Security for Future Wireless and Decentralized Communication Networks – Harnessing Cooperation, Space, and Time

André König, Matthias Hollick, Ralf Steinmetz
[Andre.Koenig; Matthias.Hollick; Ralf.Steinmetz]@KOM.tu-darmstadt.de
Multimedia Communications Lab (KOM), Technische Universität Darmstadt

Wireless and decentralized networks enable enhanced communication services beyond the borderlines of ‘traditional’ centralized, infrastructure-based systems. As an example, projects have been initiated that scrutinize the applicability of a combination of mobile ad hoc networks (MANETs) and Peer-to-Peer (P2P) systems to support on-site units in highly dynamic emergency response scenarios. This new class of networks demands for new security mechanisms. Due to the wireless and infrastructureless nature, MANETs and P2P systems lack the well defined network borders and the central trusted instances on which security mechanisms (Gateways, Firewalls, etc.) deployed in ‘traditional’ environments are based. Thus, these security mechanisms cannot be transferred directly. In our work, we present security mechanisms that cope with the challenging conditions in wireless and decentralized systems. We show how cooperative decisions can counterbalance missing central instances and how networks being aware of space and time constraints can survive without well defined network borders.

I. Harnessing Cooperation

Security mechanisms that ensure objectives such as authentication and access control are commonly based on central trusted instances. In decentralized P2P systems, the (constant) availability of these central trusted instances cannot be taken as granted. Making security relevant decisions jointly, by a set of authorized peers, is a promising approach to counterbalance missing central trusted instances. This way, a security level that is comparable to that of contemporary security mechanisms can be achieved.

The mathematical foundation for a joint decision process is given by threshold cryptography or multisignatures. Both techniques can be utilized to enforce the cooperation of a specific number $n_{threshold}$ of peers to perform cryptographic operations such as signing certificates that enable the access to restricted resources. Threshold cryptography allows for anonymous voting, whereas multisignatures render the voting traceable and enable a detailed mapping of administrative hierarchies to the structure of the network.

Predefined security policies for any security relevant decision possible will most likely not be available regarding the highly dynamic application domain targeted. Thus, a user interaction may well be required. Minimizing the number $n_{request}$ of users requested for one joint decision is an obvious optimization goal. To describe the trade-off between $n_{request}$ and the probability p_{succ} that a joint decision is successful (i.e. enough peers w.r.t. $n_{threshold}$ issued their votes within a reasonable amount of time), as shown in Figure 1, we developed stochastic models. The derived closed-form description of these models serves as a tool allowing for the online adaptation of key parameters which control the success of joint decisions while guaranteeing low overhead in the network.

II. Harnessing Space and Time

Establishing networks without an infrastructure, as it is done in a MANET, requires an accurate cooperation of the nodes involved. Effects of misbehaviour, may it be intended or not, can lead to a massive disruption of the network’s services.

A prominent example of (intended) misbehaviour in MANETs is the black hole attack. In analogy to a black hole in astronomy, a black hole in a MANET draws data, which is dropped instead of being forwarded to the actual receiver. Very few of such black hole nodes are sufficient to cause a breakdown of the entire network.

Preventing any misbehaviour possible is hardly feasible. Prevention strategies, though thoroughly designed, have been shown to be susceptible to attacks, recently. However, reactive security measures like intrusion detection systems combined with intrusion response mechanisms offer a promising means to mitigate the effects of misbehaviour in MANETs. While intrusion detection systems have been studied comprehensively, only minor attention has been paid to how to react to intrusions detected. Mostly, response mechanisms which exclude adversaries detected from the network based on their addresses have been proposed. Since devices in MANETs are beyond the control of a central instance, changing addresses is possible with little effort. This way, address-based intrusion response approaches can be subverted easily. For this reason, we have proposed *GeoSec,* a location-based intrusion response strategy. By setting up temporal quarantine zones in areas where misbehaviour has been detected, network traffic is redirected and, thus, is geographically kept away from misbehaving nodes. Figure 2 shows *GeoSec*’s performance compared to a defenseless network and to an address-based response strategy, subject to the data that is dropped by black hole nodes.

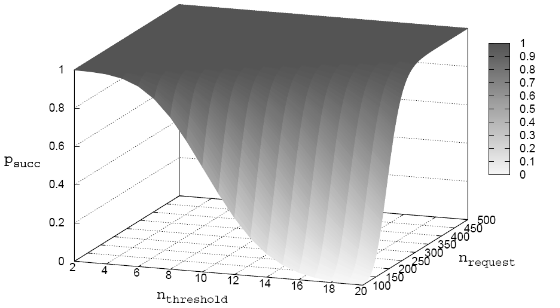

Figure 1: Success probability for cooperative decisions

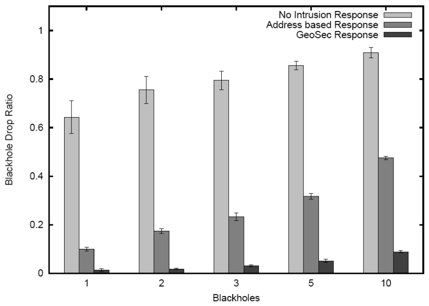

Figure 2: Address-based vs. location-based intrusion response