Requirements for Privacy-Enhancements in Mobile Ad Hoc Networks

Christer Andersson, Leonardo A. Martucci, Simone Fischer-Hübner

Department of Computer Science, Karlstad University
Universitetsgatan 2, 65866 Karlstad, Sweden
{christer.andersson, leonardo.martucci, simone.fischer-huebner}@kau.se

Abstract: This paper formulates requirements for anonymous overlay networks for enhancing the privacy of mobile ad hoc network users. Besides, it analyzes existing peer-to-peer based anonymous overlay networks and shows that none of them are compliant with those requirements. Finally, it outlines the ongoing design of an anonymous overlay network intended for mobile ad hoc environments.

1 Introduction

Mobile ad hoc networks are constituted of mobile platforms that establish on-the-fly wireless connections among themselves, and ephemera networks without central entities to control it. Mobile ad hoc networks are an important building block in the fields of ubiquitous computing and sensor networks, two upcoming technologies that promise revolutionary services for the everyday citizen, as they allow instant networking between mobile devices without the interference or aid of central devices for network establishment.

However, applications based on mobile ad hoc networks also provide many challenges to privacy. When running applications on top of mobile ad hoc networks, vast amounts of possibly sensitive data are being transmitted among the participating mobile devices. Also, traffic information generated inside such networks can reveal sensitive information about the users, such as behavioral patterns or the locations of their communication partners. Finally, since MobileIP allows users to utilize existing web applications inside mobile ad hoc networks, users also run the risk of being profiled or pinpointed by web servers.

The purpose of this paper is to analyze how privacy can be enhanced in mobile ad hoc networks with the means of anonymous overlay networks, which are outlined in section 2. A number of requirements are derived in section 3 that an anonymous overlay network must fulfill in order to be suitable for mobile ad hoc environments. As peer-to-peer (P2P) based interactions are preferred to client-server based interactions in mobile ad hoc environments, section 4 analyzes to what degree existing proposals for P2P-based anonymous overlay networks are compliant with the characteristics of mobile ad hoc networks. Finally, section 5 briefly discusses the ongoing design of an anonymous overlay network intended for mobile ad hoc environments.

2 A Possible Solution: Using Anonymous Overlay Networks

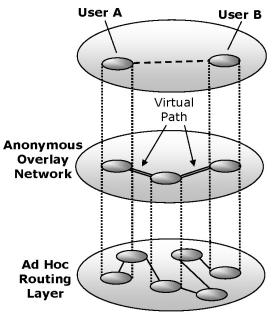

Figure 1: Anonymous communication between two nodes using an anonymous overlay network.

As a countermeasure against potential privacy problems in mobile ad hoc networks, we introduce an *anonymous overlay network* between the ad hoc routing layer and the application layer (see Figure 1) to provide anonymous communication services. Generally, an *overlay network* is a virtual network that is built on top of an existing network in order to implement network services not available in the existing network. In our case, the purpose of the overlay network is to provide all participants in the mobile ad hoc network with the means of anonymous communication. Being "anonymous" could imply both that a person's actions cannot be linked to his identity, and that it is hidden with whom he is communicating.

Many different kinds of overlay networks exists for providing anonymous communication, ranging from Chaum's classical Mixes [Ch81] for email communication to newer P2P-based approaches, such as MorphMix [RP02] and Herbivore [Go03]. Most of them work by routing encrypted messages through chains of nodes, often called *virtual paths*, in order to hide both the identity of the sender and the relation between the sender and the recipient. On its path to the recipient, the outlook of a message is usually changed at each intermediate node by the means of encryption. In the cases when an anonymous overlay network employ a P2P-based model, it is the users themselves that constitute the nodes in the virtual paths.

Making use of an anonymous overlay network in mobile ad hoc environments would allow a user to be anonymous towards both other members of the anonymous overlay network (who may or may not be a part of that user's virtual path) and people in the whereabouts not participating in the network. It would also allow a user to be anonymous towards parties that are not part of the mobile ad hoc network, but still involved in the transactions, such as web servers on the Internet.

3 Requirements for Anonymous Overlay Networks

The most relevant characteristics of mobile ad hoc networks include: (1) heterogeneous mobile devices with different capabilities regarding embedded resources, (2) on-the fly establishment of network data links through wireless interfaces without the aid of any central entity or dynamic topologies, (3) resource availability and network services are defined by the network devices themselves, and finally (4) end devices are responsible to provide routing and packet forwarding while also guaranteeing their own security. Taking these characteristics into consideration, a number of requirements can be defined that an anonymous overlay network should meet in order to be suitable for mobile ad hoc environments:

- `Requirement R1:` *The anonymous overlay network must scale well.* The network must function well even with a large number of participants.
- `Requirement R2:` *The anonymous overlay network must provide the users with strong anonymity properties.* For instance, the network must provide adequate protection against malicious users and local (and preferably also global[1]) attackers.
- `Requirement R3:` *The anonymous overlay network must be fair regarding the distribution of workload among the participants.* Alternatively, some incentives must be given to accept a higher portion of the work load.
- `Requirement R4:` *The anonymous overlay network must provide acceptable performance.* Thus, the network should preferably be "lightweight" (for example, generate few messages and few public key operations).
- `Requirement R5:` *The anonymous overlay network must employ a P2P model.* Dependency on central hardware/services is not allowed in ad hoc networks.
- `Requirement R6:` *The overlay network must handle an dynamic topology.* In a mobile ad hoc network, nodes are frequently entering or leaving the network.

4 An Evaluation of State-of-the-Art Anonymous Overlay Networks

As stated above, the anonymous overlay network in our proposal should employ a P2P model. The most notorious anonymous overlay networks that rely on P2P interactions include: Crowds, Hordes, Tarzan, MorphMix, Herbivore and P^5. Crowds [RR97] is a lightweight overlay network that achieves anonymity by hiding one user's action within the actions of many users (in a so-called "crowd"). The crowd then issues requests to end servers on behalf of its members. Hordes [SL00] functions essentially like Crowds when sending messages to the web server, but uses multicast on the way back. Unlike Hordes and Crowds, Tarzan [FM02] uses layered encryption and cover traffic to be resistant against a global attacker. MorphMix [RP02] tries to provide strong anonymity without the use of cover traffic[2]. Herbivore [Go03] combines an approach based on Chaum's DC nets [Ch89] with a hierarchical topology in which the users are grouped into smaller subsets (so-called "cliques"). In P^5 [SBS02], participants send fixed length packets onto hierarchically tree-structured broadcasts channels at a fixed rate.

Table 1 below highlights the main results[3] that were generated when the aforementioned anonymous communication mechanisms were evaluated against the requirements listed in section 3. The table lists all the requirements that seem problematic to fulfill for each studied technology together with a brief motivation. In conclusion, it seems that none of the studied anonymous communication mechanisms are fully suitable for use in mobile ad hoc environments.

[1] A global attacker has the possibility to eavesdrop on all traffic circulated in the overlay network.

[2] Traffic (lacking meaningful content) primarily employed to confuse potential eavesdroppers.

[3] Preliminary results of an earlier version of this evaluation is available at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.3.study_on_mobile_identity_management.pdf.

Table 1: Evaluation of P2P-based anonymous overlay networks.

Crowds	R2-	The attacker model in Crowds does not consider global attackers. Also, since each intermediary node decrypts and re-encrypts each packet, the level of confidentiality towards other nodes on the virtual path is limited.
	R5-	Crowds does not employ a true P2P-model as membership management and key distribution are handled by a centralized server.
Tarzan	R2-	The mechanism in Tarzan preventing malicious nodes from colluding (based on IP subnets) is not compliant with mobile ad hoc environments.
	R4-	Tarzan relies on cover traffic to protect against a global attacker.
Hordes	R2-	Hordes offers the same anonymity properties as Crowds, and thus, does not consider a global attacker.
	R5-	Similar to Crowds, membership management and key distribution are handled by a central server.
MorphMix	R2-	The attacker model assumes that a global attacker does not exist, and therefore does not protect against such an attacker.
	R3-	When building a virtual path between a node a and b, an additional node w, which is not part of the virtual path, must always act as a "witness".
	R4-	MorphMix transmits many messages when establishing its virtual paths, namely $6L + (L-2)(L+1)$ messages, where L is the number of nodes in the virtual path. Moreover, it needs four times more public key operations than Tarzan when constructing the paths.
	R6-	Path rebuilding is not efficiently done when a node leaves. Instead, the whole virtual path is rebuilt.
Herbivore	R4-	Practical experiments in [Go03] indicate a high latency when many nodes are sending simultaneously.
	R5-	The minimum and maximum size of a clique needs to be centrally administrated.
	R6-	Although constituting an interesting concept, especially in the context of interconnected ad hoc domains, Herbivore's current topology based on cliques does not seem to be suitable for highly dynamic topologies.
P^5	R3-	Users near the root of the P^5 tree have a greater workload (and a stronger level of anonymity) than those located in the leaves of the tree. However, it is not possible to increase the desired level of anonymity during operation by migrating towards the root, since once the desired level of anonymity is chosen, it cannot be increased.
	R4-	P^5 relies heavily on cover traffic. Moreover, one public-key operation is required at a node for each received packet.
	R5-	In order to set the centrally administrated a-priori value determining the depth of the P^5 binary three, the expected number of participants in the anonymous overlay network is required beforehand.

5 Conclusions & Outlook

In order to guarantee privacy in usage scenarios based on mobile ad hoc networks, novel anonymity technologies must be developed, or existing ones need to be accordingly adapted. We are currently designing an anonymous overlay network suited for mobile ad hoc environments. Based on the analysis in previous section, the lightweight protocol Crowds seemed an appropriate choice for an underlying base. This initial version of the protocol will then be modified to make it fully suitable for mobile ad hoc environments. For example, new key distribution solutions [Ma04] will be used to remove the need for a central server, and if a node in the path is leaving the network, the path will be rebuilt using as few operations as possible. Besides, we will elaborate on how to protect against global eavesdroppers without significantly reducing the performance. Finally, we will study how to hinder a malicious user from compromising an anonymous overlay network by using multiple IP addresses per device in order to increase the proportion of malicious nodes in the network (for example by using virtual interfaces).

References

[Ch81] Chaum, D.: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, Communication of the ACM, 24 (2), 1981; pp. 84-88.

[Ch89] Chaum, D.: The Dining Cryptographers Problem: unconditional sender and recepient untraceability, J. Cryptography, 1 (1), 1988; pp. 65-75.

[FM02] Freedman, M.J; Morris, R.: Tarzan: A Peer-to-Peer Anonymizing Network Layer. Published in Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), Washington, DC, USA, 2002.

[Go03] Goel, S. et. al.: Herbivore: A Scalable and Efficient Protocol for Anonymous Communication. Technical Report 2003-1890, Cornell University, Ithaca, NY, February, 2003.

[Ma04] Martucci, L.A. et. al.: A Trust-Based Security Architecture for Small and Medium-Sized Mobile Ad Hoc Networks. In: Proceedings of the 3rd Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net. June 2004. Bodrum, Turkey; pp. 278-290.

[RP02] Rennhard, M.; Platter, B.: Introducing MorphMix: Peer-to-Peer based Anonymous Internet usage with Collusion Detection. In: Proceedings of the Workshop on Privacy in Electronic Society (WPES). Washington, DC, USA, 2002.

[RR97] Reiter, M.; Rubin, A.: Crowds: Anonymity for Web Transactions. Published in DIMACS Technical report, 1997; pp. 97-115.

[SBS02] Sherwood, R.; Bhattacharjee, B.; Srinivasan, A.: P5: A protocol for scalable anonymous communication. In Proceedings of the 2002 IEEE Symposium on Security and Privacy, May, 2002. Oakland, CA, USA; pp.58-70

[SL00] Shields, C.; Neil Levine, B.: A Protocol for Anonymous Communication Over the Internet. In Proceedings of the 7th ACM Conference on Computer and Communications Security, November, 2000; pp 33-42.