

# 4040-849 OPTIMIZATION METHODS

## PROJECT PROPOSAL

Christopher Wood

April 11, 2012

### **Abstract**

Key distribution is a vital part of wireless ad-hoc communication networks that need to transfer text, audio, and video data both securely and efficiently. Traditionally, key agreement protocols are based upon the commonly known Diffie Hellman key exchange protocol, in which two (or more) parties may exchange public information in order to establish a common key. The problem with this approach is that it is very computationally inefficient, and doesn't lend itself directly to the problem of establishing a single common group key among multiple parties in a group. This is especially true in wireless ad-hoc networks where the nodes themselves have constrained processing and power resources.

For this reason, key agreement schemes for this specific type of network typically rely on pre-placed information that can be easily distributed to members of the group in order to establish a common group key. Therefore, at the physical layer of the network, where the group topology is represented as a single spanning tree, it is important that the latency of sending data between two nodes is as small as possible in order to ensure the fastest transmission of data. Depending on the radio propagation model and specific waveform used to propagate the digital data via an analog signal to each of the nodes, the structure of this tree can have a drastic impact on the time it takes to distribute a specific piece of data from node to every other node in the group.

Therefore, the purpose of this project is to minimize the time it takes this data to transmit to every other node in the group depending on the following parameters:

1. Number of slots available in the TDMA scheme
2. Maximum number of nodes in the network
3. Maximum number of node children allowed in the spanning tree
4. Data packet size
5. Radio channel bandwidth