A Multi-Path Approach for *k*-Anonymity in Mobile Hybrid Networks

C.A. Ardagna[1] A. Stavrou[2] S. Jajodia[2] P. Samarati[1] R. Martin[2]

[1] University of Milan, Italy
[2] George Mason University, USA

Abstract. The ubiquitous proliferation of mobile devices has given rise to novel user-centric applications and services. In current mobile systems, *users* gain access to remote *service providers* over *mobile network operators* which are assumed to be trusted and not improperly use or disclose users' information. In this paper, we remove this assumption, offering privacy protection of users' requests again the prying eyes of the network operators, which we consider to be honest but curious. Furthermore, to prevent abuse of the communication privacy we provide, we elevate traffic accountability as a primary design requirement. We build on prior work on network k-anonymity and multi-path communications to provide communications' anonymity in a mobile environment. The resulting system protects users' privacy while maintaining data integrity and accountability. To verify the effectiveness of our approach and measure its overhead, we implemented a prototype of our system using WiFi-enabled devices. Our preliminary results indicate that the overall impact on the end-to-end latency is negligible, thus ensuring applicability of our solution to protect the privacy of real-time services including video streaming and voice activated services.

1 Introduction

Recent technology advancements in mobile and wireless devices have fostered the development of a new wave of on-line and mobile services. Due to their pervasive nature, these services are becoming increasingly popular and wide-spread. On the other hand, the accuracy, reliability and performance of location sensing technologies, have raised concerns about the protection of users' privacy. Today, there are no mechanisms to prevent wireless communications from being broadcasted to the neighboring devices thus disclosing private information about the location of users. The worst case scenario that analysts have foreseen as a consequence of an unrestricted and unregulated availability of mobile technologies recalls the "Big Brother" stereotype: a society where the secondary effect of mobile technologies – whose primary effect is to enable the development of innovative and valuable services – becomes a form of implicit total surveillance of individuals.

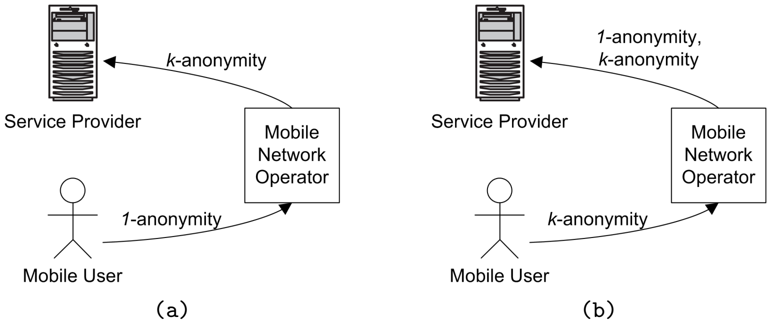


Fig. 1. Current privacy mechanisms (a) and our new vision of privacy (b)

Some recent examples can provide an idea of the extend of the problem. In September 2007, Capla Kesting Fine Art announced the plan of building a cell tower, near Brooklyn NY, able to capture, monitor and rebroadcast wireless signals, or in other terms eavesdrop WiFi communications to ensure public safety [28]. Moreover, the US Congress approved changes to the 1978 Foreign Intelligence Surveillance Act giving NSA authorization to monitor domestic phone conversations and e-mails including those stemming from the cellular network and Internet. This legislation provides the legal grounds for the cell tower's construction, and for the monitoring of users communications in the cellular network.

Current privacy protection systems are focused on preserving users from untrusted service providers. However, at the same time and assume mobile network operators to be trusted. In this paper, and to the best of our knowledge we are the first to do so, we assume mobile network operators to be honest but curious. Our approach builds on the concept of k-anonymity in the context of network communication but, unlike other approaches, aims at providing such anonymity against the mobile network operator, instead of against the service provider. Figure 1 illustrate the difference between our approach and current solutions. Current solutions (see Figure 1(a)) use k-anonymity to protect the users during the communications with the service provider and consider the mobile network operator as a fully trusted party. However, the mobile network operator has access to precise location and traffic information for each user. In our approach (see Figure 1(b)), the mobile network operator is considered honest but curious and a k-anonymity mechanism is used to protect users' privacy. The user *can* then decide if the service provider is assumed trusted. In the figure either 1-anonymity is preserved, if the service provider is assumed trusted, or k-anonymity, if the service provider is assumed untrusted. Also, our work is different from traditional research in anonymous communications [6–8, 19], because it can be applied in a mobile infrastructure and is geared towards k-anonymity, not complete sender anonymity. In addition, we treat user and traffic accountability as a fundamental requirement of our approach making sure that each user is accountable for the services requested. Having a system that can enforce data accountability prevents unwanted traffic and provides economic incentives for the deployment of privacy-preserving services.

To achieve the aforementioned goals, we extend the concept of network k-anonymity to hybrid mobile networks. In such networks, users can simultaneously create WiFi point-to-point connections, join the cellular network, and access the Internet through their mobile phones. Using a multi-path communication paradigm [23], a mobile user can achieve network k-anonymity by distributing, using WiFi network, different packets of the same message to k neighboring mobile peers, which then forward the received packet through the cellular network. This scheme achieves k-anonymity because the mobile network operator is not able to associate the users' data flow with fewer than k peers.A separate accounting mechanism can verify that the packets are legitimate. For instance, one approach is to have the data flow encrypted with a symmetric key shared between the requester and the service provider. This would assure accountability, data integrity, and confidentiality. In addition, it will prevent the abuse of anonymity [4] while providing the economic incentives to deploy anonymizing schemes. Of course, there is a clear trade-off between anonymity and latency overhead: the further we forward the packets, the better the anonymity is but the more is the latency overhead. To quantify that trade-off in practice, we have built a prototype of our system using WiFi-enabled cellphones.

The remainder of this paper is organized as follows. Section 2 illustrates the overall architecture. Section 3 discusses privacy requirements and challenges in the considered scenario and illustrates our solution. Section 4 discusses experimental results illustrating the impact of our solution on end-to-end communication. Section 5 discusses related work. Finally, Section 6 presents our conclusions.

2 Overall Architecture

Our reference model is a distributed and mobile infrastructure which forms a hybrid network [8, 9, 22], integrating both wireless, cellular and

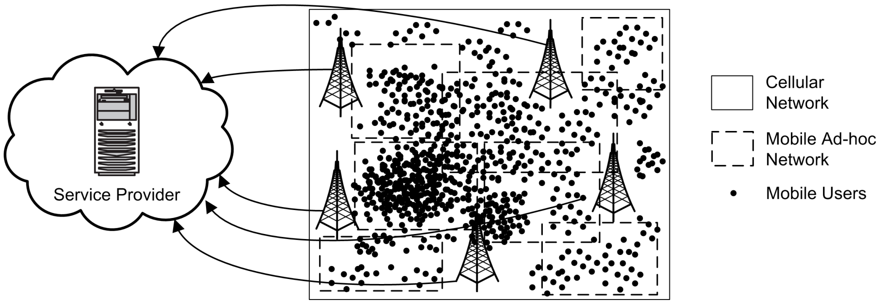


Fig. 2. Mobile Network Architecture

wired technologies. Our scenario is based on mobile parties communicating through wireless and cellular protocols to access services, either co-located in the cellular network or in the Internet. Figure 2 illustrates the overall architecture and the participating entities, which are as follows.

- *Mobile Users.* They are human users that carry mobile devices supporting both GSM/3G and WiFi protocols for communication. They request services to providers available over the network.
- *Cellular Network (and corresponding Mobile Network Operators).* It is composed of multiple radio cells (also known as cell-phone towers), which provide network access and services to mobile users. The cellular network acts as a gateway between mobile users and service providers.
- *Service Provider.* It is the entity that provides on-line services to the mobile users and collects their personal information before granting an access to its services.

Mobile users establish ad-hoc (WiFi) point-to-point connections with other mobile peers in the network, resulting in several Mobile Ad-Hoc Networks (MANETs), represented by the dashed rectangles in Figure 2. Also, mobile users receive signals from the radio cells and can connect to the cellular networks, through which they access the service. Here, we assume also mobile peers, like the provider, to be honest but curious. This means that they can try to eavesdrop a communication but do not attempt to either drop or maliciously modify it. Figure 3 illustrates the communications between the different parties in the hybrid network.

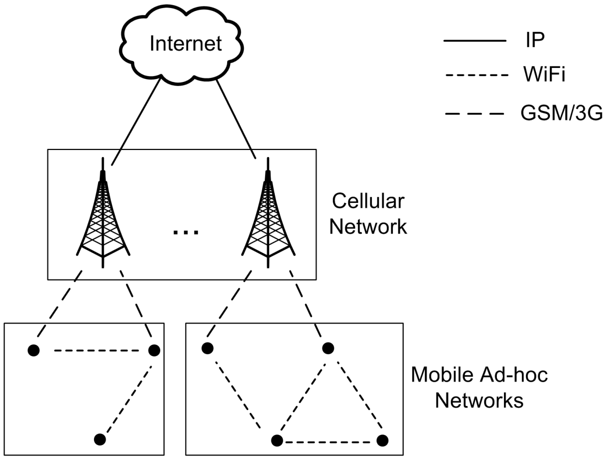


Fig. 3. Hybrid Network Communications

3 A Multi-Path Communication for Network *k*-Anonymity

We describe of our solution based on network k-anonymity by showing: *i)* how a k-anonymous request is generated and transmitted by a mobile user to the service provider through the cellular network and *ii)* how the service provider crafts a reply that can be received and decoded only by the requester concealed from the other k-1 users. Before going into details of the solution, we discuss our privacy goals and challenges.

3.1 Privacy Requirements and Challenges

In hybrid mobile networks, users privacy is at risk and is affected by several threats. In the last few years, the definition of privacy solutions was geared towards the privacy of the users, sacrificing the need for accountability. Thus, an important requirement, often neglected by mobile privacy solutions, is the necessity for mechanisms to make the users accountable for their operations. Many anonymization techniques in fact can be abused or lack economic incentives due to the lack of user accountability [4]. Service providers are often reluctant to adopt privacy solutions that completely hide the users and do not enable any form of accountability. Another challenge driving our work is the current implicit trust on mobile network operators. We believe that mobile network operators should be treated as untrusted parties with respect to confidentiality.

These challenges result in the definition of two-level privacy requirements. Two-level means that different kinds of privacy protection have to be guaranteed at: *1)* the mobile network level (*anonymous communication*) and *2)* the service level (*location hiding*).

- *Anonymous communication.* Each mobile user should communicate anonymously with the mobile network operator, possibly by masking its identity with the identities of other users joining the cellular network. At the same time, to preserve accountability, the requester's identity should be known to the service provider.
- *Location hiding.* Each mobile user interacting with a service provider should be able to hide its current location, if not otherwise required by the service provider for the service release.[3] This follows the principle of *minimum disclosure*, which states that service providers must require the least set of information needed for service provision. Conversely, location of the users must be known to the mobile network operator to provide connection to the network.

To conclude, an important requirement that any privacy solution should implement, is to provide a mechanism for expressing users' privacy preferences that strikes a balance between usability and expressiveness. In our work, the users can still express their privacy preference in terms of the number k of users that should join the *anonymity set.* This is the only effort required to the users to protect their privacy, while the application of the privacy solution is completely transparent to them.

3.2 Overview of the Approach

The concept of k-anonymity has been originally defined in the context of databases [21]. Here, we introduce a solution based on the concept of network k-anonymity, first introduced in [24], which can be defined as follow.

Definition 1 (Network k-anonymity). *Let U be a set of users and M be a message originated by a mobile user $u \in U$. User u is said to have network k-anonymity, where k is the privacy preference of the user u, if the probability of associating u as the message originator is less than or equal to $\frac{1}{k}$.*

[3] Note that, our solution is however compatible with all previous works in the context of location privacy and anonymity.

We now describe the forward and reverse anonymous communications that compose our solution. The complete protocol is shown in Figure 4. Let us define u as the mobile user that submits the request and SP the service provider. SP and the cellular network are in business relationship and u is subscribed to the cellular network. Also, SP and u are assumed to be in a producer-consumer relationship and to share a common secret key s that is generated through a Diffie-Hellman key exchange protocol. Each message M between a user and a service provider is encrypted thus protecting confidentiality and integrity of the message through symmetric encryption (e.g., 3DES, AES). $E_s(M)$ denotes a message M encrypted with symmetric key s. Also, a cryptographic message authentication code (i.e., $MAC_s(M)$) is calculated on the message M using s. SP is finally responsible for filtering of the requests.

Anonymous Request. The anonymous request process is initiated by a mobile user u, which wishes to access a service provided by service provider SP. No overhead is given to u in the management of the mobile and anonymous process; u needs only to specify her privacy preference k. First, $MAC_s(M)$ is calculated; then M is split in k data flows producing the set DS=$\{m_1, m_2, \ldots, m_k\}$.[4] The resulting packets are distributed among the neighbor mobile peers (peers for short) in the mobile ad-hoc network. Different algorithms, ranging from the ones based on *network state* to the ones based on *peer reputation*, can be implemented for distributing packets among peers. Here, we use a simple approach which consists in randomly forwarding the packets to the peers in u's communication range.

The distribution algorithm is illustrated in Figure 5(a) and works as follows. The requester u encrypts each packet in DS using the symmetric key s shared between u and SP, and then appends $MAC_s(M)$ in plaintext to each encrypted packet, that is, $E_s(DS) = \{[E_s(m_1)\|MAC_s(M)], [E_s(m_2)\|MAC_s(M)], \ldots, [E_s(m_k)\|MAC_s(M)]\}$. The presence of the MAC information in every packet allows mobile peers to distinguish between packets belonging to the same message M. Requester u then randomly picks up one of the encrypted packets $[E_s(m_j)\|MAC_s(M)] \in E_s(DS)$ for sending it to the SP, and randomly selects $k-1$ peers in the communication range. Each selected peer receives a packet $[E_s(m_i)\|MAC_s(M)] \in E_s(DS)$ and uses a *decision forwarding function* (*dff*) to manage it. Function *dff* is defined as follow.

[4] For the sake of clarity, in the following, we use the term "packet" to identify a data flow of any dimension.

Protocol 1 *Anonymous communication protocol*

Initiator: Requester u
Involved Parties: Mobile peers *PEERS*, Mobile network operator *MNO*, Service provider *SP*
Variables: Original message M, Response message M_r, Secret key s shared between u and *SP*

```
INITIATOR ($u$) u.1 Define message $M$ and privacy preference $k$.
                u.2 Generate $MAC_s(M)$ and $DS = \{m_1, m_2, \ldots, m_k\}$.
                u.3 Encrypt packets in $DS$ and append $MAC_s(M)$ to them,
                      $E_s(DS) = \{[E_s(m_1) \| MAC_s(M)], \ldots, [E_s(m_k) \| MAC_s(M)]\}$.
                u.4 Select a random packet $[E_s(m_j) \| MAC_s(M)] \in E_s(DS)$.
                u.5 Select a set of $k$-1 peers $\{p_1, \ldots, p_{k-1}\} \in PEERS$.
                u.6 Send to each $p_i \in \{p_1, \ldots, p_{k-1}\}$ a packet
                      $[E_s(m_i) \| MAC_s(M)] \in E_s(DS)$.
                u.7 Send $[E_s(m_j) \| MAC_s(M)]$ to the MNO.
                u.8 Receive $E_s(M_r)$ from the MNO (Step M.3) and decrypt it.

PEERS           P.1 Receive a packet $[E_s(m_i) \| MAC_s(M)] \in E_s(DS)$ (Step u.6).
                P.2 Apply decision forwarding function (dff).
                P.3 Send $[E_s(m_i) \| MAC_s(M)] \in E_s(DS)$ to the MNO or forward it to
                      another peer.
                P.4 Receive $E_s(M_r)$ from the MNO (Step M.3) and delete it.

MNO             M.1 Receive packets (Steps u.7 and P.3).
                M.2 Forward packets to the SP.
                M.3 Receive $E_s(M_r)$ from the SP (Step S.4) and forward it to $u$ and
                      PEERS.

SP              S.1 Receive packets from the MNO (Step M.2).
                S.2 Decrypt the packets and assemble $M$.
                S.3 Generate and encrypt the response message $E_s(M_r)$.
                S.4 Send $E_s(M_r)$ to $u$ and PEERS through the MNO.
```

Fig. 4. Anonymous communication protocol

$$dff([E_s(m_i) \| MAC_s(M)]) = \begin{cases} 1 & \text{if } count(MAC_s(M)) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

where *dff* =1 means that the peer under examination has already agreed to send a packet belonging to message M (i.e., with $MAC_s(M)$). If *dff* =1 the peer forwards the received packet m_i to some other peers. Otherwise, if *dff* =0 the peer randomly selects with probability $p_f = \frac{1}{2}$ either to send the packet to the *SP* (white circles in Figure 5(a)) or to forward it to a peer in the communication range (black circles in Figure 5(a)).

Example 1. Figure 5(a) shows an example of the distribution algorithm. The requester u defines $k = 5$ and splits the message M in five parts $\{m_1, \ldots, m_5\}$. Packets are then encrypted with the symmetric key s shared between u and *SP*, and $MAC_s(M)$ is attached to each of them.[5] The requester u selects packet m_3 to be sent directly to the *SP* and forwards the other k-1 packets to peers in the communication range. Specifically, packets m_2 and m_5 are forwarded to peers p_1 and p_3 which send them to the *SP*. Packet m_1 instead takes a forwarded path $p_4 \rightarrow p_7$, assuming p_4 does not accept to send m_1. Finally, packet m_4 takes a forwarded path $p_6 \rightarrow p_7 \rightarrow p_9$ because when the packet is received by p_7, p_7 notices that she has already accepted a packet with the same $MAC_s(M)$ (i.e., m_1) and then automatically forwards m_4 to p_9.

After packets distribution, each selected peer independently sends the packet to the *SP*, through the mobile network operator. The mobile network operator then sees packets that comes from k different users. This scenario results in the following proposition.

Proposition 1. *A user is k-anonymous to the mobile network operator if and only if at least k packets of the same message are sent to the mobile network operator by k different peers (including the requester).*

The mobile network operator forwards the k received packets to the *SP* hiding by default location information. Now, the *SP* can decrypt each packet, reconstruct the original message, and satisfy the user request. A summary of the overall anonymous request process is provided in Figure 5(a).

Anonymous Response. After the conclusion of the anonymous request process, the *SP* retrieves the original message M and starts the service provisioning, which results in the release of an anonymous response to the requester u. The communication involves the mobile network operator to manage peers mobility and route the response to the user u, and must preserve the preference k of the requester.

The anonymous response process works as follow. First of all, as showed in Figure 5(b), the service provider encrypts the response message M_r with the secret key s shared with u. Then the *SP* transmits the encrypted message $E_s(M_r)$ to the k peers involved in the anonymization process. *SP* relies on the cellular network to manage the message delivery and the mobility of the peers. Although all peers receive the message, the

[5] For the sake of clarity, we omit $MAC_s(M)$ in the figure.

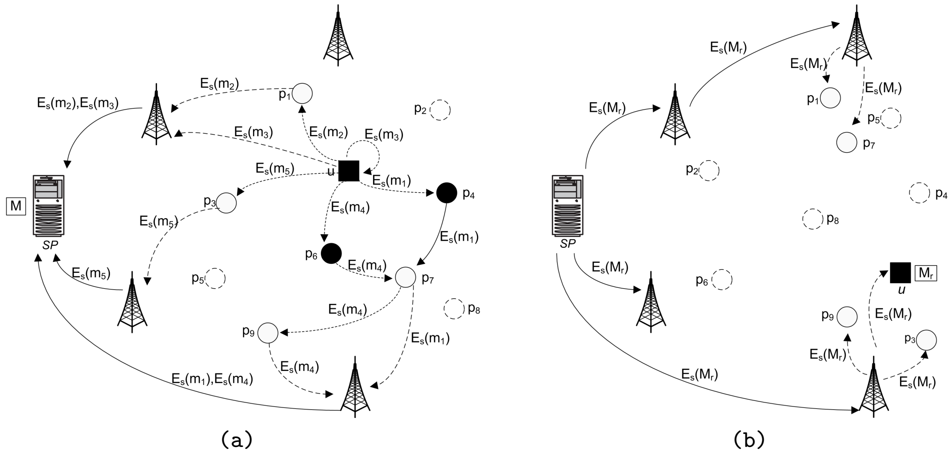


Fig. 5. Example of anonymous request (a) and anonymous response (b)

requester u is the only peer with the secret key s, and thus, she is the only one able to decrypt the message and benefit of the service.[6]

Example 2. Figure 5(b) shows an example of anonymous response. Encrypted message $E_s(M_r)$ is transmitted to all peers used in Example 1, that is, $\{u, p_1, p_3, p_7, p_9\}$. As soon as the message is received by u, it is decrypted. The other peers delete message $E_s(M_r)$, since they are not able to open it.

Recalling the requirements and challenges in Section 3.1, our solution provides both *anonymous communication* and *location hiding*. In terms of anonymous communication, we employ a message splitting and multipath solution that provides k-anonymity against mobile network operators. Considering *location hiding*, the location information of the users is hidden by the cellular network to the service providers. Finally, our solution provides requester accountability, since the requester's identity is released to the service provider.

It is important to note that our solution does not require changes to existing network protocols. All the packets in fact are routed regularly through the hybrid network using TCP and reconstructed at the destination service provider. Only some small changes are requested for specific

[6] To further strengthen our protocol, the service provider could potentially generate $k-1$ decoy messages, other than M_r. This can be performed by adding a *nonce* to the original message M_r before encrypting it with the secret key s. The cellular network sees k different response messages and it is not able to associate the response to the request.

applications on the top of existing layers, as for instance, the message splitting done by the requester u and the packet checks on the mobile ad-hoc network done by the peers.

4 Some Notes on Performance

As a first step, we were interested in quantifying the impact of our approach on the end-to-end communications. Although, this aspect is less significant for database and informational services, it is highly critical for real-time streaming services including video and live operators. Hence, we implemented a prototype of our approach using WiFi-enabled devices and measured the latency overhead when we forward packets to one-hop and two-hop neighbors using WiFi. We describe the testing scenario in Section 4.1 and discuss the performance analysis in Section 4.2.

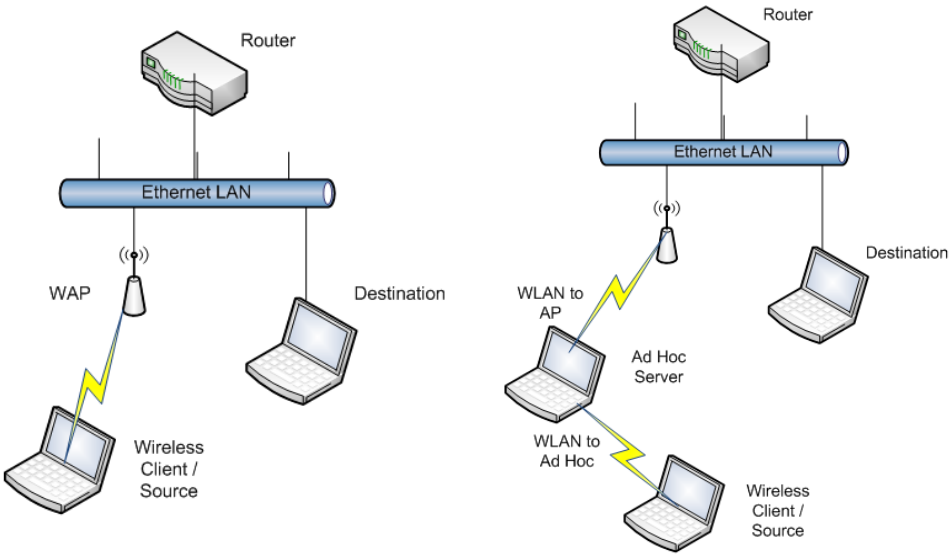
4.1 Testing Scenario Implementation

We deployed a small-scale testbed using standard IEEE 802.11 communications. We generated two scenarios depicted in Figure 6.

The first scenario (Figure 6(a)) considers baseline measurements in latency of one hop between a *wireless client* and the *target system*. Here, a device is associated directly with a *Wireless Access Point* (WAP); we varied the distance from the client to the WAP. For all practical purposes, the WAP was acting as the one-hop neighbor that forwards the packets to the cellular network.

The second scenario (Figure 6(b)) considers measurements of latency in a two-hop scenario. Here, a device is configured as an *ad-hoc server* on Wireless Adapter #1 (WA1), and with Windows' Internet Connection Sharing (ICS) enabled on Wireless Adapter #2 (WA2), for WA1's traffic. The wireless client is then connected through the ad-hoc server and the WAP to the target system. As in the one-hop scenario, no modification is needed at the WAP. To better simulate a real world scenario, the ad-hoc server has been placed in various locations and distances from the WAP. However, as expected and confirmed by our result, the closer the two systems are to each other, the less latency is observed. Additionally, any implementation in which we have more than one ad-hoc networks should utilize orthogonal channels while broadcasting in the same spectrum, to minimize the interference.

The measurements for both the infrastructure and ad-hoc connections have been taken at approximately the same points. This mitigates variables that might affect WiFi connectivity, such as amount of interference



(a) (b)

Fig. 6. Network Architecture for One-Hop (a) and Two-Hop (b) Scenarios

from other access points, construction of the building, and obstructions, and seeks to only vary distance/Signal-to-Noise Ratio (SNR).

4.2 Performance Analysis and Discussion

Initially, we measured the Round Trip Time (RTT) of each packet. In addition, we employed NetStumbler [17] to measure the Signal-to-Noise Ratio (SNR), and Wireshark [25] to verify: *i)* packets sent to and received by each device (i.e., the wireless client, ad-hoc server, WAP, and target systems), and *ii)* that the client communication remained anonymous as all packets seemed to originate from the last hop (in this case the WAP).

Table 1 shows our preliminary results. In particular, due to the wireless transmission, we observe a wide variation in latency, mainly due to interference and physical obstacles. Table 1 gives also the average RTT values from which all graphs are evaluated (each value is calculated over more than 25 measurements collected).

The results in Table 1 indicate that there is no significant latency overhead when the SNR is within acceptable bounds. However, the ad-hoc connection becomes much less reliable in weak areas. Figure 7 depicts

Table 1. Maximum, Minimum and Average RTT Values, and Packet Loss Percentages: (a) one-hop WiFi connection, and (b) two-hop WiFi connection

(a)

SNR	**RTT (ms)**			**Packet Loss (%)**
	Min	**Max**	**Avg**	
14	-	-	-	100
19	3	52	7	0
25	1	28	4	0
28	1	188	63	0
33	1	47	3	0
48	1	33	4	0
55	1	97	23	0
64	1	8	3	0

(b)

SNR	**RTT (ms)**			**Packet Loss (%)**
	Min	**Max**	**Avg**	
14	-	-	-	100
23	-	-	-	100
31	1	9	3	4
33	1	245	63	0
35	1	13	1	0
47	1	44	5	0
51	1	55	6	3
66	3	104	19	0

scattergraphs of the data sets, with the anomalous peaks representing inconsistencies due to physical obstacles. Figure 7 confirms that peaks in latency due to physical obstacles occur at the same location for all WiFi connections. This is not a measurement inconsistency but rather a verification of the jittery nature of the wireless communications in which physical obstacles affect the transmission even when the distance or the SNR reported by the device remains constant. Moreover, we believe that the RTT measurements are more immediate than the SNR reported by the device which is measured over a period of time. That is why we see this discrepancy of having a good SNR but degraded RTT measurements.

In conclusion, ad-hoc WiFi connections do not seem to suffer much of a performance hit in adding an intermediary node since almost all of our measurements stayed below 5ms of round trip time (or 2.5ms single trip). This allows to safely claim that our system is both deployable and practical even for latency-sensitive applications such as video or voice streaming. However, we must acknowledge that the signal seems unreliable in degraded SNR, so that we might consider using another node with better connectivity. Nodes acting as ad-hoc servers with lower power and bandwidth, such as cellphones instead of laptops, would incur in a performance loss, which may present itself in the form of packet loss and intermittent connectivity, such as was observed in the ad-hoc connection as SNR worsened. While waiting for a ping response, the client node was seen to hang for long periods before announcing an error. This is an issue of QoS because, for example, a page that would attempt to load for some time before displaying an error, or a call that would suspend for some time before finally disconnecting. In using a MultiNet-like technol-

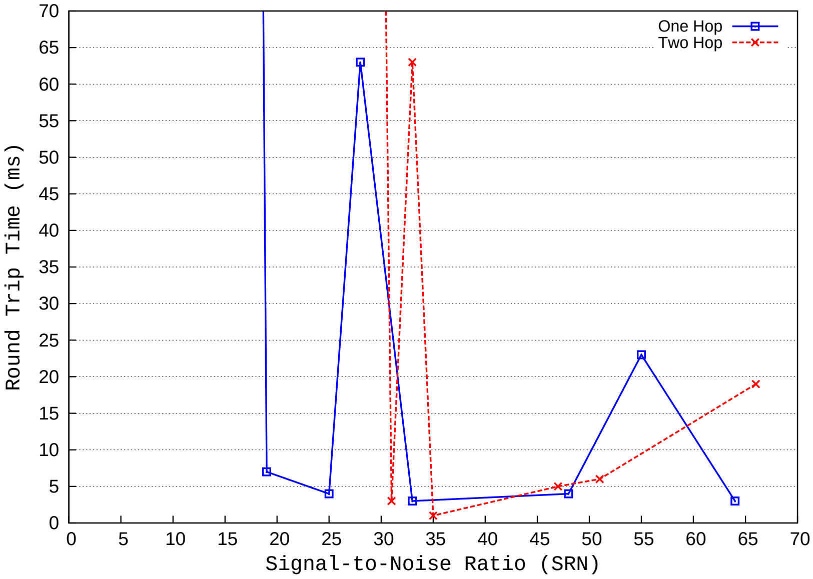


Fig. 7. Comparison Between Graph of SNR vs. RTT (ms) in One-Hop Scenario (in red) and in Two-Hop Scenario (in green). Notice that there is a shift in the graph to the right for two-hops indicating an increase in SNR from the extra hop. Also, there are two symmetric peaks indicating a loss of packets due to physical obstacles.

ogy [23], we could switch between connections, further anonymizing the packet stream. In general, there are a lot of open questions regarding the performance of the entire system, especially under an adversarial model where some of the peers are uncooperative or even malicious.

5 Related Work

While mobile networks and their management have been considered in several works in the area of mobile applications, approaches aimed at protecting the privacy of users have gained great relevance only in the last few years. Recent research in the context of mobile networks approached the privacy problem from different perspectives and have been inspired by works on fully anonymous communications [6, 7, 19].

Anonymous Communications. Chaum introduces the concept of "Mix" to provide source anonymity [6]. A mix collects a number of messages from different sources, shuffles them, and forwards them to the next destination in a random order. This solution makes the tracking of a message difficult for the attackers. In mix-based solution, the path is statically determined by the message sender. Onion routing is a solution that built on the notion of mix network [8]. In onion routing, the connection initiator creates an onion and the path of the connection through the network. Each router (named onion router) in the path knows its successor and can remove a layer of encryption to the onion with its private key. At the end, the data reach the final destination in plaintext. For instance, TOR [8] is an onion routing-based solution that provides route anonymity, by preventing adversaries from following packets from the source to the destination and vice versa. Crowds [19] is an anonymizing solution designed for Web-communications where the routing path and length is dynamically generated. The paths is determined randomly by the machines used in the communications.

An important characteristic shared by the above solutions that makes them not applicable in a mobile scenario like ours is that they use the path generated by the sender for both the request and the response. This assumption cannot be applied in mobile networks where users are moving fast over time and then the path used for the request is likely to be not available both for the response. Also, onion routing solutions are different from our approach because, each onion proxy is required to know the network topology and public certificates of routing nodes to create meaningful routes. Finally, Crowds focuses on protecting the sender's anonymity against the service providers and cannot protect anonymity against a global eavesdropper. Our approach, instead, exploits the hybrid nature of the devices to create a local network which is impervious against global eavesdroppers that operate in the cellular network (e.g., mobile network operators). Since the WiFi network is ad-hoc and of limited range, it is very difficult to have a global eavesdropper that would cover both the WiFi and cellular communications.

Anonymous Mobile Ad-Hoc Routing Protocols. Another line of research has focused on preserving the privacy of wireless traffic by studying and providing privacy-enhanced and anonymous routing protocols. Originally, the proposed mobile ad-hoc routing protocols, such as AODV [18] and DSR [14], were not designed to provide or guarantee privacy and route anonymity but rather they were aimed at increasing network performance, efficiency, security and reliability. As a consequence, in such protocols, there are many ways to compromise privacy; for instance, by abusing the protocol state since both source and destination together with hop-count are stored on each node. Subsequent work focused on routing protocols for mobile ad-hoc networks and attempted to protect anonymity and privacy. They did so by keeping secret the identities of the senders and recipients of messages from intermediate nodes. A number of anonymous routing protocols have been proposed [5, 15, 26, 27, 29, 30]. Among them, MASK [30] proposes an anonymous on demand routing protocol, which provides both MAC-layer and network-layer communications without the need of releasing real identities of the participating nodes. ANODR [15] provides route anonymity, by preventing adversaries from following packets to its source or destination, and location privacy, by preventing the adversary to discover the real identities of local transmitters. Discount-ANODR [27] limits the overhead introduced by ANODR in providing source anonymity and routing privacy. It provides a lightweight protocol based on symmetric key encryption and onion routing. Capkun et al. [20] provide a scheme for secure and privacy-preserving communication in *hybrid* ad-hoc networks. Their scheme provides the users with a means to communicate in a secure environment and preserve their anonymity and location privacy. Although our solution has similar goals and considers privacy issues in hybrid mobile networks, it is not aimed at providing a new routing protocol. Our k-anonymity solution using a multi-path communication paradigm provides privacy of the requester from the neighbors sharing the media, the mobile network operators, and the service providers. Also our solution does not heavily rely on key encryption, dynamic keys or pseudonyms; rather, it exploits the possibility of breaking a single data stream in several different packets, and of using neighbor mobile peers, which act on behalf of the request originator, to distribute these packets.

Location *k*-Anonymity. More recently, another line of research has focused on protecting the location privacy and anonymity of users that interact with Location-Based Services (LBSs) [1, 2]. The main goal of most of the current solutions [16] is to protect users' identities associated with or inferred from location information. In this case, the best possible location measurement can be provided to other entities but users identity must be kept hidden. In particular, these solutions are based on the notion of k-anonymity in data [21], which is aimed at making an individual (i.e., her identity or personal information) not identifiable by releasing a geographical area containing at least k-1 users other than the requester. In this way, the request cannot be associated to fewer than k respondents and the identity of the users is not released to the LBSs. Bettini et al. [3] propose a framework for evaluating the risk of disseminating sensitive location-based information, and introduce a technique aimed at supporting k-anonymity. Gruteser and Grunwald [12] propose a middleware architecture and an adaptive algorithm to adjust location information resolution, in spatial or temporal dimensions, to comply with a specific k-anonymity requirement. Gedik and Liu [10] describe a k-anonymity model and define a message perturbation engine responsible for providing location anonymization of user's requests through identity removal and spatio-temporal obfuscation of location information. Ghinita et al. propose PRIVÈ [11], a decentralized architecture for preserving query anonymization, which is based on the definition of k-anonymous areas obtained exploiting the Hilbert space-filling curve. Hashem and Kulik [13] provide a decentralized approach to location privacy in a wireless ad-hoc network, where each peer is responsible for generating its cloaked area by communicating with others peers, thus providing anonymity. Existing works on location k-anonymity have the following main disadvantages: *i)* they rely on either a centralized middleware for providing anonymity functionalities (centralized approach) or let the burden of the complexity in calculating the k-anonymous area to the users (decentralized approach); *ii)* they assume trusted mobile network operators; *iii)* they do not support accountability. In our approach, we protect the privacy of the users acting in a hybrid network including cellular networks. Here, we assume untrusted mobile network operators, which could track users activities [28], and we provide location k-anonymity at network level rather than at application level.

6 Conclusions and Future Work

We presented a novel privacy-preserving scheme based on network k-anonymity and multi-path that aims at balancing privacy and accountability without assuming any trusted entity between the user and the service provider. Furthermore, we put forward the idea that a reliable privacy solution should protect users against threats stemming from honest but curious mobile network operators. Our vision is then to re-cast privacy for hybrid networks and provide a privacy-assurance mechanism based on network k-anonymity that: *i)* protects users' privacy against honest but curious mobile network operators; *ii)* conceal or obfuscate the users location to service providers, *iii)* enforces user and service accountability. Note that, our solution can be integrated with obfuscation techniques, as the one in [2], to protect the location privacy of the users interacting with LBSs.

Many interesting research directions that warrant further investigation, among which: the enhancement of the decision forwarding algorithms for guaranteeing reliability and efficiency; the consideration of a comprehensive threat model including malicious and uncooperative peers; the complete implementation and extensive testing of our prototype; the consideration of economic incentives for the neighbor peers to participate in our anonymizing network.

Acknowledgments

This work was supported in part by the EU, within the 7th Framework Programme (FP7/2007-2013) under grant agreement no. 216483 “PrimeLife” and by the Italian MIUR, within PRIN 2006, under project no. 2006099978 “Basi di dati crittografate”.

References

1. C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Supporting location-based conditions in access control policies. In *Proc. of the ACM Symposium on Information, Computer and Communications Security (ASIACCS'06)*, Taipei, Taiwan, March 2006.
2. C.A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and S. Samarati. Location privacy protection through obfuscation-based techniques. In *Proc. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, Redondo Beach, CA, USA, July 2007.
3. C. Bettini, X.S. Wang, and S. Jajodia. Protecting privacy against location-based personal identification. In *Proc. of the 2nd VLDB Workshop on Secure Data Management*, Trondheim, Norway, 2005.
4. Nikita Borisov, George Danezis, Prateek Mittal, and Parisa Tabriz. Denial of service or denial of security? In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 92–102, New York, NY, USA, 2007. ACM.
5. A. Boukerche, K. El-Khatib, L. Xu, and L. Korba. Sdar: A secure distributed anonymous routing protocol for wireless andmobile ad hoc networks. In *Proc. of the 29th Annual IEEE International Conference on Local Computer Networks (LCN 2004)*, pages 618–624, Tampa, FL, USA, October 2004.
6. D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.
7. D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.
8. R. Dingledine, N. Mathewson, and P. Syverson. Tor: The Second-Generation Onion Router. In *Proceedings of the* 13^{th} *USENIX Security Symposium*, pages 303–319, August 2004.

9. T. Fujiwara and T. Watanabe. An ad hoc networking scheme in hybrid networks for emergency communications. *Ad Hoc Networks*, 3(5):607–620, 2005.
10. B. Gedik and L. Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1–18, January 2008.
11. G. Ghinita, P. Kalnis, and S. Skiadopoulos. Privè: Anonymous location-based queries in distributed mobile systems. In *Proc. of the International World Wide Web Conference (WWW 2007)*, Banff, Canada, May 2007.
12. M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. of the 1st International Conference on Mobile Systems, Applications, and Services (MobiSys 2003)*, San Francisco, CA, USA, May 2003.
13. T. Hashem and L. Kulik. Safeguarding location privacy in wireless ad-hoc networks. In *Proc. of the 9th International Conference on Ubiquitous Computing (UbiComp 2007)*, Innsbruck, Austria, September 2007.
14. D. B. Johnson and D. A. Maltz. *Dynamic Source Routing in Ad Hoc Wireless Networks*, volume 353. Kluwer Academic Publishers, 1996.
15. J. Kong and X. Hong. ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In *Proc. of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC 2003)*, pages 291–302, Annapolis, MD, USA, June 2003.
16. S. Mascetti and C. Bettini. A comparison of spatial generalization algorithms for lbs privacy preservation. In *Proc. of the 1st International Workshop on Privacy-Aware Location-based Mobile Services (PALMS 2007)*. IEEE Computer Society, 2007.
17. *NetStumbler.com*. `http://www.netstumbler.com/`.
18. C.E. Perkins and E.M. Royer. Ad-hoc on demand distance vector routing. In *Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA99)*, New Orleans, LA, USA, February 1999.
19. M.K. Reiter and A.D. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.
20. J.-P. Hubaux S. Capkun and M. Jakobsson. *Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks*, January 2004.
21. P. Samarati. Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6):1010–1027, 2001.
22. *Sphinx - A Hybrid Network Model for Next Generation Wireless Systems*. `http://www.ece.gatech.edu/research/GNAN/work/sphinx/sphinx.html`.
23. Angelos Stavrou and Angelos D. Keromytis. Countering dos attacks with stateless multipath overlays. In *CCS '05: Proceedings of the 12th ACM conference on Computer and communications security*, pages 249–259, New York, NY, USA, 2005. ACM.
24. L. von Ahn, A. Bortz, and N.J. Hopper. k-anonymous message transmission. In *Proc. of the 10th ACM Conference on Computer and Communication Security (CCS 2003)*, pages 122–130, Washingtion, DC, USA, October 2003.
25. *Wireshark*. `http://www.wireshark.org/`.
26. X. Wu and B. Bhargava. Ao2p: Ad hoc on-demand position-based private routing protocol. *IEEE Transaction on Mobile Computing*, 4(4), July/August 2005.
27. L. Yang, M. Jakobsson, and S. Wetzel. Discount anonymous on demand routing for mobile ad hoc networks. In *Proc. of the Second International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006)*, Baltimore, MD, USA, August-September 2006.

28. C. Zander. *'CIA CELL TOWER' Monitors Local Internet Users' Wireless Transmissions*, September 2007. `http://www.send2press.com/newswire/2007-09-0911-003.shtml`.
29. Y. Zhang, W. Liu, and W. Lou. Anonymous communication in mobile ad hoc networks. In *Proc. of the 24th Annual Joint Conference of the IEEE Communication Society (INFOCOM 2005)*, Miami, FL, USA, March 2005.
30. Y. Zhang, W. Liu, W. Lou, and Y. Fang. Mask: Anonymous on-demand routing in mobile ad hoc networks. *IEEE Transaction on Wireless Communications*, 5(9), September 2006.