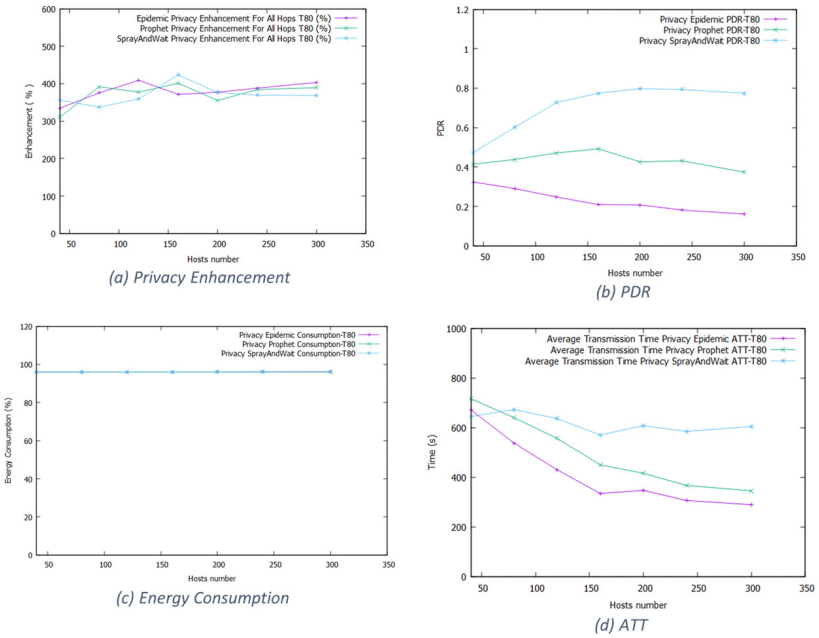

Figure 9. The result of thresholds 80% and the random way model.

- Bus movement model

Figure 10 shows the bus movement model results confirming the precedent results. The threshold value is the key parameter that controls the rate of privacy improvement and network performance. While Spray and Wait achieves a privacy enhancement rate of 300%, it has the highest PDR and ATT over other protocols.

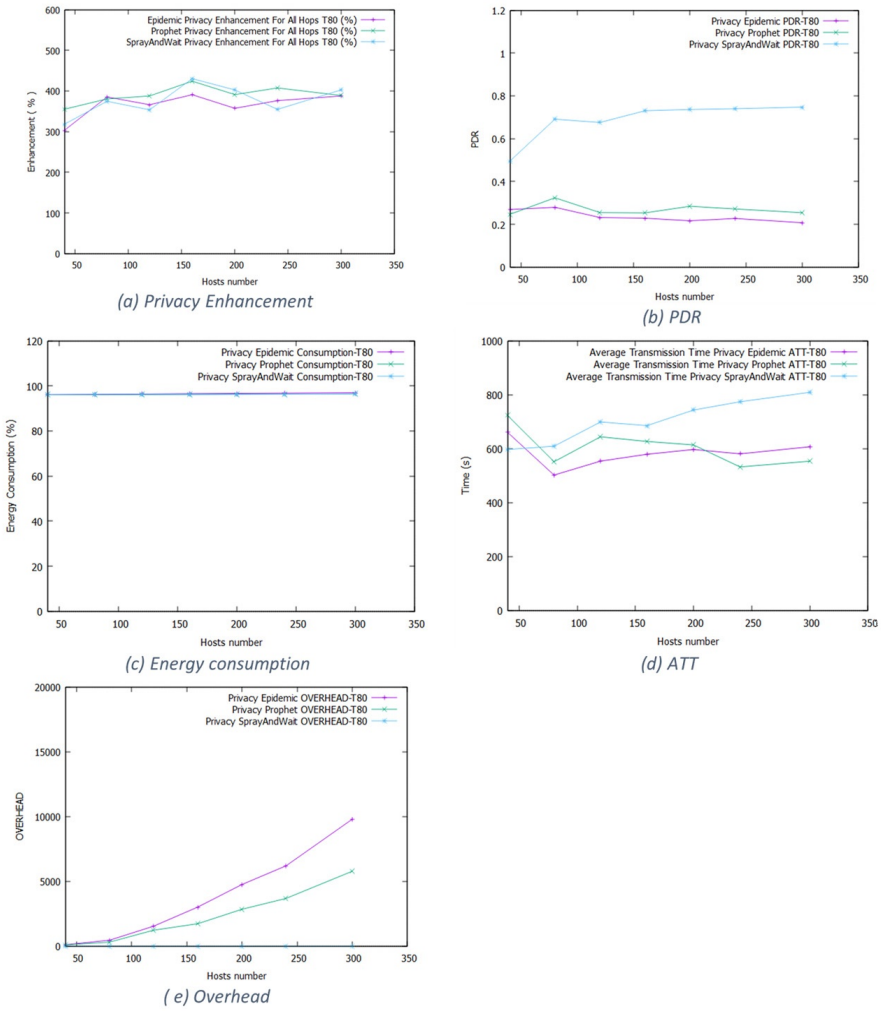

Figure 10. The result of thresholds 80 and bus model.

- Working day movement model

Figure 11 shows the working day movement model results for the 80% threshold. In Epidemic, it starts at 250% for small networks and increases when we increase the network size. For Prophet, the enhancement varies between 200% and 400%. Spray and Wait also has a high privacy enhancement rate. The wide space and long duration limit increase the forwarding opportunities, degrading the network performance.

6.2. Stranger Then Familiar Mode

In this mode, trust is calculated by Equation (4) and defines two thresholds to define stranger, weak tie, and familiar zones. We experiment with nine scenarios for three routing algorithms with three movement models.

- Random way movement model

Figure 12 shows that the Epidemic routing starts at 35% for a small-size network, then it slows down until becoming stable at around 20% with larger sizes. We achieve

around 30% for the Prophet protocol and 60% for the Spray and Wait routing protocol. We observe that the Spray and Wait algorithm exceeds the other two protocols by 30% but negatively affects the network. The delivery time suffers from an extra delay in the Spray and Wait protocol. For energy consumption, the privacy mode does not alter the level of consumption. For the PDR and the packet overhead, the Epidemic algorithm has the highest overhead rate and the lowest PDR due to its blind broadcast.

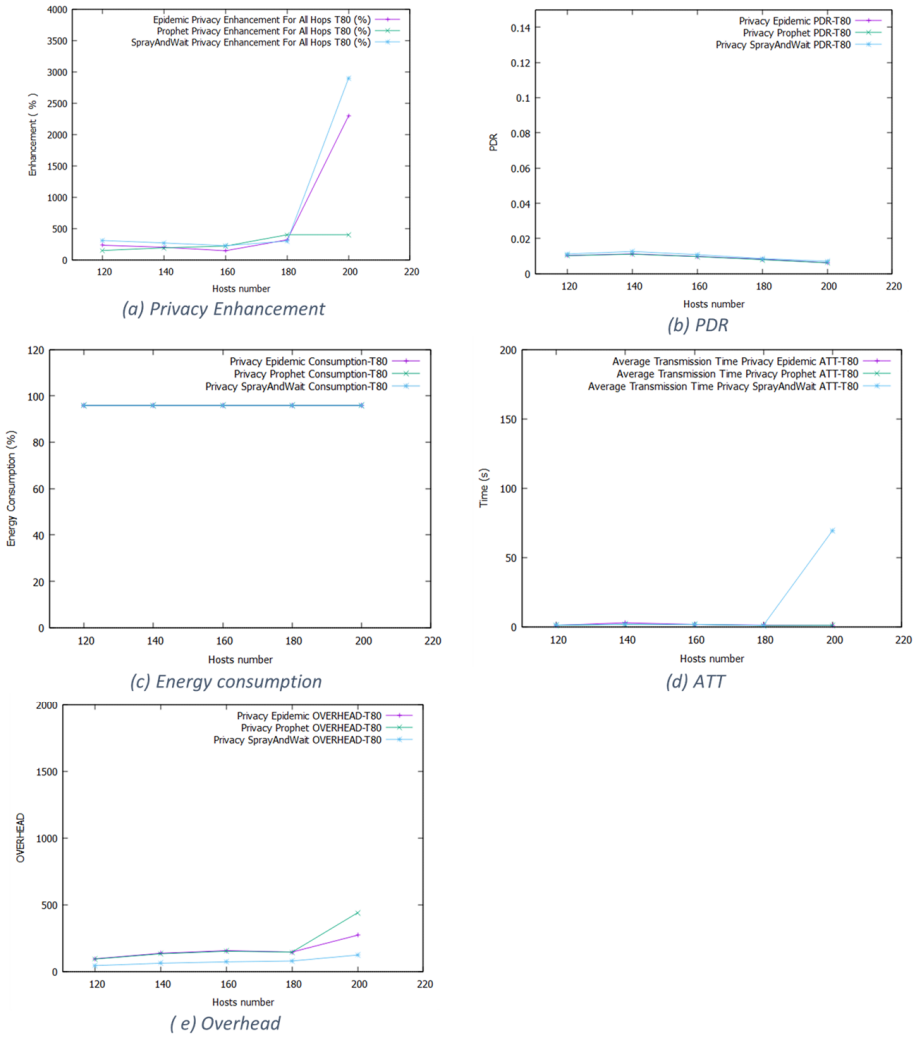

Figure 11. The result of thresholds 80% and the working day model.

- Bus movement model

The results shown in Figure 13 support the previous experiment. Privacy-aware Spray and Wait reached an enhancement of around 50%, slightly lower than the previous movement pattern. The enhancement varies between 20% and 30% in the Epidemic and the Prophet protocol. Being on the bus, mobile nodes had very limited opportunities to encounter suitable candidates, which made the two routing schemes similar. We observe the same behavior of the previous movement model for the network efficiency. Spray and Wait has the best PDR and packet overhead rates and the worst delay transmission. While the Epidemic and the Prophet protocols act almost the same, they are similar to the normal routing protocol.

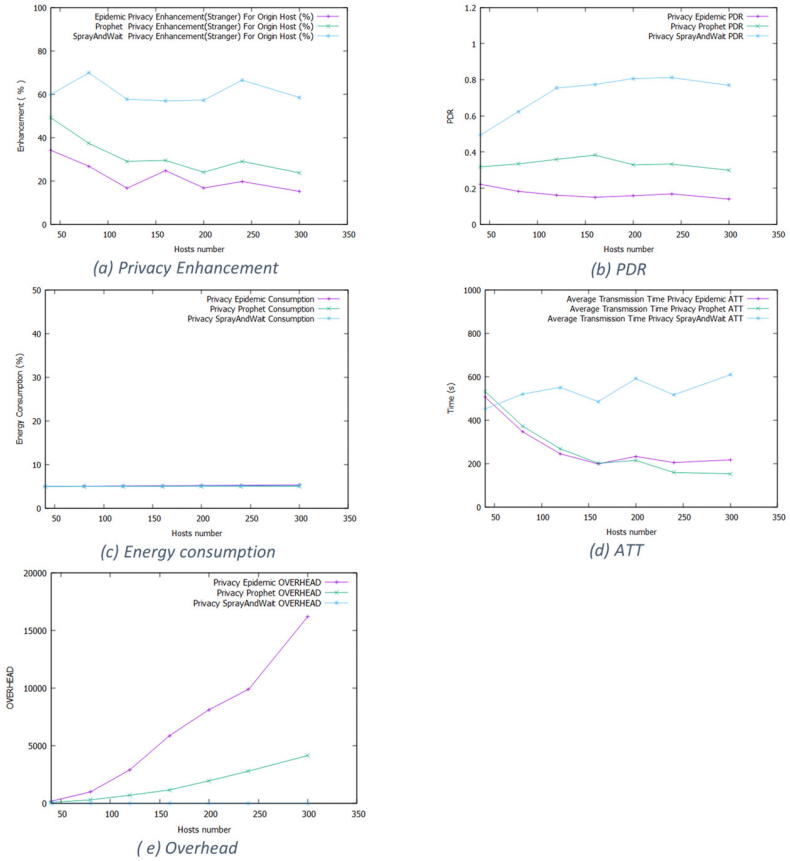

Figure 12. The result of stranger mode with random way model.

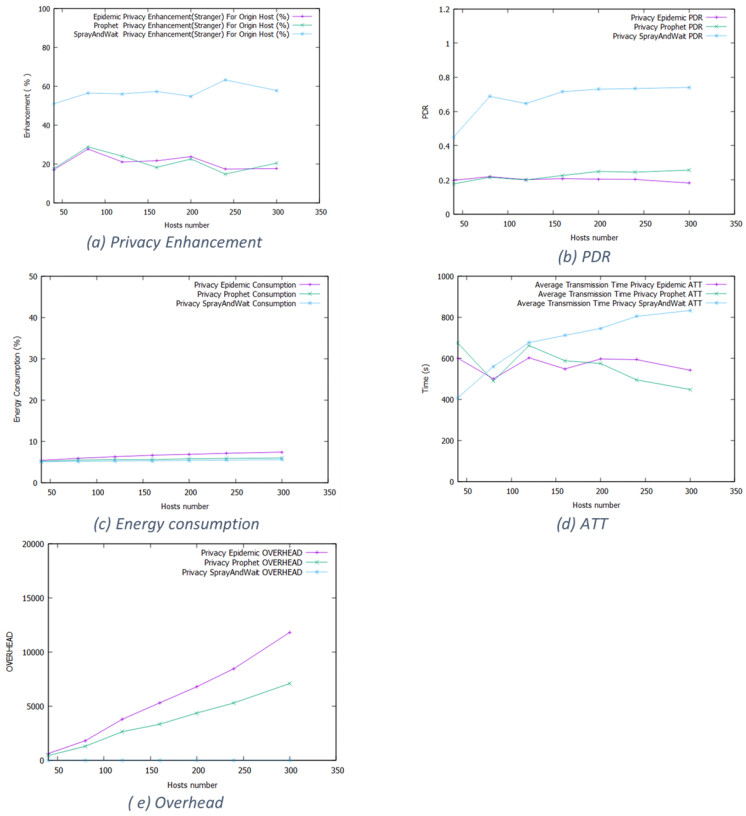

Figure 13. The result of stranger mode with bus model.

- Working day movement model

Figure 14 shows that for Epidemic, Prophet, and Spray and Wait, the privacy enhancement fluctuates around 60%, 50%, and 50%, respectively. For network efficiency, the long duration and large space of the working day movement model influenced the performances; the privacy-aware based protocols almost have the same energy consumption level and PDR. Even for the delivery time, the Spray and Wait protocol generates the same time as the others. Clearly, the working day model eliminates any advantage of the different routing schemes. In Epidemic, the packet number increases significantly for packet overhead due to the fewer forwarding opportunities, forcing the nodes to keep the messages much longer.

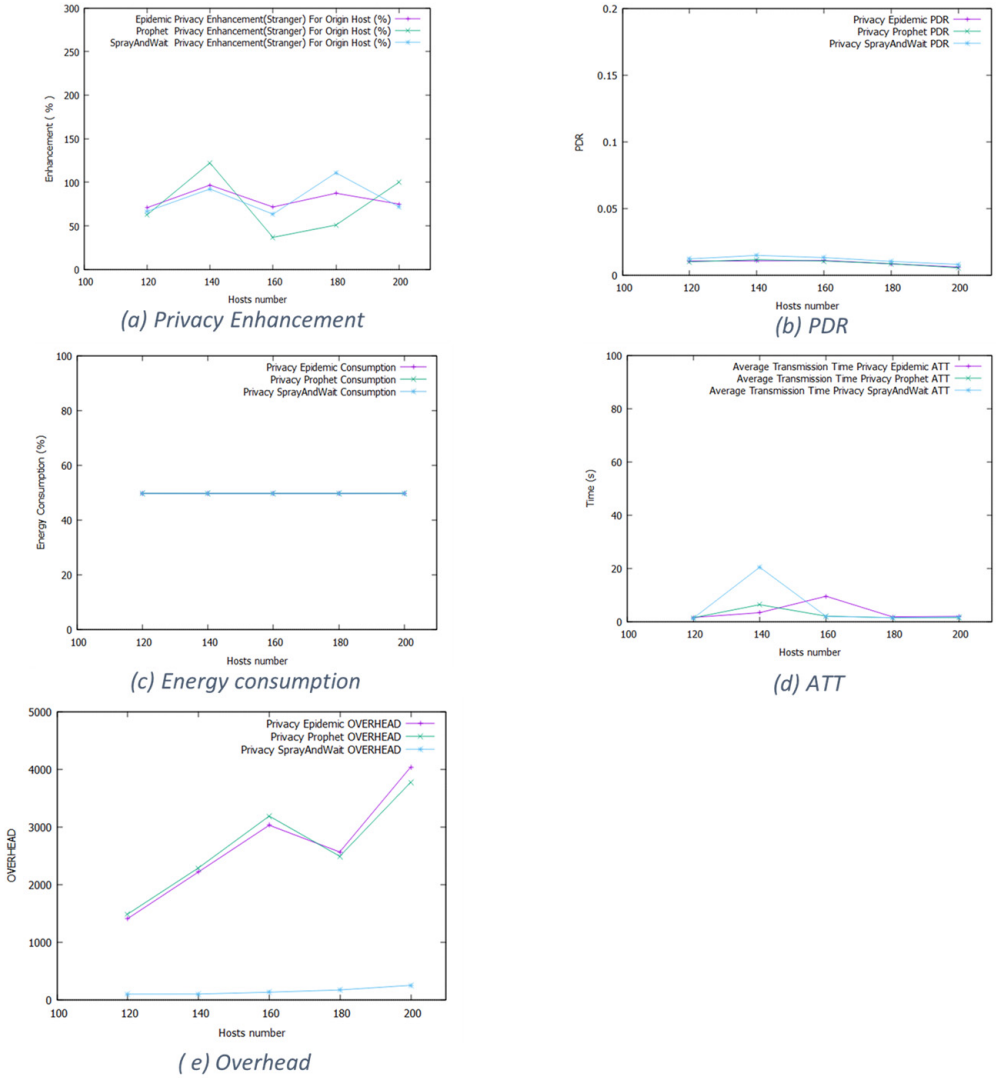

Figure 14. The result of stranger mode with working day model.

6.3. Familiar Then Stranger Mode

In this mode, we experiment with the same nine scenarios in the stranger and then the familiar mode. Following, we present the simulation results according to movement models.

- Random way movement model

Figure 15 shows the results for the random way movement model. Epidemic and Prophet protocols give almost the same results. In fact, the Prophet algorithm is an extended version of the Epidemic protocol, aiming to limit its continuous forwarding scheme. The privacy enhancement starts at around 30% for small networks and decreases to stabilize at around 10%. For the Prophet, privacy has improved by more than 20% for small-size

networks and decreased until reaching 10% for larger networks. Spray and Wait protocol controls the message copies, reduces forwarding opportunities, and eliminates unsuitable candidates. Thus, its enhancement rate for privacy rises and stabilizes at 20%, independent of the network size. For network efficiency, Epidemic and Prophet increase the delivery time while Spray and Wait achieves the highest packet delivery ratio but slows the transmission and generates the highest ATT.

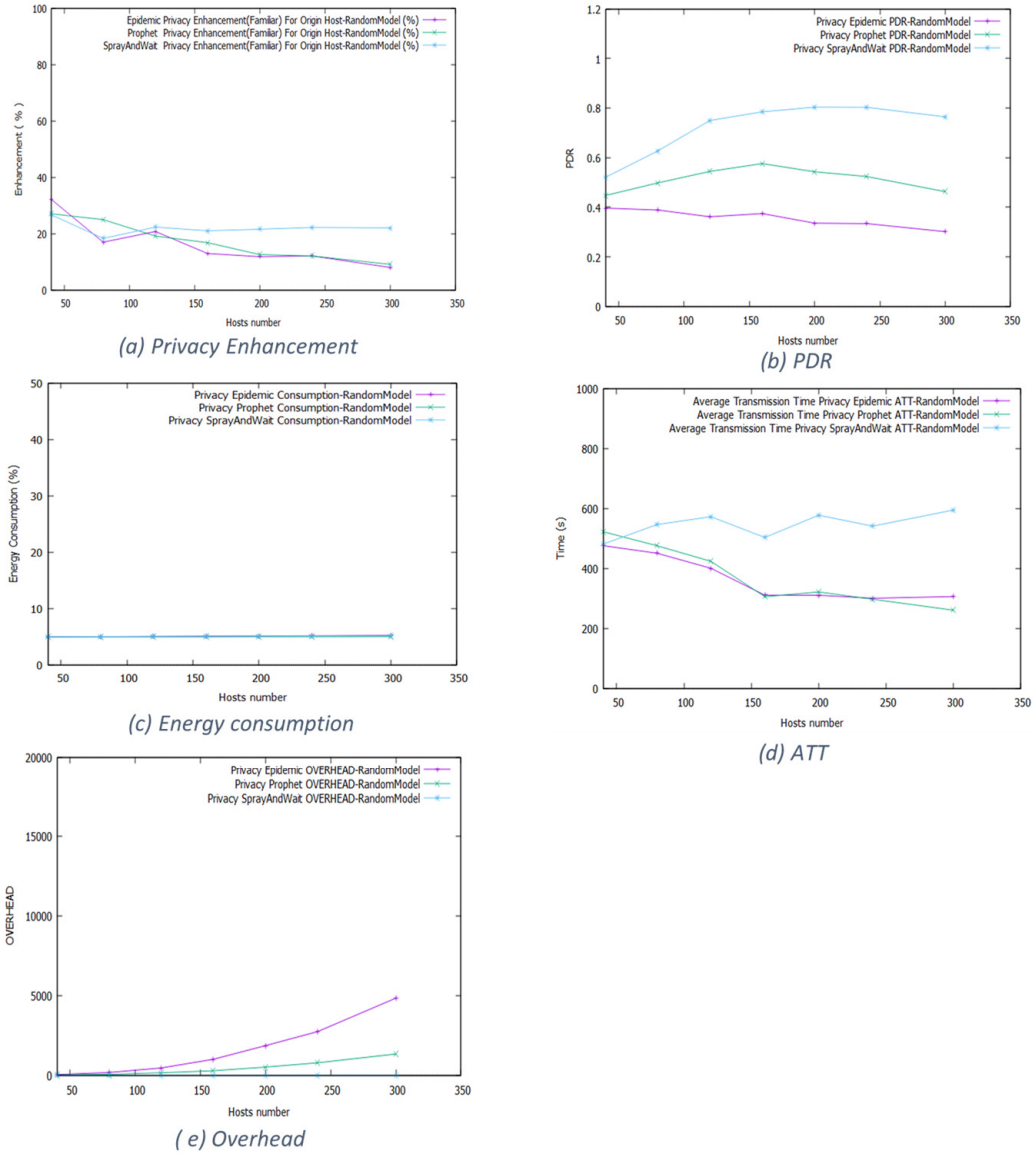

Figure 15. The result of familiar mode with the random way model.

- Bus movement model

Figure 16 supports the results of the previous movement models. The privacy-aware Spray and Wait protocol gained 20% better privacy enhancement. Epidemic and Prophet behave mostly the same for network efficiency, while the Spray protocol has the highest PDR.

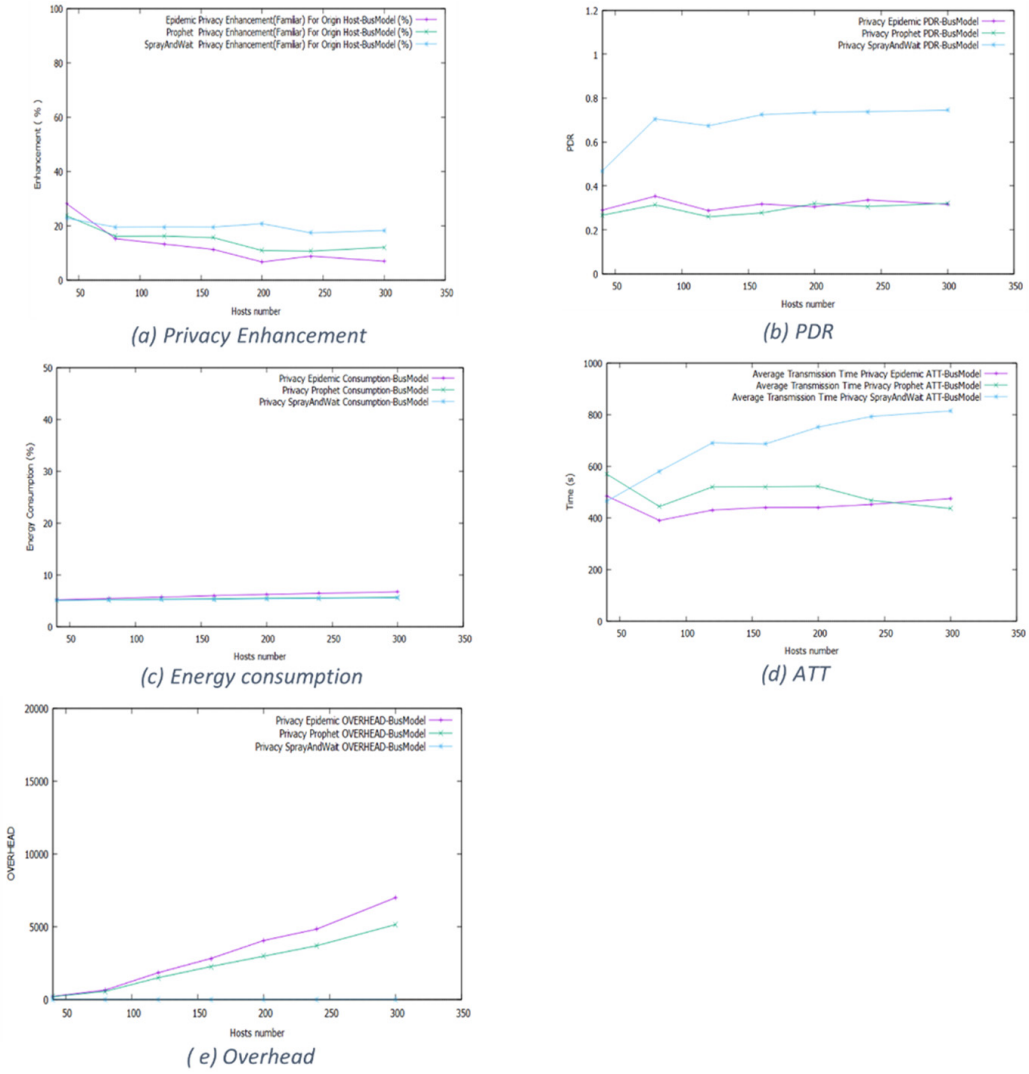

Figure 16. The result of familiar mode with bus model.

- Working day movement model

Figure 17 shows that the privacy enhancement in Epidemic overpasses 20%, rises to 50%, and then slows down to 20% for larger networks, while in Prophet, it gains up to 60%. The Spray and Wait protocol is improved by 20% in a small network compared to the normal routing, by 40% with medium size, and back to 20% with a larger network and, consequently, has the longest delivery time.

6.4. Management Overhead Characterization and Evaluation

The three proposed privacy-aware modes are based on social metrics collected to calculate the trust metric. Mostly, the mobile nodes analyze their previous communications and extract the needed information (NCF, NEM) without gathering them. When the nodes obtain information directly by contacting their neighbors, they initiate a "data collection" process by sending requests and receiving responses from the other nodes, which induces an overhead to the network.

To evaluate the "data collection" process, we defined simulation scenarios based on the protocols and movement models used in the previous experiments. We run privacy-aware routing in each scenario with a data collection process activated. We measure the following metrics: energy consumption, the average transmission time (ATT), and the overhead, which measures the average number of used packets for each node in the network during the "data collection process"—following the results organized by the movement model.

- Random way movement model

Figure 18 shows that the data collection process consumed a negligible amount of energy. The privacy-aware Epidemic routing consumes less than 0.05%, and the two others provide lower values. This result is expected since the "data collection" is a direct process of transferring packets to the final recipient.

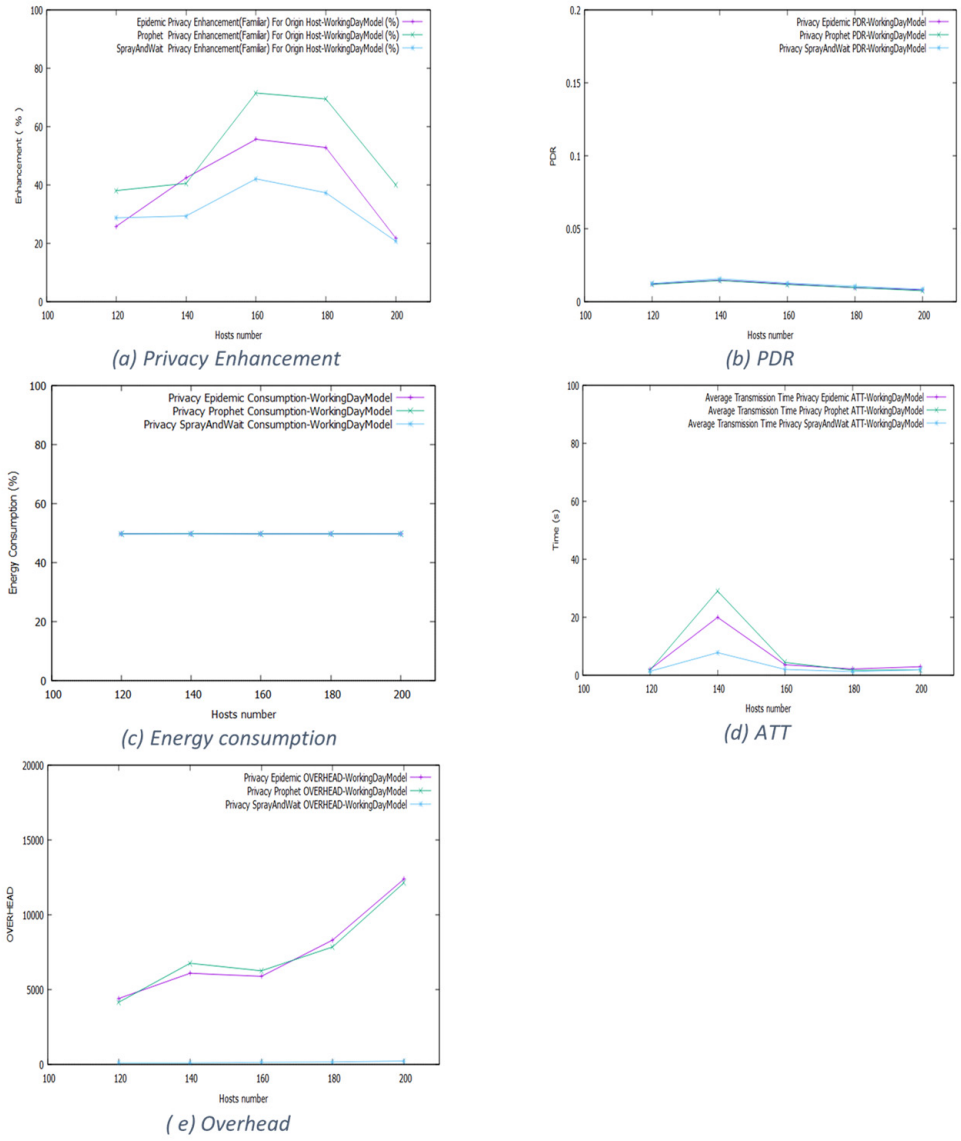

Figure 17. The result of familiar mode with working day model.

For the average transmission time for "data collection" packets per node, we see that the Epidemic routing protocol generates an average time of less than 2 s. In contrast, the Prophet protocol shows values around 0.5 s. The Spray and Wait protocol gives the highest values, with an ATT increasing with the network size from 0.5 to 4 s. Limiting the packet transmission to only direct transfer between nodes and saving the collected data locally to avoid sending new requests enabled the routers to retrieve needed data without causing a new delay. For the average number of packets used during the "data collection" process, the Spray and Wait protocol gives the lowest values (around five packets per node). The two other protocols increase on average from 5 to 500 packets per node. We can observe that, depending on the network size and the routing scheme, we need an average of less than (2 * size of the network) to ensure that all nodes have all the needed information. For example, using the Prophet protocol and 300 nodes in the network, we obtain an overhead

average of 500 packets per node. The average overhead registered is low and remains acceptable in the opportunistic networks.

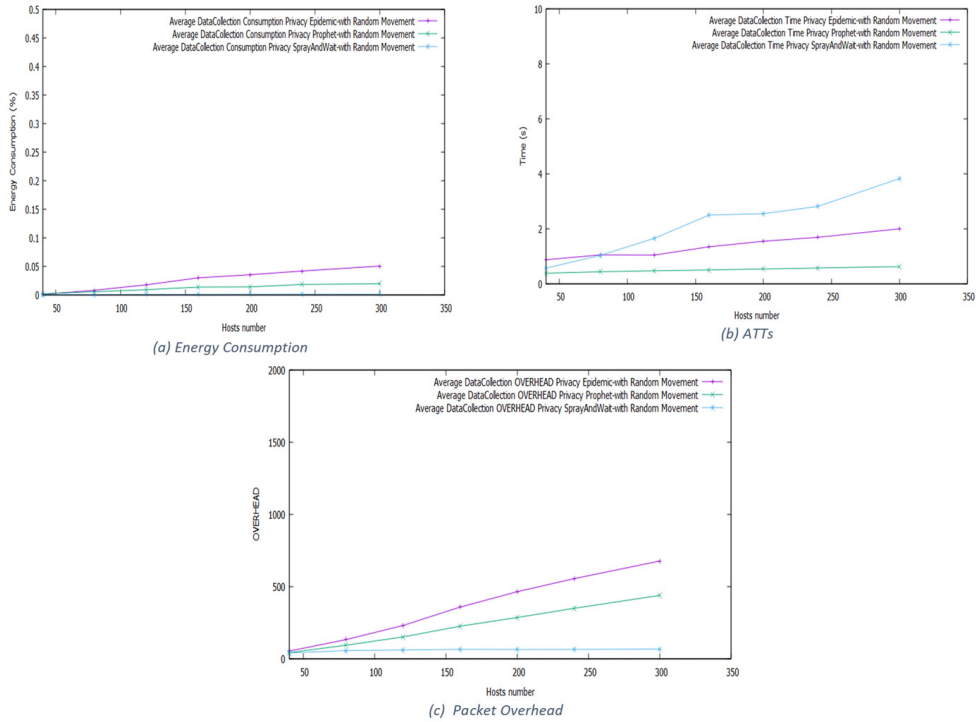

Figure 18. The result of the data collection process in the random way model.

- Bus movement model

Figure 19 shows the result of the data collection process evaluation using the bus movement model. The data collection process consumed more energy in this experiment than in the previous one. The Epidemic protocol reached 0.4%, the Prophet protocol 0.3%, and Spray and Wait registered the lowest value (under 0.1%). Those results confirm that the collection of relationship information did not consume high node energy. The registered values remain in the same interval as the previous movement model for the average transmission time. The ATT is less than 2 s for small-size networks for all used routing protocols. Then, it increases depending on the routing scheme, but still by less than 4 s. The results for packet overhead confirm the previous observations that routers use a small amount of packets to acquire the necessary information. On average, we need a number of operations close to the size of the network.

- Working day movement model

Figure 20 represents the evaluation of the collection process using the working day movement model with the three routing protocols. We observe that for all schemes, the impact of the collection process is very low. Unlike the previous movement models, the working day generates extreme conditions for message transfer. It defines a wide space and long duration. Thus, opportunities for new encounters are rare; routers will seldom need to launch a data collection process. Consequently, the data collection process lightly affects the network efficiency.

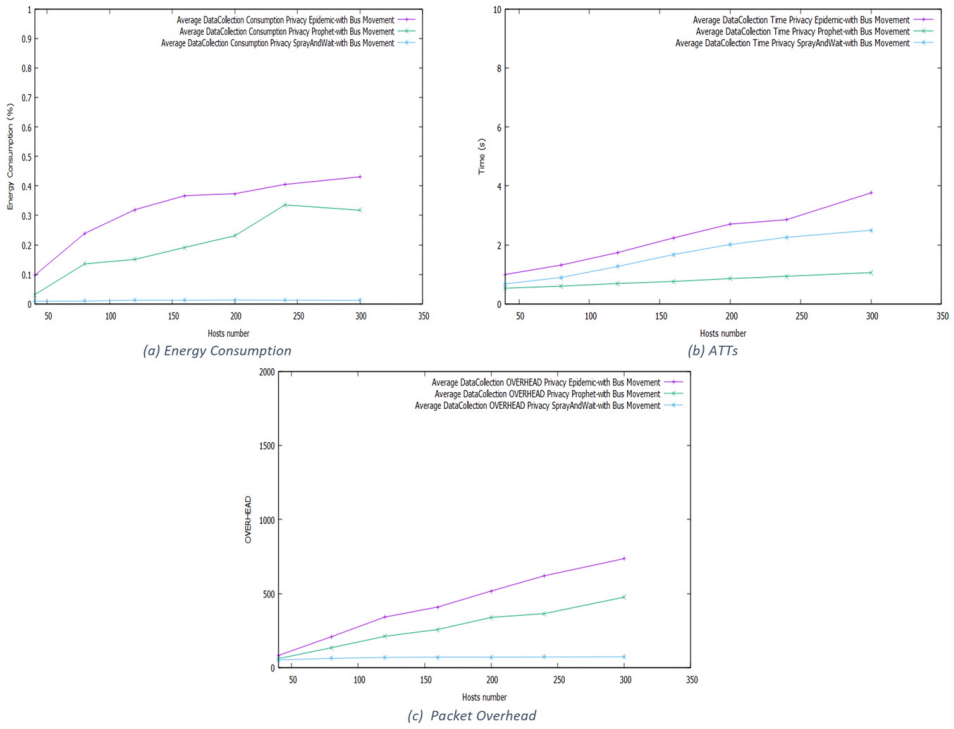

Figure 19. The result of the data collection process with the bus model.

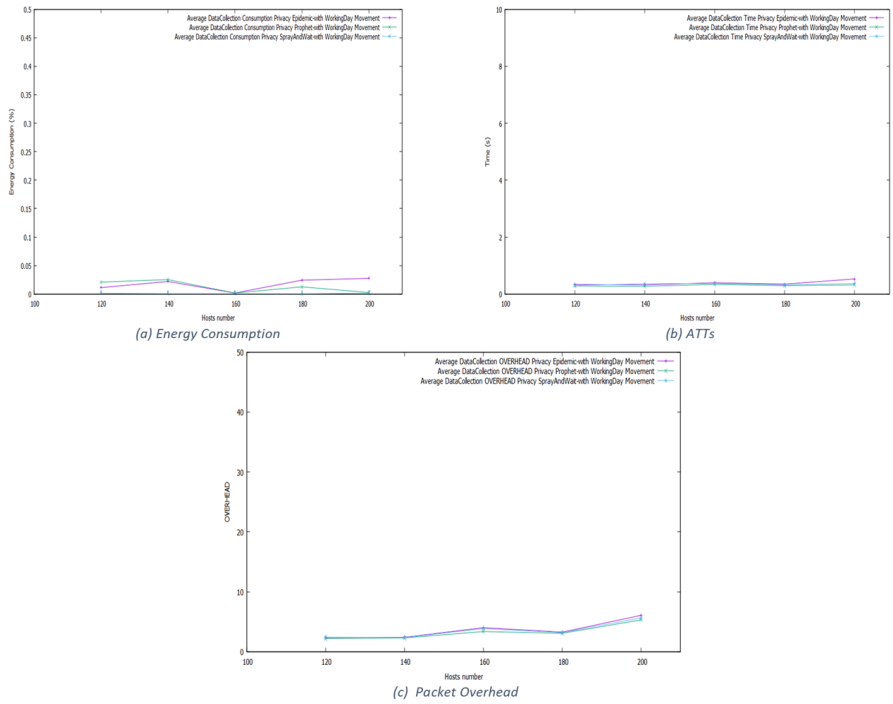

Figure 20. The result data collection process with the working day model.

7. Discussion

Table 2 illustrates the privacy enhancement ratios for each proposed mode. Firstly, the privacy enhancement increases with the threshold values. Secondly, the network conditions affect the improvement of privacy, especially the size of the used space. In a small zone, mobile nodes can meet each other more often than in a large zone.

Table 2. PER of the trust-threshold-based mode.

Routing Algorithm	Network Size Privacy Mode	Movement Model					
		Random Way		Bus Model		Working Day Model	
		Small	Large	Small	Large	Small	Large
Epidemic	30%	45.71	44.94	46.74	41.89	40	21.73
	50%	94.72	102.96	96.23	90.52	133.33	133.18
	80%	334.11	403.23	303.17	387.8	233.33	2300
Prophet	30%	40.50	40.96	50.54	46.67	19.99	40.0
	50%	94.20	93.18	104.49	102.59	33.33	104.54
	80%	310.47	389.18	355.02	388.82	150	400
Spray and Wait	30%	45.20	43.94	46.79	40.47	38.02	20.68
	50%	96.38	102.18	98.45	99.5	108.51	133.33
	80%	356.30	368.44	318.15	402.78	308.33	289.99
Epidemic	Stranger then Familiar	34.18	15.17	17.015	17.64	70.83	75
	Familiar then Stranger	32.26	8.011	28.07	6.9	25.75	21.73
Prophet	Stranger then Familiar	49.24	23.71	17.56	20.44	62.5	50.9
	Familiar then Stranger	27.07	9.12	23.63	12.04	38	40
Spray and Wait	Stranger then Familiar	59.74	58.46	50.9	57.76	66.53	71.85
	Familiar then Stranger	26.73	22.06	22.75	18.22	28.64	20.68

Thirdly, with some protocols like Spray and Wait, routers are already selective in choosing the next hop nodes. Adding the privacy conditions will make the choosing process more selective, leading to fewer forwarding opportunities and increasing the enhancement ratio. Fourthly, we observe a good privacy enhancement for the stranger then familiar and familiar then stranger modes. Indeed, their privacy enhancement ratios vary between 6% and 71%.

The overall effect of the privacy-aware selection methods is minimal concerning the network performance. The energy consumption is minimal since the selection process did not use active transmission or reception. The packet delivery ratio and the packet overhead are also slightly affected. The selection method will find fewer forwarding nodes than the normal routing, leading to fewer used packets in transmitting messages. The average transmission time (ATT) increases because nodes must select acceptable candidates before transferring messages to them, which induces a delay in transmission.

The proposed modes ensure a good privacy enhancement without losing the network and message-delivery performance. However, in real-world implementations, encryption is a critical component of privacy and security, especially when sensitive information is transmitted. Even when trust-based routing is used, encryption would still be necessary to protect the content of messages from being accessed by malicious nodes that might be part of the routing path. This paper focuses on the social aspect of privacy, such as selecting trustworthy nodes for message forwarding, rather than on the technical aspects of securing the content of the messages through encryption. Thus, we shift away from encryption to focus on the impact of such social trust and privacy-aware forwarding on network performance on top of routing protocols that do not include encryption as part of their core functionality. However, our proposed modes can be easily integrated with solutions that use encryption as a standard practice in their core functions, mainly when encryption is designed as a complementary layer that secures the content regardless of the routing path.

There are several promising directions for future work to build upon the privacy-aware routing techniques presented in this paper. Firstly, the social trust model can be enriched by incorporating additional contextual cues such as user profiles, interests, relationships, and interactions to enable more fine-grained trust evaluations between users. Secondly, exploring encryption, anonymization, and pseudonymization techniques along with social

routing can further enhance privacy. Thirdly, designing proper incentives to encourage participation in privacy-preserving message propagation can improve adoption. Fourthly, equipping the privacy layer with machine learning capabilities to automatically learn user preferences can make the system more adaptive.

8. Conclusions and Future Work

This paper presents a user-centric solution to enhance privacy in OMSNs through privacy-aware message-forwarding modes. Leveraging social metrics to approximate real-world relationship strengths and trust contexts, the proposed modes empower users to control the dissemination of messages by guiding the selection of trusted intermediary nodes. The extensive simulations demonstrate the ability of these modes to significantly improve privacy by up to 45% across various network scenarios and routing schemes while maintaining reasonable delivery efficiency and performance. The lightweight privacy layer integrates seamlessly into existing routing logic, providing flexibility to users in specifying their privacy preferences.

There are several promising directions for future work to build upon the privacy-aware routing techniques presented in this paper. Firstly, the social trust model can be enriched by incorporating additional contextual cues such as user profiles, interests, relationships, and interactions to enable more fine-grained trust evaluations between users. Secondly, exploring encryption, anonymization, and pseudonymization techniques along with social routing can further enhance privacy. Thirdly, equipping the privacy layer with machine learning capabilities to automatically learn user preferences can make the system more adaptive.

Author Contributions: Conceptualization, A.A. and H.S.; methodology, H.S.; software, A.A. and H.S.; validation, A.A. and H.S.; formal analysis, H.S. and A.A.; investigation, A.A.; resources, A.A. and H.S.; writing—original draft preparation, A.A. and H.S.; writing—review and editing, H.S.; visualization, A.A.; supervision, H.S.; project administration, H.S.; funding acquisition, A.A. and H.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by Research and Development Grants Program for National Research Institutions and Centers (GRANTS), Graduate Research Program, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia, grant number 1-18-02-007-0007.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Clement, J. Number of Global Social Network Users 2017–2025 2020. Available online: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users (accessed on 28 January 2024).
2. Mao, Z.; Jiang, Y.; Min, G.; Leng, S.; Jin, X.; Yang, K. Mobile social networks: Design requirements, architecture, and state-of-the-art technology. *Comput. Commun.* **2017**, *100*, 1–19. [CrossRef]
3. Chang, C.; Srirama, S.N.; Ling, S. Mobile social network in proximity: Taxonomy, approaches, and open challenges. *Int. J. Pervasive Comput. Commun.* **2015**, *11*, 77–101. [CrossRef]
4. Kadadha, M.; Al-Ali, H.; Al Mufti, M.; Al-Aamri, A.; Mizouni, R. Opportunistic mobile social networks: Challenges survey and application in smart campus. In Proceedings of the 2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), New York, NY, USA, 17–19 October 2016; pp. 1–8.
5. Li, M.; Yu, S.; Cao, N.; Lou, W. Privacy-preserving distributed profile matching in proximity-based mobile social networks. *IEEE Trans. Wirel. Commun.* **2013**, *12*, 2024–2033. [CrossRef]
6. Wang, Y.; Vasilakos, A.V.; Jin, Q.; Ma, J. Survey on mobile social networking in proximity (msnp): Approaches, challenges and architecture. *Wirel. Netw.* **2014**, *20*, 1295–1311. [CrossRef]
7. Sai, A.M.V.V.; Li, Y. A survey on privacy issues in mobile social networks. *IEEE Access* **2020**, *8*, 130906–130921.
8. Hu, X.; Chu, T.H.; Leung, V.C.; Ngai, E.C.-H.; Kruchten, P.; Chan, H.C. A survey on mobile social networks: Applications, platforms, system architectures, and future research directions. *IEEE Commun. Surv. Tutor.* **2014**, *17*, 1557–1581. [CrossRef]
9. Wagner, I.; Eckhoff, D. Technical privacy metrics: A systematic survey. *ACM Comput. Surv. (CSUR)* **2018**, *51*, 57. [CrossRef]

10. Rathore, S.; Sharma, P.K.; Loia, V.; Jeong, Y.-S.; Park, J.H. Social network security: Issues, challenges, threats, and solutions. *Inf. Sci.* **2017**, *421*, 43–69. [CrossRef]
11. Malekhosseini, R.; Hosseinzadeh, M.; Navi, K. An investigation into the requirements of privacy in social networks and factors contributing to users' concerns about violation of their privacy. *Soc. Netw. Anal. Min.* **2018**, *8*, 41. [CrossRef]
12. Vastardis, N.; Yang, K. Mobile social networks: Architectures, social properties, and key research challenges. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 1355–1371. [CrossRef]
13. Hui, P.; Crowcroft, J.; Yoneki, E. Bubble rap: Social-based forwarding in delay tolerant networks. In Proceedings of the 9th ACM International Symposium on Mobile ad hoc Networking and Computing, Hong Kong, China, 26–30 May 2008; pp. 241–250.
14. Daly, E.M.; Haahr, M. Social network analysis for information flow in disconnected delay-tolerant manets. *IEEE Trans. Mob. Comput.* **2008**, *8*, 606–621. [CrossRef]
15. Moreira, W.; Mendes, P.; Sargento, S. Opportunistic routing based on daily routines. In Proceedings of the 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), San Francisco, CA, USA, 25–28 June 2012; pp. 1–6.
16. Costa, P.; Mascolo, C.; Musolesi, M.; Picco, G.P. Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 748–760. [CrossRef]
17. Zhang, Y.; Zhao, J. Social network analysis on data diffusion in delay tolerant networks. In Proceedings of the Tenth ACM International Symposium on Mobile ad hoc Networking and Computing, New Orleans, LA, USA, 18–21 May 2009; pp. 345–346.
18. Kim, S.-K.; Yoon, J.-H.; Lee, J.; Jang, G.-Y.; Yang, S.-B. A cooperative forwarding scheme for social preference-based selfishness in mobile social networks. *Wirel. Netw.* **2016**, *22*, 537–552. [CrossRef]
19. Bulut, E.; Szymanski, B.K. Friendship based routing in delay tolerant mobile social networks. In Proceedings of the 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, Miami, FL, USA, 6–10 December 2010; pp. 1–5.
20. Wang, J.-W.; Jiang, Y.-T.; Liu, Z. A trusted routing mechanism for mobile social networks. In Proceedings of the 2019 IEEE 7th International Conference on Computer Science and Network Technology (ICCSNT), Dalian, China, 19–20 October 2019; pp. 365–369.
21. Liu, Y.; Li, L.; Li, Z.; Ye, Y. Trust-based optimized routing scheme in mobile social networks. In Proceedings of the 2013 International Conference on Communications, Circuits and Systems (ICCCAS), Chengdu, China, 15–17 November 2013; Volume 1, pp. 87–90.
22. Chang, M.; Chen, I.-R.; Bao, F.; Cho, J.-H. Trust-threshold based routing in delay tolerant networks. In Proceedings of the Trust Management V: 5th IFIP WG 11.11 International Conference, IFIPTM 2011, Copenhagen, Denmark, 29 June–1 July 2011; Proceedings 5. Springer: Berlin/Heidelberg, Germany, 2011; pp. 265–276.
23. Meng, X.; Xu, G.; Guo, T.; Yang, Y.; Shen, W.; Zhao, K. A novel routing method for social delay-tolerant networks. *Tsinghua Sci. Technol.* **2019**, *24*, 44–51. [CrossRef]
24. Yao, L.; Man, Y.; Huang, Z.; Deng, J.; Wang, X. Secure routing based on social similarity in opportunistic networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 594–605. [CrossRef]
25. Yang, S.; Wang, X.; Zhang, S.; Yi, B.; Huang, M. Trust-based security routing mechanism in mobile social networks. *Neural Comput. Appl.* **2020**, *32*, 5609–5620. [CrossRef]
26. Yang, Y.; Zhao, H.; Ma, J.; Han, X. Social-aware data dissemination in opportunistic mobile social networks. *Int. J. Mod. Phys. C* **2017**, *28*, 1750115. [CrossRef]
27. Zhang, S.; Liu, H.; Chen, C.; Shi, Z.; Song, W.W. Activity-based routing algorithm in opportunistic mobile social networks. *Int. J. Distrib. Sens. Netw.* **2021**, *17*. [CrossRef]
28. Huang, R. Providing Location-Privacy in Opportunistic Mobile Social Networks. Ph.D. Dissertation, University of Ottawa, Ottawa, ON, Canada, 2018.
29. Li, H.; Zhu, H.; Du, S.; Liang, X.; Shen, X. Privacy leakage of location sharing in mobile social networks: Attacks and defense. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 646–660. [CrossRef]
30. Keranen, A. *Opportunistic Network Environment Simulator*; Special Assignment Report; Department of Communications and Networking, Helsinki University of Technology: Espoo, Finland, 2008.
31. Vahdat, A.; Becker, D. *Epidemic Routing for Partially Connected ad hoc Networks*; Duke University: Durham, NC, USA, 2000.
32. Lindgren, A.; Doria, A.; Schelen, O. Probabilistic routing in intermittently connected networks. In Proceedings of the Service Assurance with Partial and Intermittent Resources: First International Workshop, SAPIR 2004, Fortaleza, Brazil, 1–6 August 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 239–254.
33. Spyropoulos, T.; Psounis, K.; Raghavendra, C.S. Spray and wait: An efficient routing scheme for intermittently connected mobile networks. In Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking, Philadelphia, PA, USA, 26 August 2005; pp. 252–259.