Implementation of Diffie-Hellman in UDOO

Sahaj Biyani and Sachin Rathod
{sahajbiyani,rathod}@cs.ucsb.edu

April 23, 2015

1 Abstract

DiffieHellman key exchange (DH) is a specific method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle[1]. The DiffieHellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel.

In this project, we aim to implement the D-H algorithm in C programming language on the UDOO[2] development board. Our first main goal is to have a fully operational D-H implementation running on the UDOO and communicating with a remote client. We will measure the overall speed of the algorithm in the basic implementation, using some set of predefined values. These measurements will be used as baseline measurements for the rest of the project.

We will then modify the basic implementation with improved algorithms and measure the performance after modifications. We will then be able to conclude what benefit each improvement have on the algorithm compared to the added complexity.

References

1. Merkle, Ralph C: "Secure Communications Over Insecure Channels". Communications of the ACM 21 (4): 294299. doi:10.1145/359460.359473. Received August, 1975; revised September 1977
2. www.udoo.org