O USO DA CRIPTOGRAFIA COM CURVAS ELÍPTICAS NA OTIMIZAÇÃO DA SEGURANÇA EM REDES DE SENSORES SEM FIO

Tiago SANTOS (1); Jeferson SILVA (2); Júlio VERAS (3); Rafael OLIVEIRA (4)
(1) CEFET-PB, Av. 1º de Maio, 720 Jaguaribe João Pessoa – PB, e-mail: tiagoferreira_22@yahoo.com.br
(2) CEFET-PB, e-mail: jefersondelasilva@hotmail.com
(3) CEFET-PB, e-mail: juliocveras@gmail.com
(4) CEFET-PB, e-mail: beljaburu@gmail.com

RESUMO

Na última década, houve um grande avanço tecnológico nas áreas de sensores, circuitos integrados e comunicação sem fio, o que levou a criação das Redes de Sensores Sem Fio (RSSF's). Tais redes podem ser utilizadas para diferentes aplicações, como detectar a presença de material perigoso, monitoramento de variáveis ambientais, identificação e cadastramento de pessoas em grandes ambientes como aeroportos, e têm um papel importante na computação ubíqua (onipresente). Um dos principais tópicos de discussão acerca das redes de sensores é a sua segurança, devido a vulnerabilidade que a própria infra-estrutura proporciona, o ambiente em que são executadas e de sua escassez de recursos. O baixo poder computacional dos sensores torna inviável a utilização de algoritmos de Criptografia de Chave Pública (PKC) convencionais, tais como o RSA/DAS. A segurança do sistema Criptográfico com Curvas Elípticas (ECC) baseia-se em um problema matemático de resolução complexa, que são os logaritmos discretos e que, aliado com o método das curvas elípticas torna-se ainda mais difícil de ser resolvido. Este trabalho tem como objetivo mostrar que a criptografia de curvas elípticas pode e deve ser considerada uma boa opção para uma maior segurança das redes de sensores sem fio, discutindo o uso de sistemas de ECC para estas redes.

Palavras-chave: sensores, segurança, criptografia, curvas elípticas

1. INTRODUÇÃO

O desenvolvimento e uso de sensores "inteligentes" em áreas ligadas a processos físicos, químicos biológicos, dentre outros é motivado pelo avanço que vem ocorrendo na área de comunicação sem fio, circuitos digitais, novos materiais de sensoriamento, micro-processadores, sistemas micro-eletromecânicos (MEMS – *Micro Electro-Mecanical Systems)*. Partindo desse ponto, alguns pesquisadores têm mostrado ser possível integrar sensores (acústicos, infravermelho, câmera, temperatura, calor, sísmico, etc), comunicação e fonte de alimentação em dispositivos miniaturizados usando apenas estas tecnologias, dando início a uma nova tecnologia na área de redes sem fio a*d hoc,* as Redes de Sensores Sem Fio, ou RSSF's, também conhecidos como sistemas *Smart Dust* (KAHN, 1999).

Porém, um dos principais tópicos a respeito das RSSF é quando trata acerca de sua segurança. Devido à sua escassez de recursos, como o baixo poder computacional e de energia, além da vulnerabilidade que o meio em que são executadas proporciona, estas redes necessitam de um método de segurança eficaz, que alie boa proteção ao tráfego de dados e economia de recursos para a rede. Nesse contexto, a criptografia baseada em curvas elípticas surge como a melhor opção dentre as existentes, pois sendo um sistema criptográfico de chave pública, provém a segurança requisitada pela rede e se encaixa dentro de seus padrões ideais de consumo de energia.

Ao longo deste trabalho, serão discutidos os motivos que fazem desse método criptográfico o ideal para o uso em RSSF's, analisando a criptografia baseada em curvas elípticas em si, bem como seu uso nestas redes.

2. CARACTERIZAÇÃO DAS RSSF'S

As RSSF's podem ser vistas como um tipo especial de rede móvel ad hoc, também conhecida como MANET's (*Móbile Ad hoc Network*). Numa rede tradicional, a comunicação entre os elementos computacionais é feita através de estações rádio-base, onde um Host Móvel (HM) está em contato direto com uma Estação de Suporte à Mobilidade (ESM), ou Ponto de Acesso (AP), que constituem uma infra-estrutura de comunicação, como ilustrado na figura 1a. Esse é o caso da Internet. Por outro lado, numa rede móvel ad hoc, também conhecida como MANET (*Mobile Ad hoc NETwork*), os dispositivos ou elementos computacionais são capazes de trocar informações diretamente entre si, como ilustrado na figura 1b.

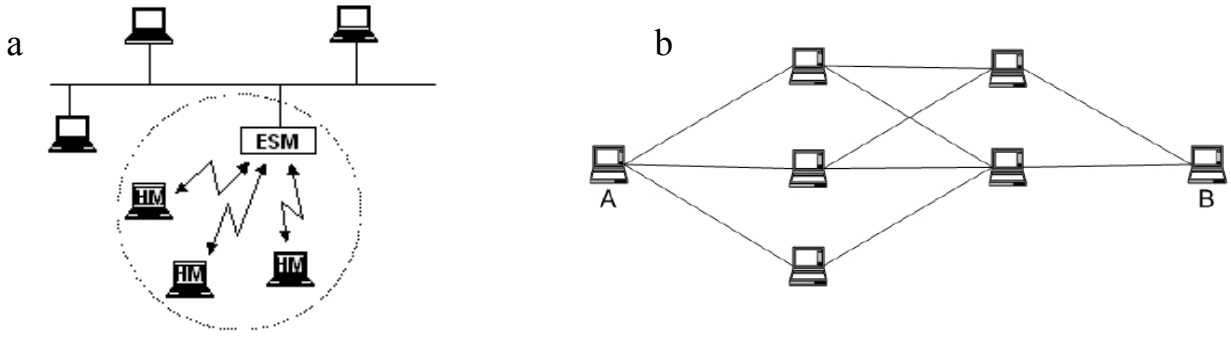

Figura 1 – Modelo de rede móvel infra-estruturada (a) e modelo de rede móvel ad-hoc (b)

As MANET's basicamente provêem suporte à comunicação entre esses elementos, que individualmente podem executar tarefas distintas. Já as RSSF's tendem a executar uma função colaborativa onde os elementos, nodos sensores, também chamados apenas de sensores, provêem dados que são processados (ou consumidos) por nodos especiais, em um ou mais pontos de concentração de informação e que possuem maior poder de processamento, chamados de sorvedouros (*sink nodes*), que podem comunicar-se com o mundo externo, para que seja possível o monitoramento remoto da rede por parte do usuário.

Analisando de maneira isolada, o trabalho de um nodo sensor é basicamente captar informações (através dos seus sensores), e transmitir tais informações logo após processá-las. Entretanto, devido suas limitações de hardware (processamento, memória e bateria), a realização das tarefas pelos nodos sensores é feita de forma colaborativa.

2.1. Características das RSSF's

Conforme as áreas em que são aplicadas, as RSSF's apresentam características particulares, fazendo com que questões específicas a tais características tenham que ser resolvidas. Algumas dessas características e questões são discutidas a seguir.

Homogeneidade ou heterogeneidade da rede. As RSSF's podem ser homogêneas ou heterogêneas em relação aos tipos, dimensões e funcionalidades dos nodos sensores. Um exemplo disso são as aplicações de monitoração de segurança, que podem utilizar sensores acústicos e de imagem embutidos no mesmo nodo sensor ou em nodos diferentes. Neste caso, os tipos de dados coletados pela rede de sensores são imagens, vídeos e sinais de áudio. Também existem aplicações em que todos os nodos são homogêneos em suas dimensões, possuindo as mesmas características físicas, como aplicações de monitoração de temperatura.

Endereçamento dos sensores ou nodos. Cada sensor pode ser endereçado unicamente ou não, o que depende da aplicação. Exemplificando: sensores embutidos em peças numa linha de montagem devem ser endereçados unicamente quando se deseja saber exatamente o local de onde o dado está sendo coletado. Por outro lado, sensores monitorando o ambiente em uma determinada região externa possivelmente não precisam ser individualmente identificados, já que o ponto importante é saber o valor de uma determinada variável nessa região.

Agregação dos dados. Indica a capacidade de uma RSSF de resumir ou agregar dados coletados pelos sensores. É possível reduzir o número de mensagens que devem ser transmitidas pela rede, caso ela tenha essa funcionalidade, conforme é ilustrado na figura 2. Os dados coletados são combinados e resumidos ainda na rede, antes de serem enviados à estação base.

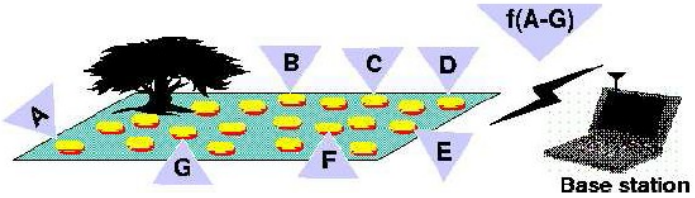

Figura 2: Agregação de dados coletados individualmente

Mobilidade dos sensores. Indica se os tem mobilidade ou não em relação ao sistema em que estão coletando dados. Por exemplo, sensores colocados na superfície de um oceano para medir o nível de poluição da água são móveis, enquanto sensores colocados numa floresta para coletar dados de umidade e temperatura são tipicamente estáticos.

Quantidade de sensores. Redes previstas para aplicações ambientais, como monitoramento de oceanos e florestas, contêm de 10 a 100 mil sensores. Portanto, a previsão da quantidade de sensores para determinadas aplicações é importante.

Limitação da energia disponível. Para diversas aplicações, os sensores são posicionados em áreas remotas, o que dificulta o acesso e, conseqüentemente, a manutenção desses elementos. Neste cenário, a quantidade de energia disponível determina o tempo de vida de um sensor. Aplicações, protocolos, e algoritmos para RSSF's devem ser escolhidos considerando a quantidade de energia consumida e não apenas sua "elegância" e capacidade de desempenho. Deve ser considerados o consumo, o modelo de energia e o mapa de energia da rede para quaisquer projetos desse tipo de rede e sua solução.

Auto-organização da rede. A deterioração física ou falta de energia são causas de perdas de sensores numa RSSF, que também podem ficar incomunicáveis por decisão de algum algoritmo de gerenciamento da rede ou devido a problemas no canal de comunicação sem fio. No caso de decisão do algoritmo, isso pode acontecer, por exemplo, para economizar energia ou por causa da presença de outro sensor que já coleta o dado desejado na mesma região que.

Porém, pode ocorrer justamente o oposto: sensores inativos se tornarem ativos ou novos sensores passarem a fazer parte da rede. Em qualquer um dos casos, é necessário que existam mecanismos de auto-organização para que a rede continue a executar a sua função.

Tarefas colaborativas. O objetivo principal de uma RSSF é executar alguma tarefa colaborativa onde é importante detectar e estimar eventos de interesse e não apenas prover mecanismos de comunicação. Devido às restrições das RSSF's, normalmente os dados são "fundidos" ou resumidos para aperfeiçoar o desempenho no processo de detecção de eventos.

Capacidade de responder a consultas. Uma consulta sobre uma informação coletada numa dada região pode ser colocada para um nodo individual ou um grupo de nodos. Dependendo do grau de sumarização executado, pode não ser viável transmitir os dados através da rede até o nodo sorvedouro. Assim, pode ser necessário definir vários nodos sorvedouros que irão coletar os dados de uma dada área e responderão consultas referentes aos nodos sob sua "jurisdição".

3. APLICAÇÕES PARA REDES DE SENSORES SEM FIO

Com o avanço no desenvolvimento de hardwares e softwares para RSSF's, existe a expectativa de que elas executem uma grande diversidade de tarefas nos mais variados lugares, além de atrair cada vez mais a atenção da comunidade acadêmica.

Graças ao seu potencial de controle e observação do mundo real, as RSSF's se apresentam como uma boa solução para uma diversidade de aplicações:

Controle. Para prover algum mecanismo de controle, seja em um ambiente industrial ou não. Por exemplo, sensores sem fio podem ser embutidos em "peças" numa linha de montagem para fazer testes no processo de manufatura.

Ambiente. Para monitorar variáveis ambientais em locais internos como prédios e residências, e locais externos como florestas, desertos, oceanos, vulcões, etc.

Tráfego. Para monitorar tráfego de veículos em rodovias, malhas viárias urbanas, etc.

Segurança. Para prover segurança em centros comerciais, estacionamentos, etc.

Medicina/Biologia. Para monitorar o funcionamento de órgãos como o coração, detectar a presença de substâncias que indicam a presença ou surgimento de um problema biológico, seja no corpo humano ou animal, como ilustrado na figura 3.

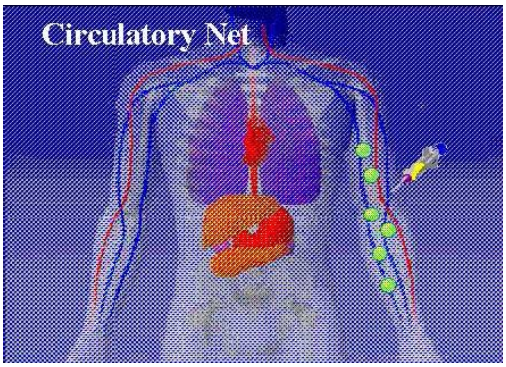

Figura 3: Sensores introduzidos no corpo humano para monitorar condições físicas

Militar. Para detectar movimentos inimigos, explosões, a presença de material perigoso como gás venenoso ou radiação, etc. Neste tipo de aplicação, os requisitos de segurança são fundamentais. O alcance das transmissões dos sensores é geralmente reduzido para evitar escutas clandestinas. Os dados são criptografados e submetidos a processos de assinatura digital. As dimensões são extremamente reduzidas e podem utilizar nodos sensores móveis como os transportados por robôs.

4. SEGURANÇA EM REDES DE SENSORES SEM FIO

Assim como em qualquer outra rede, as Redes de Sensores Sem Fio podem sofrer vários tipos de ataques. Além das RSSF's usarem comunicação sem fio, o que faz com que elas fiquem mais vulneráveis, algumas características dessas redes, como o baixo poder de processamento e a limitação de sua energia, fazem com

que não seja aconselhável a utilização de algoritmos criptográficos que precisem de alto poder de processamento.

Para que se possa prover segurança em uma Rede de Sensores, é necessário saber quais os requisitos e objetivos da aplicação que será utilizada. Alguns dos requisitos de segurança em RSSF's são apresentados abaixo:

- **Confidencialidade** – garante que o inimigo não obtenha informações.
- **Autenticidade** – garante a origem das informações.
- **Integridade** – garante que a mensagem recebida não foi modificada durante o trajeto.
- **Disponibilidade** – garante que os sensores conseguirão usar os recursos da rede.

A maioria dos requisitos de segurança podem ser alcançados através do uso da criptografia. Porém, não basta apenas utilizar um algoritmo criptográfico qualquer, é preciso escolher um algoritmo que, ao mesmo tempo, atenda as necessidades de segurança da aplicação e que utilize o mínimo de recursos de processamento possível.

4.1. Tipos de Ataques em RSSF

A literatura apresenta vários tipos de ataques contra RSSF's, que estão descritos em Karlof et al. (2003):

Denial of Service (DoS) - Este é um tipo de ataque que busca obstruir ou limitar o acesso a um certo recurso, que pode ser um componente ou um nó específico, um serviço ou toda a rede, exaurindo os recursos dela e sobrecarregando-a. A rede deve estar sempre disponível apenas para usuários autorizados, para estar livre deste tipo de ataque.

Spoofing – Alteração ou repetição de informações de roteamento. Nesse tipo de ataque, um nodo malicioso tenta alterar as informações de roteamento que são trocadas entre os nodos sensores. Essa alteração pode fazer, por exemplo, com que o roteamento de informações entre em loop, ou seja, a informação nunca vai chegar ao destino, passando sempre pelos mesmos nodos, que gastarão muita energia para enviar e recebê-la. A figura 4 mostra um tipo de ataque de spoofing onde o nodo malicioso se passa por um nodo sorvedouro, fazendo com que todas as informações da rede sejam destinadas a ele.

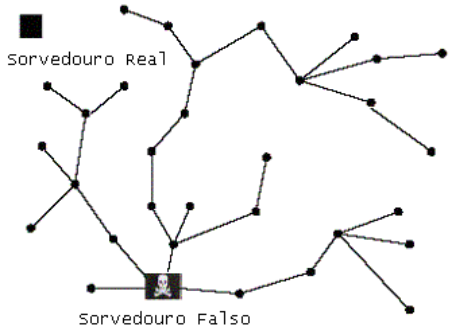

Figura 4 - Ataque de Spoofing

Encaminhamento seletivo - Nesse tipo de ataque, o nodo malicioso, que está na rota que a informação deve seguir, pode se recusar a enviar a mesma. Uma forma simples desse ataque é quando um nodo funciona como um buraco negro, se recusando a enviar todas as informações que chegam a ele.

Um ataque de encaminhamento seletivo é mais eficaz quando o nodo que faz esse ataque está na rota principal da Rede de Sensores, pois mais informações irão passar por esse nodo. A figura 5 mostra um tipo de ataque de encaminhamento seletivo.

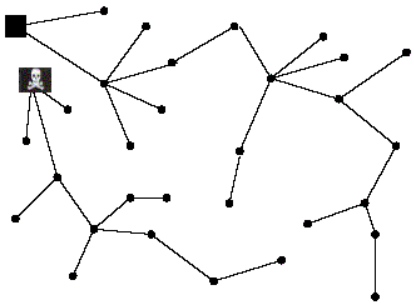

Figura 5 – Ataque de encaminhamento seletivo

Ataque de inundação de HELLO - Muitos protocolos de roteamento necessitam que os nodos sensores enviem pacotes de HELLO para que seus vizinhos saibam que eles existem. Porém, um nodo malicioso de maior porte pode enviar esse tipo de pacote para a quantidade máxima de nodos sensores que ele consiga, para que estes aceitem suas mensagens como sendo autênticas. Então os nodos sensores mudarão suas rotas e tentarão enviar mensagens para os nodos maliciosos, mas não irão conseguir, pois são de menor porte. A figura 6 mostra um exemplo de um ataque de inundação de HELLO.

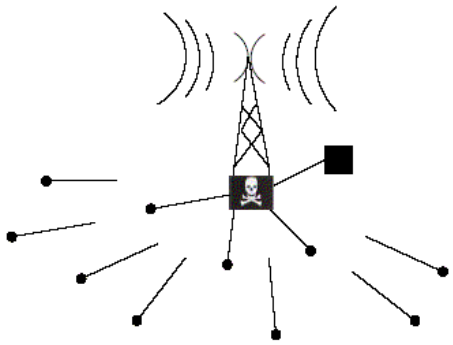

Figura 6 - Ataque de inundação de HELLO

Ataque Sybil - A figura 7 mostra um exemplo do tipo de ataque Sybil. Um nodo malicioso ‘A’ apresenta várias identidades que não existem (‘A1’, ‘A2’ e ‘A3’), e faz com que o nodo ‘B’ pense que o próximo nodo do roteamento é o nodo ‘A1’, logo o nodo ‘B’ nunca vai conseguir enviar uma mensagem para ‘A1’, pois ele não existe, conseqüentemente não vai enviar mensagens para o nodo real ‘C’.

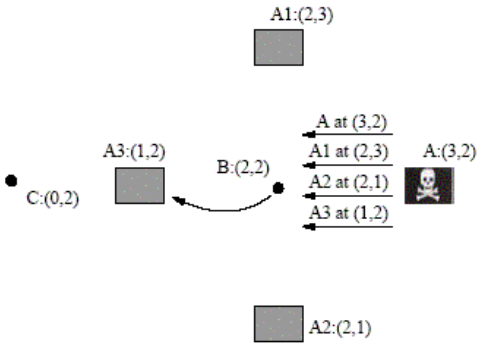

Figura 7 - Ataque Sybil

4.2. Sistemas de criptografia com Chave Pública

Dentro do contexto de criptografia, os sistemas existentes apoiam-se no fato de existirem problemas matemáticos que, dado o elevado nível de trabalho envolvido na sua resolução, tornam-se de difícil solução. Conseqüentemente, busca-se proteção no fato de que o "adversário" não conseguirá, mesmo contando com as mais modernas ferramentas computacionais, reverter a função de criptografia (na qual o sistema se baseia) e acessar os parâmetros e entradas do sistema em um tempo aceitável.

Em termos de criptografia computacional, um problema matemático é dito "de difícil solução" quando, mesmo aplicando-se o algoritmo mais eficiente para resolvê-lo, esse leva um longo período para que sua execução se conclua. Esse tempo de execução possui uma relação direta com o tamanho dos dados de entrada do algoritmo utilizado. Cientistas da área defendem o fato de que, em geral, um problema de fácil solução tem o tempo de execução polinomial, enquanto que problemas de difícil solução têm esse tempo em formato exponencial. Conseqüentemente, existe o interesse em saber o quanto um problema se torna difícil (tempo de execução) com o aumento do tamanho de sua entrada e, adicionalmente, em selecionar problemas que maximizem esse tempo, sempre que se desejar obter um sistema de criptografia mais seguro.

Os sistemas de criptografia com chave pública foram inicialmente propostos por Whitfield Diffie e Martin Hellman (DIFFIE e HELLMAN, 1976). Esses sistemas trabalham com duas chaves, independentes e não facilmente deriváveis: a chave pública, utilizada para criptografar mensagem e a chave privada, utilizada para descriptografar.

Tem se observado que, ao se projetar sistemas criptográficos de chave pública, é necessário também haver um compromisso entre o nível de segurança e o tempo de resposta que se deseja obter. Nesse aspecto, quanto mais desenvolvidos forem as ferramentas e algoritmos utilizados para violação dos sistemas de criptografia existentes, maiores têm que ser os parâmetros (chaves) e, conseqüentemente, maior o esforço no trabalho de codificação e decodificação dos textos cifrados.

Nesse ponto, os métodos mais usados na criptografia de chave pública, como o RSA, não atendem aos requisitos de consumo de energia das RSSF's, pois consomem uma quantidade de recursos muito acima da desejada.

A criptografia com o uso de curvas elípticas foi inicialmente proposta por Victor Miller e Neal Koblitz (KOBLITZ e MILLER, 1985). Este sistema está baseado no *Elliptic Curve Discrete Logarithm System* – ECDLS. A definição matemática deste problema é a seguinte:

"Dada uma curva elíptica E (Fq), definida sobre um conjunto finito de valores inteiros, denominado **campo finito: Fq** (sendo **q** o número de elementos do conjunto) e os pontos P, Q Є E (Fq) (BOTES, 2003). Com essas precisas tenta-se determinar um inteiro M (0 < M < q-1) tal que se cumpra a relação Q = M * P."

Considera-se matematicamente simples definir o ponto Q = M * P, sendo mais difícil determinar o inteiro M, dados Q, P Є E (Fq). Até então não existe um algoritmo sub-exponencial no tempo que resolva o problema do logaritmo discreto em curvas elípticas – ECDLP.

A seguir, é feita uma comparação entre alguns sistemas de criptografia, incluindo a criptografia com curvas elípticas, relação à eficiência de processamento e exigência de espaço para a sua execução.

4.3. Comparação de Sistemas de Criptografia

4.3.1. Eficiência

A discussão acerca da eficiência de cada um dos sistemas de criptografia descritos aqui, leva em consideração os seguintes fatores: carga computacional, tamanho de chave e tamanho de banda. Para uma comparação mais justa, os dados apresentados levam em consideração o mesmo nível de segurança para todas as propostas (ECC, RSA ou DSA).

- **Carga Computacional**: Mede a eficiência com que os algoritmos podem implementar as transformações com as chaves públicas e privadas (sistema em operação). As melhores implementações de cada um dos sistemas ("state-of-the-art implementations") indicam que o ECC executa numa ordem de 10 vezes mais rápido que o RSA ou DSA.
- **Tamanho de Chave**: Conforme citado anteriormente, o ECC também apresenta grande vantagem nesse aspecto. Enquanto RSA e DSA apresentam pares de chave (pública, privada) com tamanhos, em

bits, RSA (1088, 2048) e DSA (1026, 160), temos, no caso da implementação de curvas elípticas o par ECC (161, 160).

- **Tamanho de Banda**: Corresponde a quantos bits (a mais) temos que transmitir após criptografar ou assinar uma mensagem, em relação a mensagem original. Todas as três opções apresentam valores parecidos nesse quesito, com o ECC se destacando exclusivamente nos casos em que queremos processar mensagens pequenas. Se visualizarmos os sistemas de criptografia com chave pública como eficiente ferramenta de troca de chave de seção (usa transformação de mensagens pequenas), essa vantagem do ECC torna-se ainda mais significativa.

Na tabela 1 são mostrados os testes realizados pela Certicom Corp., que comparou os tempos requeridos para operações de 163 bits no ECC e 1024 bits no RSA (CERTICOM, 1998). A Elliptic Curve Nyberg-Rueppel Algorithm – ECNRA é uma curva elíptica que utiliza o algoritmo Nyberg-Rueppel, e Elliptic Curve Digital Signature Algorithm – ECDSA é uma versão de uma Curva Elíptica baseada em Algoritmos de Assinatura Digital – DAS. A Certicom Corp., realizou os testes utilizando 67 Mhz UltraSparc sobre o sistema operacional SOLARIS.

Tabela 1. *Benchmarks* sobre o sistema operacional SOLARIS [Certicom 1998].

Função	Security Builder 1.2 163-bit ECC (em *ms*)	BSAFE 3.0 1024-bit RSA (em *ms*)
Geração de pares de chaves	3.8	4708.3
Assinatura	2.1 (ECNRA) 3.0 (ECDSA)	228.4
Verificação	9.9 (ECNRA) 10.7 (ECDSA)	12.7
Troca de chaves Diffie-Hellman	7.3	1654.0

4.3.2. Exigências de Espaço

A tabela 2 compara o tamanho dos parâmetros do sistema e a seleção do par de chaves dos dois sistemas, e demonstra-se que os pares de chaves são mais curtas no ECC de 160-bits que no RSA de 1024-bits.

Tabela 2. Requerimentos de espaço.

	Parâmetros do sistema (em bits)	Chave Pública (em bits)	Chave Privada (em bits)
1024-bit	n/a	1088	2048
160-bit	481	161	160

A Certicom Corp. mostra que ambos sistemas têm exigências similares de largura de banda quando são usados para cifrar ou assinar mensagens cumpridas, mas existem certas mudanças desta situação para os casos onde as mensagens de menor tamanho estão sendo criptografadas.

Em síntese, o ECC pode permitir maior eficiência que qualquer outro sistema que utiliza a fatoração de números inteiros em términos de o*verhead* computacional, tamanho de chave e largura de banda. Na pratica, as implementações significam execuções mais rápidas, aproximadamente 10 vezes em relação ao RSA, com consumo de energia mais baixo e redução no tamanho do código (CERTICOM, 1997).

Também são comparados os tempos de quebra para o ECC e o RSA utilizando tamanhos variados de módulos do melhor algoritmo conhecido. Os valores foram computados em MIPS (milhão de instruções por segundo). É geralmente aceito 10^{12} MIPS anos que representam uma segurança razoável. Um outro detalhe é que para o melhoramento do nível de segurança, é necessário um aumento mais significativo do tamanho das chaves do RSA, em comparação ao ECC. Os resultados são listados na tabela 3.

Tabela 3. Tamanho de chave [Randall 1999]

Tempo para quebra (em Anos MIPS)	Tamanho da chave RSA (em bits)	Tamanho da chave ECC (em bits)	Razão do tamanho da chave RSA/ECC
10^4	512	106	5 : 1
10^8	768	132	6 : 1

10^{11}	1024	160	7 : 1
10^{20}	2048	210	10 : 1
10^{78}	21000	600	35 : 1

4.4. Distribuição de Chaves com Curvas Elípticas

As Curvas Elípticas oferecem uma segurança computacional equivalente à apresentada com o Algoritmo Diffie-Hellman baseada no DLP, que utiliza chaves pequenas comparando-o com os algoritmos exponenciais existentes do DLP.

A implementação do algoritmo Diffie-Hellman sobre curvas elípticas oferece uma alternativa para a troca de "segredos compartilhados" com perfeita segurança no envio destes. Esse segredo é difícil de calcular por uma terceira pessoa, pois o nó receptor não consegue obter informação atualizada da chave privada do nó emissor durante a transmissão, de tal forma que, a chave do emissor continua sendo privada. A utilidade do segredo compartilhado é que pode ser utilizado como chave para outra sessão de criptografia.

As principais tarefas da distribuição de chaves é a gestão e o gerenciamento de chaves, que deve controlar o acesso, o tempo de validade de cada chave, e a forma de envio destas. A base para a distribuição de chaves públicas pode incluir a presença de autoridades certificadoras que fazem parte de uma infraestrutura de chave pública ou *Public Key Infraestructure* – PKI.

4.5. Criptografia de Curvas Elípticas em Redes de Sensores

A Criptografia de Curvas Elípticas é uma alternativa viável e eficiente que vai de encontro a uma crença que perdurou por muito tempo nessa área: a impossibilidade de usar criptografia de chave pública em redes de sensores, uma vez que seu custo computacional seria excessivamente alto para os poucos recursos dos dispositivos usados nessas redes.

Devido à dificuldade relativa em resolver os problemas de fatoração ou de logaritmos discretos e de logaritmos discretos em curvas elípticas, as chaves usadas em algoritmos baseados em curvas elípticas são bem menores que as dos outros algoritmos, o que gera um custo computacional menor para a rede. Em concordância com os dados apresentados até aqui, isto corrobora com a tese da viabilidade de aplicação da Criptografia de Curvas Elípticas as RSSF's, por sua adaptabilidade as características intrínsecas dessas redes. Conforme a necessidade de segurança vai aumentando, sua eficiência se torna ainda mais significativa.

5. CONSIDERAÇÕES FINAIS

Os sistemas criptográficos de chave pública são mais eficientes no provimento de segurança de redes. Entretanto, estes demandam um alto custo computacional para a execução de suas tarefas e nem todas as redes possuem uma alta capacidade de recursos para que os tais sistemas criptográficos sejam executados com toda sua eficiência. Este é o caso das Redes de Sensores Sem Fio, que além de possuírem uma gama menor de recursos, são executadas em ambientes que proporcionam uma maior vulnerabilidade a seu tráfego de informações.

A criptografia de chave pública baseada em curvas elípticas é um método recente, em relação aos demais de chave pública, porém não menos eficiente e com um diferencial que a torna uma excelente opção para as RSSF's, senão a mais indicada, não somente em termos de nível de segurança como também em todos os principais pontos relativos à eficiência de operação: a economia de recursos que proporciona, quando comparada com métodos mais tradicionais e tão eficientes quanto ela, como o RSA.

Dadas suas características, essa técnica pode ser utilizada, principalmente, em sistemas "embutidos" ou sistemas com restrições físicas de espaço e/ou capacidade de processamento. Porém, não deve demorar muito o surgimento de sensores mais rápidos e com mais memória, que permitam a utilização de qualquer protocolo ou algoritmo de redes tradicionais.

REFERÊNCIAS

BOTES, J.J.; PENZHORN, W.T. **Public-Key Cryptosystems Based on Elliptic Curves**. Communications and Signal Processing, 1993. *In*: IEEE SOUTH AFRICAN SYMPOSIUM ON, 6 August 1993.

CERTICOM CORP. **Current Public-Key Cryptographic Systems**. 1997. http://www.certicom.com/research/wecc2.html.

CERTICOM CORP. **The Elliptic Curve Cryptosystems for Smart Cards**. 1998. http://www.certicom.com/research/wecc4.html.

CHAN, H.; PERRIG, A. **Security and Privacy in Sensor Networks**. IEEE computer, October 2003.

DIFFIE, W.; HELMANN, M. **New Directions on Cryptography**. IEEE Transactions on Information Theory, 1976.

GANESAN, P.; VENUGOPALAN, R.; PEDDABACHAGARI, P.; DEAN, A.; MUELLER, F.; SICHITIU, M. **Analyzing and Modelling Encryption Overhead for sensor Network Nodes**. *In*: ACM INTERNATIONAL CONFERENCE ON WIRELESS SENSOR NETWORKS AND APPLICATIONS, 2., September, 2003.

GURA, N.; PATEL, A.; WANDER, A.; EBERLE, H.; SHANTZ, S. C. **Comparing elliptic curve cryptography and rsa on 8-bit cpus**. *In*: INTERNATIONAL WORKSHOP ON CRYPTOGRAPHY HARDWARE AND EMBEDDED SYSTEMS, 6., (CHES'04), Cambridge, Boston, USA, 2004.

KAHN, J. M.; KATZ, R. H.; PISTER K. S.; EECS, U. C. **Emerging Challenges Mobile Networking for "Smart Dust"**. Berkeley, http://www.eecs.berkeley.edu/~jmk/,1999.

KARLOF, C.; WAGNER, D. **Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures**, 2003.

KOBLITZ, N.; MENEZES, A.; VANSTONE, S. **The State of Elliptic Curve Cryptography**. http:://modular.fas.harvard.edu/ - 2000.

LAW, Y. W.; DOUMEN, J.; HARTEL, P. **Survey and Benchmark of Block Ciphers for Wireless Sensor Networks**. *In:* PROC. 1st IEEE MASS, Oct 2004.

LINDSEY, S.; RAGHAVENDRA, C.; SIVALINGAM, K. M. **Data gathering algorithms in sensor networks using energy metrics**. IEEE Transactions on Parallel and Distributed Systems, 2002. 13 (9): 924-935 p.

LOUREIRO, A. A. F; NOGUEIRA, J. M. S.; RUIZ, L. B.; DE FREITAS MINI, R. A.; NAKAMURA, E. F.; FIGUEIREDO, C. M. S. **Redes de sensores sem fio**. *In:* SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 2003. 179, 226 p.

MILLER, V. **Uses of Elliptic Curves in Cryptography**. Advances in Cryptography, Crypto 85, Springs Verlag LNCS, 1986. 218, 417-426 p.

NEWSOME, J.; SHI, E.; SONG, D. PERRIG, A. **The Sybil Attack in Sensor Networks: Analysis & Defenses.** *In:* IPSN, 2004.

RANDALL, K. **ICSA Guide to Cryptography**. Computing McGraw-Hill, First Edition, 1999.