E0314

CRIPTOGRAFIA EFICIENTE PARA REDES DE SENSORES SEM FIO

Felipe Gomes Daguano (Bolsista PIBIC/CNPq) e Prof. Dr. Ricardo Dahab (Orientador), Instituto de Computação - IC, UNICAMP

Redes de Sensores Sem Fio (RSSFs) são redes ad hoc compostas basicamente por pequenos sensores de recursos limitados e uma ou mais estações rádio base, as quais são mais poderosas e conectam os sensores com o ambiente externo. Tais redes podem ser utilizadas para diferentes aplicações, tais como operações de resgate em áreas de conflito e/ou desastre, espionagem industrial e detecção de exploração ilegal de recursos naturais. Como qualquer outro tipo de rede ad hoc sem fio, RSSFs são vulneráveis a ataques. Porém, devido a sua maior escassez de recursos e o ambiente em que são executadas, essas redes são ainda mais vulneráveis. O baixo poder computacional dos sensores torna inviável a utilização de algoritmos de Criptografia de Chave Pública (PKC) convencionais (RSA/DSA, por exemplo). Nesse trabalho, investigou-se o emprego de técnicas mais eficientes de PKC, especificamente a criptografia baseada em curvas elípticas (ECC) e, dentro de ECC, o uso da Encriptação Baseada em Identidade (IBE). Através da análise e escolha de parâmetros no contexto de RSSFs, e da implementação de algoritmos de emparelhamentos de Tate e esquemas simples de IBE em sensores de recursos limitados, pudemos verificar a viabilidade de IBE para RSSFs, além da sua natural aplicabilidade nesse contexto.

Redes de sensores sem fio - Criptografia - Emparelhamentos bilineares