Abstract

Ad hoc network is created with a purpose for a temporary period. Author terms ad hoc network of sensor nodes as wireless sensor network (WSN). Since there is no pre-existing infrastructure in an ad hoc network, formation of network by network elements (for example, sensor node) has to be initiated by itself. This is called as self organization. Self organization requires a network element to have some unique characteristics such as routing/forwarding of packets, ability to decide whether to join a network or not. There are, however many challenges to this self organization approach. Especially when this is used in classified application such as WSN. A self organizing WSN may be used in different areas. For example, in monitoring ecosystem, industry, or in emergency such as fire, earthquake or medical. Depending upon the sensitivity of application, security is one of the biggest challenges for a self organizing WSN. It is very difficult, if not impossible, to prevent a malicious network element such as sensor node or a powerful base station from joining in an ad hoc network. If by means of proper authentication a malicious node is prevented from joining the network, there can be flooding attack where the network will be starved with resources such as band width and energy. Therefore, self organization of an ad hoc network needs to be secure enough so that a malicious node cannot join the network and there is no external attacker to starve the network. Security comes with cost; meaning if better security is provided then cost in terms of resource consumption such as energy, memory will be more. It is also commonly observed that security is inversely proportional to performance. For an ad hoc network application such as WSN, performance is equally important as the security is. In this thesis work author investigates the problems of secure self organization of ad hoc network of sensor nodes (or WSN) and give solution to this problem. First of all, the process of self organization in a WSN is defined and divided into three phases: node discovery, node joining and data communication. Author proposes a node discovery algorithm based on a unique triangulation method. Proposed solution considers need based approach to security while self organizing the ad hoc network and subsequently provides three modes for security: low, medium and high. Accordingly, three different schemes for node joining is proposed. Finally, for data communication a scheme is described for end to end security of data. As a secure network needs a complete framework of its own to avoid attack, therefore a solution to the key management problem is also provided for a self organizing WSN. Further, author discusses how to carry out security planning for a WSN in this thesis.