Avaliando Protocolos de Criptografia Baseada em Emparelhamentos em Redes de Sensores Sem Fio

*Leonardo B. Oliveira[1], Felipe Daguano[1], Ricardo Dahab[1]

[1] Instituto de Computação – UNICAMP

{leob,daguano,rdahab}@ic.unicamp.br

Abstract. *The advent of Pairing-Based Cryptography (PBC) has enabled a wide range of new cryptographic solutions. Recently, pairing computation was shown to be feasible in resource-constrained nodes. In this work, we propose to assess costs of complete PBC protocols and present the cost for one of them in particular. To the best of our knowledge, our work is the first to measure costs of complete PBC protocols on 8-bit sensor nodes.*

Resumo. *Criptografia Baseada em Emparelhamentos é uma nova primitiva criptográfica que despertou enorme interesse da comunidade internacional de criptografia, pois possibilita o projeto e utilização de esquemas criptográficos originais e muito elegantes, além de tornar mais eficientes protocolos já conhecidos. Bem recentemente foi mostrado que o cálculo de emparelhamentos é viável em redes de sensores sem fio. Contudo, custos de protocolos inteiros não foram apresentados. Neste trabalho, propomos aferir o custo total de protocolos baseados em emparelhamentos e apresentamos, até onde sabemos, as primeiras medidas de custos para um de seus protocolos em nós sensores de 8-bits.*

1. Introdução

Redes de Sensores Sem Fio (RSSFs) são redes *ad hoc* compostas basicamente por pequenos sensores de recursos limitados (pouca energia, largura de banda, capacidade computacional etc.) e uma ou mais estações rádio base (ERBs), as quais são mais poderosas e conectam os sensores com o ambiente externo. RSSFs são utilizadas com o objetivo de monitorar regiões, oferecendo dados sobre a área monitorada para o resto do sistema. Dentre suas aplicações estão operações de resgate em áreas de desastre e detecção de exploração ilegal de recursos naturais.

Como qualquer outro tipo de rede *ad hoc*, RSSFs são vulneráveis a ataques. Porém, além das vulnerabilidades já existentes em redes *ad hoc*, RSSFs enfrentam problemas adicionais. Elas comumente são dispostas em ambientes abertos, muitas vezes hostis, o que as tornam fisicamente acessíveis a adversários. Não obstante, nós sensores são mais escassos de recursos que nós de redes *ad hoc* (o nó sensor MICAz Motes, por exemplo, possui um processador de 7.38 MHz e 4 KB de memória RAM, e soluções convencionais não lhes são adequadas. Por exemplo, o fato de que nós sensores devem ser descartáveis e, por conseguinte, de baixo custo torna pouco viável equipá-los com dispositivos contra violação (*tampering*). Logo, dotar RSSFs de segurança é uma tarefa especialmente desafiadora.

Nesta conjuntura, um evento auspicioso foi o surgimento da Criptografia Baseada em Emparelhamentos (*Pairing-Based Cryptography* – PBC) [Sakai et al. 2000]. PBC

*Financiado pela FAPESP, processo 2005/00557-9.

é uma nova primitiva criptográfica que vem despertando enorme interesse da comunidade internacional de criptografia, pois possibilita o projeto e utilização de esquemas criptográficos originais e muito elegantes, além de tornar mais eficientes protocolos já conhecidos. Dentre essas aplicações está a Encriptação Baseada em Identidade (*Identity-Based Encryption* – IBE) [Boneh and Franklin 2003]. IBE foi originalmente proposta por Shamir [Shamir 1984], mas só se tornou viável com o advento de PBC.

Recentemente foi mostrado [Oliveira et al. 2007] que o cálculo de emparelhamentos é, de fato, viável em RSSFs. Tal resultado é importante pois abre uma nova gama de possibilidades para a área de segurança e criptografia em RSSFs. Contudo, custos totais de protocolos de PBC ainda são desconhecidos. Neste trabalho, nós (i) propomos aferir o custo total de protocolos inteiros de PBC; e (ii) apresentamos os custos para a execução completa do protocolo de IBE no MICAz – a mais nova geração dos nós MICA *motes*. Até onde sabemos, nosso trabalho é o primeiro a calcular o custo total de IBE em uma plataforma de nós sensores de 8 bits.

O restante deste documento está organizado da seguinte maneira. Primeiramente, apresentamos os trabalhos correlatos na Seção 2. Em seguida, na Seção 3, introduzimos como alguns protocolos de PBC podem ser aplicados às RSSFs. Resultados premilinares são apresentados na Secão 4. Finalmente, concluímos e descrevemos os trabalhos futuros na Seção 5.

2. Trabalhos Correlatos

O número de propostas de segurança para RSSFs cresceu consideravelmente nos últimos anos. Devido às restrições de espaço, focaremos aqui apenas os trabalhos especialmente voltados para Criptografia de Chave Pública (*Public-Key Cryptography – PKC*).

Os trabalhos sobre PKC em RSSFs mostram tentativas tanto de adequar algoritmos convencionais (RSA, por exemplo) para nós sensores, como o uso de técnicas mais eficientes (ECC, por exemplo). Watro *et al.* [Watro et al. 2004] propuseram TinyPK. Na distribuição de chaves, TinyPK atribui aos nós sensores as eficientes operações públicas RSA, enquanto as operações privadas RSA, mais caras, são designadas a entidades externas dotadas de maior poder computacional. Gura *et al.* [Gura et al. 2004] apresentaram resultados sobre ECC e RSA em microcontroladores ATmega128 e mostraram a superioridade de desempenho do primeiro sobre o segundo. Nesse caso, a implementação de ECC utilizava corpos primos. Já Malan *et al.* [Malan et al. 2004] implementaram ECC utilizando corpos binários e base polinomial, e apresentaram resultados do protocolo de Diffie-Hellman baseado no ECDLP.

Os trabalhos acima mostraram que nós sensores são capazes de computar operações de PKC, mas outros problemas – como por exemplo a autenticação de chaves públicas – não foram foco de pesquisa. Motivadas por isso, novas propostas têm surgido ([Zhang et al. 2005, Doyle et al. 2006], por exemplo) visando tratar tais questões. Zhang *et al.* [Zhang et al. 2005] utilizaram emparelhamentos e IBE para distribuição de chaves em RSSFs. Eles acreditavam que emparelhamentos eficientes em nós sensores seria algo factível a curto-prazo e, com isso, não se preocuparam com detalhes de implementação. O trabalho de Doyle *et al.* [Doyle et al. 2006] foi também voltado ao uso de IBE e apresentou resultados de simulação para aferir custos de cálculo de emparelhamentos. O trabalho, entretanto, considera uma classe de nós sensores com grande poder computacional. Finalmente, recentemente Oliveira *et al.* [Oliveira et al. 2007] mostraram que o cálculo de emparelhamentos é viável mesmo em plataformas de nós sensores extremamente limitadas. Contudo, o trabalho só apresenta números para o cálculo de emparelhamentos e não considera custos para a execução de protocolos como um todo.

3. Protocolos de PBC em RSSFs

PBC é uma nova tendência em criptografia pois proporciona uma nova gama de esquemas criptográficos [1]. Em seguida, listamos alguns desses esquemas e brevemente discutimos porque seriam interessantes no contexto de RSSFs.

Assinaturas Agregadas. protocolos de assinaturas agregadas ([Bellare et al. 2006], por exemplo) permitem, dados certos requisitos, a "fusão" de múltiplas assinaturas em uma somente. Tais assinaturas são atraentes para RSSFs pois consomem menos largura de banda e, com isso, poupam energia dos nós sensores. Além disso, a forma com a qual o roteamento é feito em RSSFs (isto é, em estrutura de árvore) e a usual agregação de dados que é feita em direção à ERB faz com que assinaturas agregadas pareçam uma primitiva feita sob medida para RSSFs.

Cifrassinatura. protocolos de cifrassinatura ([Barreto et al. 2005], por exemplo) são especialmente atraentes para RSSFs pois permitem a execução de duas primitivas criptográficas (isto é, encriptação e assinatura) em um só protocolo. Isto torna o processo mais rápido e poupa energia de nós sensores em redes em que encriptação e assinatura são requeridas.

Encriptação Baseada em Identidade: hoje, esquemas inspirados em Identidade ([Boneh and Franklin 2003], por exemplo) parecem ser a única maneira prática de prover encriptação de chave pública em RSSFs, uma vez que não demanda uma infra-estrutura de chaves públicas. Ao invés disso, o esquema emprega identificadores unívocos dos usuários (o ID de um sensor, por exemplo), como chaves públicas.

4. Resultados

Nesta seção, apresentamos resultados para a execução completa do protocolo IBE no MICAz, a mais nova geração dos nós sensores MICA motes. O MICAz é dotado do microcontrolador ATmega128 (8-bit/7.38 MHz, 4KB SRAM, 128KB *flash*). Novamente, devido às restrições de espaço, não descreveremos as questões de implementação por completo. Aqui, apenas esclarecemos que o protocolo IBE utilizado é o de Boneh e Franklin [Boneh and Franklin 2003] e que nossa implementação emprega a biblioteca TinyTate [Oliveira et al. 2007]. Para mais detalhes sobre a implementação, pedimos para que o leitor se refira ao trabalho TinyTate [Oliveira et al. 2007], uma vez que empregamos a biblioteca com os os mesmos parâmetros do trabalho que a apresentou.

IBE: custos		
Tempo (segundos)	**RAM (bytes)**	**ROM (bytes)**
80,37	1.904	20.918

Tabela 1: Custos da execução completa do protocolo IBE no MICAz.

Os resultados da Tabela 1 foram medidos em um MICAz rodando TinyOS. O tempo médio de execução para se efetuar o protocolo IBE completo (isto é, encriptação e decriptação) é de 80,37s. Os custos em termos de memória RAM e ROM (*flash*) são de 1.904 e 20.918 $bytes$, respectivamente. É importante lembrar que IBE, muito provavelmente, será empregada apenas para distribuir chaves simétricas e, a partir de então, toda a criptografia será feita utilizando essas chaves. Portanto, os custos acima não são, absolutamente, um fardo para o sistema como um todo.

[1] Em função das restrições de espaço não aprofundaremos em definições e referências.

5. Conclusão

Apesar de anos de pesquisa, as áreas de segurança e criptografia em RSSFs ainda possuem um grande número de problemas em aberto. PBC, por sua vez, é uma área emergente, promissora, e que possibilita uma nova gama de esquemas criptográficos. Neste trabalho, propomos aferir o custo total de protocolos de PBC e apresentamos números preliminares sobre o custo de um de seus protocolos, isto é, sobre IBE.

Este é um trabalho em andamento e diversas frentes estão em ação a fim de finalizá-lo. Uma delas é implementar a computação do emparelhamento em corpos binários, o que pode tornar o cálculo mais eficiente. Outra é a implementação dos demais protocolos, como cifrassinatura e assinatura agregada. Finalmente, planejamos também apresentar resultados referentes aos custos em termos de energia para todos os protocolos.

Referências

Barreto, P. S. L. M., Libert, B., McCullagh, N., and Quisquater, J.-J. (2005). Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. In Roy, B., editor, *Asiacrypt 2005*, pages 515–532. Springer.

Bellare, M., Namprempre, C., and Neven, G. (2006). Unrestricted aggregate signatures. Cryptology ePrint Archive, Report 2006/285. `http://eprint.iacr.org/`.

Boneh, D. and Franklin, M. (2003). Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615. Also appeared in CRYPTO '01.

Doyle, B., Bell, S., Smeaton, A. F., McCusker, K., and O'Connor., N. (2006). Security considerations and key negotiation techniques for power constrained sensor networks. *The Computer Journal (Oxford University Press)*, 49(4):443–453.

Gura, N., Patel, A., Wander, A., Eberle, H., and Shantz, S. C. (2004). Comparing elliptic curve cryptography and rsa on 8-bit cpus. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES'04)*, pages 119–132.

Malan, D. J., Welsh, M., and Smith, M. D. (2004). A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks*.

Oliveira, L. B., Aranha, D., Morais, E., Daguano, F., López, J., and Dahab, R. (2007). TinyTate: Computing the tinytate in resource-constrained nodes. In *6th IEEE Int'l Symposium on Network Computing and Applications*. To appear.

Sakai, R., Ohgishi, K., and Kasahara, M. (2000). Cryptosystems based on pairing. In *Symposium on Cryptography and Information Security (SCIS2000)*, pages 26–28.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *CRYPTO'84: on Advances in cryptology*, pages 47–53. Springer-Verlag.

Watro, R., Kong, D., Cuti, S., Gardiner, C., Lynn, C., and Kruus, P. (2004). Tinypk: securing sensor networks with public key technology. In *2nd ACM Workshop on Security of ad hoc and Sensor Networks (SASN'04)*, pages 59–64.

Zhang, W. L., Lou, W., and Fang, Y. (2005). Securing sensor networks with location-based keys. In *IEEE Wireless Communications and Networking Conference (WCNC'05)*.