Acimn protocol: A protocol for Anonymous Communication In Multi hop wireless Networks

Volker Fusenig, Dagmara Spiewak, and Thomas Engel
University of Luxembourg
Faculté des Sciences, de la Technologie et de la Communication
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
{Volker.Fusenig, Thomas.Engel, Dagmara.Spiewak}@uni.lu

Abstract

Anonymity is the state of not being identifiable within a set of subjects. Different strategies exist for assuring anonymity in computer networks, such as the Dining Cryptographers network and Mix networks. But these strategies were designed for wired networks requiring direct communication links or fixed infrastructure. Therefore they are not applicable to multi hop wireless networks without modification. The Acimn protocol bases on the combination of these two main strategies enabling nodes to communicate anonymously among each other. Every node of the network acts as a mix so that the Mix approach can be used to hide the multi hop communication. By using this technique only one message overhead per communication path is generated because of the key establishment among the nodes on the path. During following communications only little computational power is needed by every node on the path to decrypt the messages before forwarding them to the next node. Additionally every one hop communication is kept anonymously by using the DC-net protocol. Therefore the nodes are arranged in groups of at most three members that are in communication range of each other. Sending of messages takes place in rounds where in every round only one group member is able to transmit information but every member has to send data. Because of the maximal group size of three there can be maximally three times more messages compared to the sending without the DC-net approach. By utilizing the combination of both techniques neither non participating eavesdropper nor nodes on the communication path are able to track the communication partners while the overhead is kept small.