Distribuição de Chaves Criptográficas em Redes de Sensores Sem Fio

Leonardo B. Oliveira[1], **Orientador: Professor Ricardo Dahab**[1]

[1]Instituto de Computação – Universidade Estadual de Campinas (Unicamp)
Caixa Postal 6.176 – 13083-970 – Campinas – SP – Brasil

{leob,rdahab}@ic.unicamp.br

Abstract. *Wireless Sensor Networks (WSNs) have enabled applications in which security properties are of paramount importance. Security, in turn, is frequently bootstrapped through key distribution schemes. Most of the key distribution techniques, however, are ill-suited to WSNs. This makes extremely hard and challenging the objective of securing WSNs. In this work, we aimed at proposing key distribution schemes that are both (i) lightweight and (ii) able to fulfill architecture-specific needs. To our knowledge, ours is the first work in performing authenticated key distribution in WSNs in a non-interactive way through the use of Pairing-Based Cryptography.*

Resumo. *Redes de Sensores Sem Fio (RSSFs) possuem aplicações críticas nas quais propriedades de segurança são de vital importância. Segurança, por sua vez, é comumente alavancada através de esquemas de distribuição de chaves. A maioria dos padrões de distribuição de chaves presentes na literatura, todavia, não são apropriados para RSSFs. O objetivo deste trabalho foi propor soluções de distribuição de chaves que, concomitantemente, (i) fossem compatíveis com os recursos dos sensores e (ii) considerassem as particularidades das arquiteturas para as quais são propostas. Até onde sabemos, nosso trabalho foi o pioneiro em empregar Criptografia Baseada em Emparelhamentos para distribuição de chaves de forma autenticada e não interativa em RSSFs.*

1. Introdução

Redes de Sensores Sem Fio (RSSFs) (Estrin et al. 1999) são um tipo particular de Redes Móveis Ad hoc (*Mobile Ad hoc Networks* – MANETs). Elas são compostas em sua maioria por pequenos nós (*nodes*) sensores cujos recursos (energia, largura de banda, processamento etc.) são extremamente limitados. Estes sensores, por sua vez, se conectam com o mundo externo por meio de dispositivos poderosos chamados de sorvedouros (*sink*) ou Estações Rádio Base (ERBs). RSSFs são utilizadas para monitorar regiões, fornecendo dados sobre a área monitorada, também chamada de *área de interesse (interest area)* para o resto do sistema. Dentre sua vasta gama de aplicações estão operações de resgate em áreas de conflito e/ou desastre, espionagem industrial e detecção de exploração ilegal de recursos naturais. Ainda vale mencionar que, em 2003, ocorreu um *workshop* (NSF 2003) patrocinado pelo *National Science Foundation* para identificar tópicos de pesquisa fundamentais em redes e a área de RSSFs foi um dos seis selecionados. Paralelamente, aqui no Brasil, a área RSSFs foi também elencada como tema de pesquisa prioritário (Loureiro 2006).

Embutir segurança em RSSFs é uma tarefa complexa, muito desafiadora, e essencial em muitas aplicações. Por exemplo, fazendeiros e indústrias que lançarem mão das redes para monitorar sua cadeia de plantações e suprimento, respectivamente, desejarão manter os dados monitorados secretos, impedindo que os mesmos cheguem ao conhecimento de competidores. Ademais, autenticação – outra propriedade de segurança – poderá ser útil até mesmo em RSSFs domésticas, evitando que sensores de redes vizinhas interajam entre si acidentalmente.

Idealmente, um esquema de segurança para RSSFs tem que prover perfeita conectividade e resiliência. Em outras palavras, sensores devem ser capazes de (i) comunicar-se com quaisquer outros sensores de forma segura e (ii) os danos do comprometimento de um sensor devem ficar restritos ao mesmo – note-se que essas propriedades têm que ser satisfeitas mesmo para sensores que foram dispostos [1] em diferentes momentos. Ademais, o esquema deve ser de baixo custo tanto em termos de processamento, como de comunicação e armazenamento.

Segurança, por sua vez, é comumente alavancada (*bootstrapped*) através de esquemas de distribuição de chaves. A maioria dos padrões de distribuição de chaves presentes na literatura, todavia, não são apropriados para RSSFs (Perrig et al. 2002): métodos baseados em esquemas de chave pública convencionais, devido aos seus requisitos de processamento e banda; chaves de grupo, em função das suas vulnerabilidades de segurança; chaves par-a-par (*pairwise*), por causa da sua baixa escalabilidade.

Em suma, realizar o acordo de chaves em em RSSFs é uma tarefa especialmente desafiadora e fundamental para a ampla adoção da tecnologia de RSSFs. O objetivo deste trabalho é, portanto, propor soluções de distribuição de chaves que, concomitantemente, (i) sejam compatíveis com os recursos dos sensores e (ii) considerem as particularidades das arquiteturas para as quais são propostas. Em particular, propusemos três diferentes soluções de distribuição de chaves: LHA-SP, SecLEACH e TinyPBC. Iniciamos o trabalho com soluções personalizadas para certas arquiteturas de RSSFs e evoluímos para soluções mais flexíveis em que a segurança é alavancada de forma não interativa, o que é ideal para este tipo de rede. Até onde sabemos, este trabalho é pioneiro em soluções de segurança para RSSFs hierárquicas e o primeiro a realizar distribuição de chaves não interativa usando Criptografia Baseada em Emparelhamentos (*Pairing-Based Cryptography* – PBC) (Sakai et al. 2000) em RSSFs. Neste documento, em razão da limitação de espaço, focaremos apenas nesta última solução (TinyPBC) e , portanto, recomendamos que o leitor se refira ao primeiro capítulo da nossa tese para uma visão geral de todas as soluções.

Este documento está organizado da seguinte forma. Na Seção 2 descrevemos quantitativamente as contribuições. Subsequentemente, na Seção 3, apresentamos uma das soluções. Por fim, concluímos os resultados na Seção 4. Mencionamos também que a versão completa da tese encontra-se em:
`http://sites.google.com/site/barbosaleonardo/Home/tese-LBOliveira.pdf`

2. Contribuições

Cientes da dificuldade de se mensurar a nossa contribuição (tanto em função da abrangência do concurso, que engloba diversas áreas da Ciência da Computação, como

[1] Neste documento, empregaremos o verbete dispor como tradução do inglês *deploy*.

das restrições de espaço do documento) achamos conveniente mencionar fatos que atestam a relevância do trabalho em questão. Além das publicações listadas abaixo [2], fomos agraciados com o prêmio *Microsoft PhD Fellowship Award*[3] e tivemos passagens por grupos excelência, tais como o *Cryptography Group/Dublin City University*, o *Information Security Group/University of London* e o *Networked Embedded Computing Group/Microsoft Research*.

2.1. Publicações Internacionais: Capítulos & Periódicos

1) **L. B. OLIVEIRA** *et al.*. *On the Identity-Based Encryption for Sensor Networks.* Handbook of Wireless Mesh and Sensor Networking. McGraw-Hill International, NY.

2) **L. B. OLIVEIRA** *et al.*. *P2P over MANETs: Application and Network Layers Routing Assessment*. Handbook on Mobile P2P Computing for Next Generation Distributed Environments: Advancing Conceptual and Algorithmic Applications. IGI Global.

3) D. Hora, D. Macedo, **L. B. OLIVEIRA** *et al.*. *Enhancing Peer-to-Peer Content Discovery Techniques over Mobile Ad Hoc Networks*. Elsevier computer communications. To appear.

4) **L. B. OLIVEIRA** *et al. SecLEACH - On the Security of Clustered Sensor Networks, Signal Processing* (Elsevier pub.). Volume 87, issue 12, 2007 (pages 2882–2895).

5) **L. B. OLIVEIRA** *et al.*. *On the Design of Secure Protocols for Hierarchical Sensor Networks.* International Journal of Security and Networks (IJSN). Special Issue on Cryptography in Networks. Volume 2, issue 3/4, 2007 (p. 216-227) – índice de aceite: 17%.

6) **L. B. OLIVEIRA** *et al.*. *On the Performance of Ad hoc Routing Protocols under a Peer-to-Peer Application.* Journal of Parallel and Distributed Computing (JPDC). Volume 65, Issue 11, November 2005 (p. 1337-1347).

2.2. Publicações Internacionais: Anais de Congressos

1) **L. B. OLIVEIRA** *et al.* Authenticating Node to Multi-user Communication in Shared Sensor Networks. The 8th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN'08) – índice de aceite: 21%.

2) **L. B. OLIVEIRA** *et al.* TinyPBC: Pairings for Authenticated Identity-Based Non-Interactive Key Distribution in Sensor Networks. 5th International Conference on Networked Sensing Systems (INSS'08). Sponsored by IEEE. 2008 – índice de aceite: 21%.

3) P. Szczechowiak, **L. B. OLIVEIRA**, *et al.*. NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks, European conference on Wireless Sensor Networks (EWSN'08). Lecture Notes in Computer Science. 2008 – índice de aceite: 21%.

4) **L. B. OLIVEIRA** *et al.*. *TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes.* 6th IEEE International Symposium on Network Computing and Applications (NCA'07). 2007.

5) **L. B. OLIVEIRA** *Identity-Based Cryptography for Sensor Networks.* 5th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'07). 2007.

6) **L. B. OLIVEIRA** *et al*. *SOS: Secure Overlay Sensornets.* 5th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'07). 2007.

7) **L. B. OLIVEIRA**. *SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks.* 5th IEEE International Symposium on Network Computing and Applications (NCA'06). 2006 – índice de aceite: 35%.

8) **L. B. OLIVEIRA**. *Pairing-Based Cryptography for Sensor Networks.* 5th IEEE International Symposium on Network Computing and Applications (NCA'06). 2006 (fast abstract).

9) A. Mota, **L. B. OLIVEIRA**. *WISENEP: A Network Processor for Wireless Sensor Networks.* 11th IEEE Symposium on Computers and Communications (ISCC'06). 2006.

10) **L. B. OLIVEIRA**. *LHA-SP: Secure protocols for Hierarchical Wireless Sensor Networks.* 9th IFIP/IEEE International Symposium on Integrated Network Management (IM'05). 2005 – Top ranked paper – índice de aceite: 23.5%.

11) Adrian C. Ferreira, Marco A. Vilaca, **L. B. OLIVEIRA**. *On the Security of Cluster-Based Communication for Wireless Sensor Networks.* 4th IEEE International Conference on Networking (ICN'05). Lecture Notes in Computer Science. Springer, 2005.

12) **L. B. OLIVEIRA**. *Evaluation of Peer-to-Peer Network Content Discovery Techniques over Mobile Ad Hoc Networks.* IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM'05). 2005.

2.3. Publicações Nacionais

1) D. Aranha, D. Camara, J. Lopez, **L. B. OLIVEIRA**, and R. Dahab. *Implementação eficiente de criptografia de curvas elípticas em sensores sem fio*. 8th Brazilian Symposium on Information and Computer System Security (SBSeg'08). 2008.

[2] Optamos por listar as publicações aqui, separadas das demais referências, para pouparmos espaco.

[3] Tal prêmio é concedido a apenas dois alunos de doutorado da América Latina por ano.

2) **L. B. OLIVEIRA** *et. al.* . Daguano, and R. Dahab. *Avaliando Protocolos de Criptografia Baseada em Emparelhamentos em Redes de Sensores Sem Fio*. 7th Brazilian Symposium on Information and Computer System Security (SBSeg'07). 2007.

3) **L. B. OLIVEIRA** *et. al.*. *SOS: Sensoriamento Overlay Seguro em Redes de Sensores Sem Fio Hierárquicas*. 6th Brazilian Symposium on Information and Computer System Security (SBSeg'06). 2006.

4) **L. B. OLIVEIRA** *et. al.*. *SecLEACH - Uma Solução Segura de Distribuição de Chaves para Redes de Sensores Sem Fio Hierárquicas*. 5th Brazilian Symposium on Information and Computer System Security (SBSeg'05). 2005.

5) **L. B. OLIVEIRA** *et al.*. *Avaliação de Técnicas de Descoberta de Conteúdo em Redes Peer-to-Peer sobre Redes Móveis Ad hoc*. 23rd Brazilian Symposium on Computer Networks (SBRC'05). 2005.

6) **L. B. OLIVEIRA** *et al*. *Um Protocolo de Segurança para Redes de Sensores Hierárquicas* 22nd The Brazilian Symposium on Computer Networks (SBRC'04). 2004. – índice de aceite: 25%.

3. Solução

3.1. Definição

Formalmente, emparelhamentos são definidos da seguinte maneira. Seja ℓ um inteiro positivo. Sejam $\mathbb{G}_1$ e $\mathbb{G}_2$ grupos aditivos de ordem ℓ com identidade $\mathcal{O}$, e seja $\mathbb{G}_T$ um grupo multiplicativo de ordem ℓ com identidade 1. Um *emparelhamento bilinear* é uma função $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$, computável, não-degenerativa, cuja propriedade mais importante para criptografia é a bilinearidade, dada por

$$\forall\, P \in \mathbb{G}_1, \forall\, Q \in \mathbb{G}_2 \text{ e } \forall\, a, b \in \mathbb{Z}_\ell^*, \text{ temos que } e([a]P, [b]Q) = e(P, Q)^{ab}.$$

Na prática, os grupos $\mathbb{G}_1$ e $\mathbb{G}_2$ são implementados usando subgrupos de pontos de curvas elípticas e o grupo $\mathbb{G}_T$ é implementado usando um grupo finito multiplicativo.

A seguir discorremos sobre a sinergia entre RSSFs e IBC (Seção 3.2) e explicamos como esquemas de IBC baseados em PBC poderiam ser empregados para alavancar a segurança em RSSFs (Seção 3.3).

3.2. Sinergia entre RSSFs e IBC

A Criptografia Baseada em Emparelhamentos (PBC) (Sakai et al. 2000) é uma nova tecnologia que vem despertando enorme interesse da comunidade internacional de Criptografia, pois propicia projetos de esquemas criptográficos originais, além de tornar protocolos já conhecidos mais elegantes e eficientes. Não obstante, por meio da PBC, problemas antes em aberto puderam ser resolvidos elegantemente. Talvez a mais fascinante de suas aplicações seja a Cifração Baseada em Identidade (*Identity-Based Encryption* – IBE) (Boneh and Franklin 2003), a qual por sua vez possibilitou por completo esquemas de Criptografia Baseada em Identidade (*Identity-Based Criptography* – IBC) [4] (Shamir 1984).

IBC foi originalmente proposta por Shamir (Shamir 1984), mas só se tornou viável com o advento de PBC. Diferentemente das demais propostas de PKC, em que PKIs e verificação de certificados são demandados, em IBC chaves públicas são derivadas de informações conhecidas (públicas) que univocamente identificam o usuário (seu endereço de correio eletrônico ou o IP da máquina onde trabalha, ou mesmo seu CPF ou RG, por exemplo) e, por conseguinte, dispensam mecanismos de autenticação. Grosso modo, as chaves são "auto-autenticáveis".

Alguém pode então se perguntar por que IBC ainda não é amplamente utilizada em sistemas de segurança. Bem, além do tempo usual que novas tecnologias levam para

[4]Note-se que atualmente existem também outras formas de se construir um esquema de IBE.

ser de fato adotadas, isso se deve a algumas inconveniências da IBC. Particularmente, IBC requer uma Autoridade de Confiança (*Trusted Authority* – TA) a qual é responsável por gerar e manter a custódia das chaves privadas do sistema. Ou seja, ela é capaz de personificar qualquer usuário. Por esta razão, uma TA tem que ser uma entidade de inteira confiança de todos os usuários do sistema. O problema é que na maioria dos sistemas computacionais, infelizmente, não existem elementos com tamanho grau de confiança.

Em RSSFs, entretanto, isso não é um problema. O "dono" (*deployer*) da rede – aquele que carrega o *software* nos sensores, os dispõe em áreas de interesse e analisa os dados coletados – é, obviamente, de confiança. No mundo das RSSFs, esse papel de dono é protagonizado por uma ERB. As ERBs são dispositivos dotados tanto de alto poder computacional, como de proteção física. Em outras palavras, elas são ideais para o papel de TAs.

Outra exigência da IBC é que chaves devem ser entregues aos usuários através de canais confidenciais e autenticados. No entanto, se o mecanismo de criptografia estiver sendo usado para alavancar (*bootstrap*) o esquema de segurança – o que usualmente é o caso – tais canais ainda não existem. Mas, novamente, isso não chega a ser um problema em RSSFs. Em seu modelo de segurança, existe claramente um período de tempo – isto é, antes da disposição (*deployment*) – em que há, sim, canais seguros entre sensores e as ERBs. Portanto, além do *software* da aplicação, chaves privadas podem ser carregadas nos sensores antes dos mesmos serem dispostos.

3.3. Configuração

Para se principiar um esquema de IBC, a TA necessita primeiro gerar e distribuir chaves públicas e seus parâmetros. Grosso modo, esse procedimento pode ser realizado da seguinte maneira. Primeiro, a ERB gera uma chave mestra secreta s e então calcula as chaves pública e privada de cada um dos sensores. Para tal, ela mapeia cada identidade dos sensores para um ponto distinto da curva elíptica utilizando uma função *hashing-and-mapping* ϕ, de forma que para cada sensor X sua chave pública é dada por $P_X = \phi(id_X)$. A seguir, para cada sensor X, a TA computa sua chave privada $S_X = [s]P_X$ e o carrega com a seguinte informação: (i) O identificador id_X do sensor; (ii) A chave privada S_X do sensor.

Cada sensor é também equipado com a função ϕ de forma que qualquer um deles, de posse de um certo identificador (por exemplo id_Y), pode calcular a chave pública correspondente a este identificador (por exemplo P_Y). Observe que, além da ERB, apenas o sensor X conhece a chave S_X.

3.4. TinyPBC: Distribuição de Chaves Não-Interativa Baseada em Identidade

Agora, suponha que os sensores A e B que conhecem os identificadores um do outro [5] desejem acordar em uma chave secreta. Eles podem então empregar o protocolo não interativo de distribuição de chaves baseado em PBC (Sakai et al. 2000).

Lembre-se (Seção 3.3) que as chaves privadas de A e B são $S_A = [s]P_A$ e $S_B = [s]P_B$, respectivamente. Consequentemente, pela bilinearidade (Seção 3.1), temos que

[5]Essa é uma premissa bem razoável posto que o algoritmo de roteamento já requer que os sensores saibam os identificadores um do outro.

$$\begin{aligned}\hat{e}(S_A, P_B) &= \hat{e}([s]P_A, P_B) \\ &= \hat{e}(P_A, P_B)^s \\ &= \hat{e}(P_A, [s]P_B) \\ &= \hat{e}(P_A, S_B) \\ &= \hat{e}(S_B, P_A).\end{aligned}$$

Observe que A possui S_A e pode então computar $P_B = \phi(id_B)$. De forma análoga, B possui S_B e pode então computar $P_A = \phi(id_A)$. Desta forma, ambos A e B são capazes de computar a chave secreta

$$k_{A,B} = \hat{e}(S_A, P_B) = \hat{e}(S_B, P_A).$$

Além disso, o protocolo é não-interativo, o que permite sensores acordar em chaves mesmo quando não estão *online* simultaneamente. Isso é especialmente útil em RSSFs, em que sensores podem conter padrões de dormência, serem dispostos em diferentes momentos e tornarem-se indisponíveis devido a obstáculos físicos ou falhas.

3.5. Segurança

Acerca da segurança do protocolo, note que A sabe que apenas B (e a ERB, uma entidade confiável) possui S_B e vice-versa; e por conseguinte o protocolo é autenticado. Além disso, formalmente, uma função de derivação de chaves deve ser primeiro aplicada à chave $k_{A,B}$ a fim de se gerar uma chave apropriada para criptossistemas. Esta chave pode então ser empregada como uma chave mestra para a derivação de chaves secretas (simétricas) para autenticação – ou seja, para a geração de Códigos de Autenticação de Mensagens ou *Message Authentication Codes* (MACs) – e sigilo – isto é, para cifração de mensagens.

No que tange à segurança da primitiva de emparelhamentos, em particular, esta e a maior parte das aplicações de PBC dependem da intratabilidade do seguinte problema (Sakai et al. 2000). Sejam $E/\mathbb{F}_q$ uma curva elíptica sobre o corpo finito $\mathbb{F}_q$ e $E(\mathbb{F}_q)$ um grupo de pontos desta curva. Dados P, Q, $[a]P$ e $[b]P$ em que P e Q são pontos de uma curva elíptica, a e b são escalares e $e(P, Q) \neq 1$, calcule $e([ab]P, Q)$. Este problema é conhecido como o *Problema Diffie-Hellman Bilinear*.

A intratabilidade deste problema, por sua vez, depende da intratabilidade do problema de Diffie-Hellman em $E(\mathbb{F}_q)$ e em $\mathbb{F}_{q^k}$. Portanto, os parâmetros q, ℓ e k (em que k é o menor inteiro tal que $\ell | q^k - 1$) devem satisfazer aos seguintes requisitos de segurança: (i) ℓ precisa ser grande o suficiente para que o Problema do Logaritmo Discreto em Curvas Elípticas (*Elliptic Curve Discrete Logarithm Problem* – ECDLP) em um sub-grupo de ordem ℓ de $E(\mathbb{F}_q)$ seja impraticável de ser resolvido usando o algoritmo rho de Pollard; (ii) k precisa ser grande o suficiente para que o problema do logaritmo discreto (*Discrete Logarithm Problem* – DLP) em $\mathbb{F}_{q^k}$ seja impraticável de ser resolvido usando o método de cálculo de índices.

Tabela 1. Custos de tempo para o cálculo do η_T no ATmega128L usando a TinyPBC.

Tempo	
Multiplicação	**Emparelhamento**
4,019.46μs	5.45s

Tabela 2. Custos de memória para o cálculo do η_T no ATmega128L usando a TinyPBC.

Memória (bytes)		
Pilha	**RAM**	**ROM**
2,867	368	47,948

3.6. Implementação

A despeito de todas as suas vantagens, PBC é um sistema assimétrico e, portanto, ordens de magnitude mais complexo computacionalmente que criptossistemas simétricos. Pior, sua operação mais custosa – o cálculo do emparelhamento – é cara mesmo para os padrões de PKC. Consequentemente, era necessário mostrar a viabilidade da solução, ou seja, provar que os sensores são capazes de realizar operações de PBC eficientemente.

Em nosso trabalho, então, apresentamos a TinyPBC – até onde sabemos a mais eficiente implementação de primitivas de PBC para um processador de 8 bits – e medidas de desempenho da mesma quando executada no microcontrolador ATmega128L/8-bit/7.3828-MHz/4KB-RAM/128-ROM (presente nos sensores MICA2 e MICAz). Para um nível de segurança de 80 bits (equivalente ao RSA-1024 bits), a TinyPBC é capaz de computar o emparelhamento η_T (Barreto et al. 2006) em menos de 5.5s (Tabela 1) consumindo apenas 2,867 bytes de RAM e 47,948 de ROM.

4. Conclusão

Em nossa tese, propusemos três soluções de distribuição de chaves (LHA-SP, SecLEACH e TinyPBC) compatíveis com os recursos dos sensores e, simultaneamente, adequadas para as particularidades das arquiteturas para as quais são propostas. Em resumo, as principais contribuições desta tese foram:

1. apresentar a primeira proposta de segurança para RSSFs Hierárquicas com número arbitrário de níveis (LHASP);
2. oferecer um conjunto de protocolos para proteger a configuração, operação e manutenção de RSSFs hierárquicas (LHASP);
3. apresentar a primeira solução de segurança para proteger RSSFs com formação dinâmica de agrupamentos e rotativa de CHs (SecLEACH);
4. mostrar como a pré-distribuição de chaves aleatórias pode ser empregada para proteger RSSFs com formação dinâmica de agrupamentos (SecLEACH);
5. identificar a sinergia existente entre RSSFs e IBC (TinyPBC);
6. demonstrar como sensores podem estabelecer chaves par-a-par de maneira eficiente, autenticada e não interativa (TinyPBC);
7. provar que o cálculo de emparelhamentos pode ser computado eficientemente mesmo em sensores com extrema escassez de recursos (TinyPBC).
8. principiar o estudo de PBC em RSSFs (TinyPBC);
9. no Brasil, ajudar a principiar o estudo de segurança em RSSFs (todas as soluções);

Neste documento em especial, descrevemos o TinyPBC, uma solução de distribuição de chaves utilizando IBC baseado em PBC. Primeiramente, defendemos a

idéia de que IBC e RSSFs são muito compatíveis e, em seguida, descrevemos como IBC pode ser usada para solucionar o problema da distribuição de chaves no contexto de RSSFs – ou seja, estabelecendo chaves par-a-par entre quaisquer pares de sensores de forma autenticada e não interativa. Ao final, apresentamos resultados do cálculo do emparelhamento η_T em sensores de recursos extremamente limitados. Resultados estes, até onde sabemos, os mais rápidos para uma arquitetura de 8 *bits*.

Foram publicados ao todo 24 trabalhos no decorrer desta tese e outros mais estão sob avaliação. É importante dizer, ainda, que este trabalho principiou-se pouco depois que a área de segurança em RSSFs começou de fato a ser estudada – foram anos de intensa pesquisa. Foram anos de intensa pesquisa em que os trabalhos evoluíram de propostas inovadoras, sim, mas as vezes ingênuas, para soluções robustas e mais apropriadas a essa tecnologia. Deste ponto de vista, quando ainda acreditava-se na inexequibilidade de PKC em RSSFs, contribuímos com criptossistemas simétricos. Mais adiante, contribuímos com soluções de PKC as quais permitiram troca de chaves de maneira não autenticada – ideais para RSSFs em que a largura de banda é baixa e o custo de comunicação alto.

Para se mensurar a contribuição deste trabalho é importante, primeiro, colocar os resultados aqui apresentados sob perspectiva. As soluções de pré-distribuição de chaves foram propostas quando não se havia, ainda, a alternativa do emprego de PKC em RSSFs. Mais que isso, quando principiamos este trabalho sequer existiam soluções de segurança na camada de enlace para RSSFs. Se soubéssemos que sensores viriam a computar primitivas de PKC, por exemplo, teríamos mais flexibilidade para arquitetarmos soluções.

Outro legado que o trabalho deixa é a aplicação de PBC em RSSFs. Após apontarmos a sinergia entre os sistemas e mostrarmos a viabilidade de serem empregados em conjunto, a comunidade de segurança em RSSFs também passou a focar o tema – em razão do espaço não citaremos trabalhos, mas o convidamos leitor a pesquisar na *web*.

Referências

[Barreto et al. 2006] Barreto, P. S. L. M., Galbraith, S., hEigeartaigh, C. O., and Scott, M. (2006). Efficient pairing computation on supersingular abelian varieties. In *Designs Codes And Cryptography*.

[Boneh and Franklin 2003] Boneh, D. and Franklin, M. (2003). Identity-based encryption from the weil pairing. *SIAM J. Comput.*, 32(3):586–615.

[Estrin et al. 1999] Estrin, D., Govindan, R., Heidemann, J. S., and Kumar, S. (1999). Next century challenges: Scalable coordination in sensor networks. In *MobiCom'99*, pages 263–270.

[Loureiro 2006] Loureiro, A. A. F. (2006). Grandes desafios da pesquisa em computação para o período 2006-2016.

[NSF 2003] NSF (2003). Report of the national science foundation workshop on fundamental research in networking.

[Perrig et al. 2002] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks*, 8(5):521–534.

[Sakai et al. 2000] Sakai, R., Ohgishi, K., and Kasahara, M. (2000). Cryptosystems based on pairing. In *SCIS'00*, pages 26–28.

[Shamir 1984] Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In *CRYPTO'84*, pages 47–53. Springer-Verlag.