Chapter 7
Anonymous Communication

ABSTRACT
Schemes of anonymous communication enable entities to send or receive their messages without disclosing their identities to others including managers of communication systems and receivers or senders of the messages. Among various existing schemes this chapter introduces Crowds, DC net, Mix-net, ESEBM (Enhanced Symmetric key Encryption Based Mix-Net), and Onion Routing. Mechanisms to protect anonymous communication systems from malicious entities are also discussed.

INTRODUCTION
Identities of message senders or receivers are sometimes as sensitive as messages themselves. For example, a company may acquire highly confidential information about its rival companies from identities of their customers and suppliers. Therefore, the importance of anonymous communication is increasing as more people are being involved in network based communication. Anonymous communication mechanisms enable entity S that sends message M or entity R that receives M, to exchange M without disclosing their identities to others. According to subjects to be made anonymous, there are 3 types of anonymous communication schemes, i.e. when S can send M without disclosing its identity, the mechanism is called sender anonymous, when R can receive M without disclosing its identity, it is called receiver anonymous, and when both S and R can exchange M without disclosing their identities it is called mutually anonymous. This chapter mainly discusses sender anonymous communication mechanisms because receiver and mutually anonymous ones can be developed based on them, and except in the last section of this chapter, the word anonymous communication is used for representing the sender anonymous communication.

Now, (sender) anonymous communication mechanisms enable entity S to send message M to its receiver R without disclosing the identity of S to any entity except S including R and managers.
Anonymous Communication of the communication channel. Here, message $M$ usually reaches $R$ from $S$ while being relayed by multiple entities as shown in Figure 1, because when $M$ reaches $R$ directly from $S$, $R$ can easily know the source $S$. In the remainder, entities that send messages and receive messages are called senders and receivers, respectively. Also entities that relay messages are called relay servers or simply servers.

The requirements for sender anonymous communication are summarized as follows, i.e.

1. No one except sender $S$ itself can identify the sender of massage $M$,
2. No one except sender $S$ itself can know that messages $M_1$ and $M_2$ sent from $S$ are the messages sent from the same sender,
3. Sender $S$ can confirm the successful delivery of its message $M$ to receiver $R$ without disclosing its identity to others,
4. Sender $S$ can receive reply messages to its message $M$ from receiver $R$ without disclosing its identity to any other entity, and
5. Communication channels can protect themselves from accesses from unauthorized entities.

Firstly as the most important requirement, sender $S$ must be concealed not only from receiver $R$ but also from any other entities including wiretappers, managers of the communication channels such as relay servers, etc. About the 2nd requirement, although this is satisfied automatically when the 1st one is satisfied in many cases, it is important because a set of messages sent from a same sender usually include a lot of information to identify the sender. The 3rd and the 4th requirements are also important, and especially the 4th one is essential because information exchanges between entities in many kinds of important applications are carried out as conversations between them. Satisfying the 3rd requirement is not so difficult, e.g. senders can confirm the deliveries of their messages when receivers put signals designated by the senders at the specified subs in BBs after the arrivals of their messages so that the senders can notice them. Also, anonymous message reply mechanisms automatically make communication channels satisfy the 3rd requirement, i.e. senders can confirm their message deliveries when they receive replies. However, development of practical mechanisms that satisfy the 4th requirement is not easy as it looks. For example, $R$, which generates its reply message $M_R$ and knows its contents, can identify sender $S$ by eavesdropping on the communication channel connected to possible senders including $S$. Namely, $R$ can identify $S$ as the entity to which $M_R$ is delivered, where it must be noted that identifying an entity that receives $M_R$ is not difficult for $R$ when it is conspiring with the server that finally delivers messages. About the 5th requirement, because entities are anonymous,

Figure 1. Configuration of Crowds
Related Content

Reducing Risk Through Inversion and Self-Strengthening

Protecting Privacy by Secure Computation: Privacy in Social Network Analysis
[www.igi-global.com/chapter/protecting-privacy-secure-computation/61504?camid=4v1a](www.igi-global.com/chapter/protecting-privacy-secure-computation/61504?camid=4v1a)

Managing the Commonplace: Small Water Emergencies in Libraries
[www.igi-global.com/article/managing-the-commonplace/148213?camid=4v1a](www.igi-global.com/article/managing-the-commonplace/148213?camid=4v1a)

Behavioral Modeling of Malicious Objects in a Highly Infected Network Under Quarantine Defence