Providing bi-directional anonymity using unstructured overlay networks

In this research problem, we try to provide a methodology that provides bi-directional anonymity over unstructured overlay networks. By bi-directional, we mean that anonymity is provided not only to the request message but also to the reply message. Neither the sender of the request message nor the sender of the reply message, therefore, is not supposed to be aware of the real-life identity of each other. Part of delivery networks in between may know the identity of either the requester or the replier. No part of the delivery networks, however, is not able to recognize the identities of both. This type of anonymity will be required in many future applications in digital society. Electronic voting may be a good example of this class of applications. The reason for using unstructured overlay networks, for example, Gnutella, is its popularity. Structured ones may provide a better way of limiting upper bounds of message delivery time. Intuitively speaking, this may require impractical co-operation among participants, which may need to grow in scale of millions. While unstructured ones are easy to build and maintain, its uncontrollability may be a significant challenge for its advanced use in future applications, for example, anonymity. While innovative solutions are sought, the scope of solutions is rather open. Solutions to a limited scope of the research problem will still be welcomed.
2 Unstructured overlay networks: An effective measure against DDoS

DDoS is a cyber attack that tries to exhaust either network bandwidth of a target system or a target system’s internal resources such as memory and CPU cycles. Intuition says that if network paths to a target are capable of doing something good to protect targets, the effectiveness of DDoS will be (significantly) lower. Overlay networks may be a good candidate methodology to organize network paths reaching to a target for the purposes. In this research problem, therefore, a novel methodology is solicited, which is able to organize participants in an unstructured way, like Gnutella, and enforce some security measures, and finally drop attack packets some where in the middle of overlay networks before they can successfully reach a target through the overlay networks. Solutions to a limited scope of the research problem will still be welcomed.

3 Dynamic topology for efficient routing in wireless ad-hoc mobile sensor networks

Bluetooth is one of the promising technologies for ad-hoc mobile sensor networks. Although it has large potential for wide adoption everywhere in the future, advanced algorithms and protocols for its general use have not been either standardized or fully investigated. While routing and packet forwarding have been studied rather independently of applications in wired networks, these are tightly coupled with applications in wireless ad-hoc mobile sensor networks. Therefore, the logical and physical network topology for routing and packet forwarding needs to change according not only to geographical requirements but also to applications requirements. Moreover, in advanced applications, sensor nodes will be able to move to better carry out the well defined tasks. Changing logical and physical network topologies, therefore, a prime interest in an early stage of wireless ad-hoc mobile sensor networks research. In this research problem, innovative solutions are solicited on algorithms and protocols for dynamic topology change. Solutions to a limited scope of the research problem will still be welcomed.