**REVISTA CIENTÍFICA ELETRÔNICA DE SISTEMAS DE INFORMAÇÃO** - ISSN 1807-1872
PUBLICAÇÃO CIENTÍFICA DA FACULDADE DE CIÊNCIAS JURÍDICAS E GERENCIAIS DE GARÇA/FAEG
ANO II, NÚMERO, 04, FEVEREIRO DE 2006. PERIODICIDADE: SEMESTRAL

# ESTRATÉGIAS DE SEGURANÇA EM HARDWARE PARA REDES DE SENSORES

**MUZZI, Fernando Augusto Garcia**
**TAMAE, Rodrigo Yoshio**
**ROSA; Adriano Justino**
Docentes da Faculdade de Ciências Gerenciais e Jurídicas de Garça – FAEG/Garça
fagmuzzi@yahoo.com.br ; rytamae@yahoo.com.br; adriano@faef.br

## RESUMO

Na ultima década, houve um grande avanço tecnológico nas áreas de sensores, circuitos integrados e comunicação sem fio, que levou à criação de redes de sensores sem fio (RSSF) que podem ser utilizados para monitoramento, rastreamento, coordenação e processamento em diferentes contextos. No entanto, é necessário que tais sensores tenham sido implementados com rotinas de segurança no envio de pacotes com módulos criptográficos em hardware. Este trabalho consiste em uma apresentação inicial destes dispositivos.
**Palavras-chave**: Rede de sensores sem fio, Segurança e FPGA.

## ABSTRACT

In the last decade, had a great technological advance in the areas of sensors, integrated circuits and wireless communication, that led to the creation of wireless networks (RSSF) that they can be used for watching, tracking, coordination and processing in different contexts. However, it is necessary that such sensors have been implemented with routines of security in the sending of packages with criptography modules build in hardware. This work consists of an initial presentation of these devices.
Keywords: Wireless Network Sensor, Security, FPGA

## 1. INTRODUÇÃO

As redes móveis sem fio estão sendo utilizadas nas mais diferentes áreas como a militar, turismo, educação, controle de estoque, descoberta de desastres ecológicos, emergência médica entre outras. Na computação móvel sem fio o usuário tem acesso contínuo às informações através de uma rede de

comunicação sem fio. Este tipo de rede é apropriada para situações onde não se pode ter uma instalação com fios e que requer acesso imediato à informação. As aplicações de sistemas celulares permitem conectar um computador portátil via uma rede sem fio a uma *LAN* (*Local Area Network*) para carregar dados atuais de um determinado documento ou de um banco de dados. As aplicações baseadas em *WLAN* (*Wireless LAN*) são sistemas de comunicação de dados flexíveis implementados como uma extensão de uma *LAN* com fio. As ondas eletromagnéticas transmitem e recebem dados pelo ar, minimizando a necessidade de conexões com fio. O uso de redes sem fio tem aumentado de forma significativa, e a rede de sensores sem fio funciona com sensores trocando informações entre sí, dessa forma é necessário mecanismos de segurança que possam garantir a confiabilidade da informação coletada a partir de sensores. Uma forma de prover segurança é a implementação de criptografia para a troca de informações entre sensores, dessa forma se um dado for capturado não poderá ser lido, somente o nó que tiver a chave poderá decifrar e ler o dado. Uma das maneiras de realizar a prototipação e abstrair o funcionamento de uma rede de sensores é realizar a implementação de um algoritmo de criptografia utilizando FPGAs, a fim de avaliar resultados e verificar a viabilidade da realização de criptografia em redes de sensores.

## 2. CARACTERÍSTICAS DAS REDES DE SENSORES

Nesta seção são apresentadas as principais características de redes de sensores. As redes de sensores possuem como características principais: o sensor, o observador e o fenômeno. O **sensor** é o dispositivo que implementa a monitoração física de um fenômeno ambiental e gera relatórios de medidas (através de comunicação sem fio). Um sensor produz uma resposta mensurável a mudanças em condições físicas, tais como temperatura, campo magnético e luz. Os dispositivos de detecção, geralmente, têm características físicas e teóricas diferentes. Muitos modelos de complexidade variada podem ser construídos baseados na necessidade da aplicação e características dos dispositivos. Na maioria dos modelos de dispositivos sensores a habilidade de detecção diminui com o aumento da distância do sensor ao fenômeno e com o aumento do tempo que o sensor fica exposto para coletar informações. Um sensor, tipicamente,

consiste de cinco componentes: detector de hardware, memória, bateria, processador embutido e transmissor/receptor.

As principais métricas para avaliar protocolos de redes de sensores são: eficiência de uso da energia, vida útil do sistema, latência, precisão, tolerância a falhas, escalabilidade e exposição dos sensores.

## 3. ARQUITETURA

Uma rede de sensores é uma ferramenta para medir e passar informação sobre um determinado fenômeno para o observador dentro do limite de desempenho desejado e com melhor custo/benefício possível. Para tal, a rede deve ser organizada da seguinte forma: infra-estrutura, protocolo de rede e de aplicação/observador.

A **infra-estrutura** consiste de sensores e da forma como utilizá-los. Mais especificamente, a infraestrutura é influenciada pelo número de sensores, pelas características deles (precisão de detecção, tamanho de memória, vida útil da bateria, extensão da transmissão) e estratégia de utilização (quantidade, localização e mobilidade do sensor).

O **protocolo de rede** é responsável por criar caminhos e realizar comunicação entre os sensores e o(s) observador(es).

Na **aplicação/observador** o interesse de um observador no fenômeno é expresso através de consultas realizadas a respeito do fenômeno. Para responder às consultas, os dados distribuídos que os sensores são capazes de monitorar são aproximados. Estas consultas podem ser estáticas (os sensores são programados para reportar dados de acordo com um padrão específico) ou dinâmicas. A rede pode participar na sintetização da consulta. Por exemplo, filtrando alguns dados dos sensores ou fundindo diversas medidas num único valor. As otimizações nestes três níveis são possíveis para melhorar o desempenho da rede RSSF.

O protocolo numa rede de sensores é responsável por dar suporte a toda comunicação, entre os próprios nós sensores e entre os nós sensores e os observadores. O desempenho do protocolo pode ser altamente influenciado pelo dinamismo das redes, assim como pelo modelo construído de envio de dados específicos. Para determinar como o protocolo de rede comporta-se para diferentes cenários é importante classificar estas características. Intuitivamente,

para um dado tipo de sensor, aumentar o número de sensores no campo deveria resultar num melhor desempenho na rede, considerando que: (i) a precisão da monitoração deveria aumentar, já que há mais sensores numa posição para relatar sobre o fenômeno; (ii) a disponibilidade de energia dentro da rede aumentaria e (iii) a densidade do sensor adicional ofereceria o potencial para uma rede melhor conectada com caminhos mais eficientes entre os sensores e os observadores. Entretanto, aumentar o número de sensores resulta num número maior de sensores reportando seus resultados na unidade de tempo. Se o aumento de carga excede a capacidade da rede em termos de acesso ao meio sem fio compartilhado, pode-se gerar congestionamento nos nós intermediários, assim um aumento do número de nós ativos pode afetar o desempenho da rede. Com relação à capacidade, o problema pode ser visto em termos de colisão e congestionamento. Para evitar colisões, deve-se evitar a transmissão simultânea entre sensores que estiverem na extensão de transmissão de outros sensores.

Nem todos os sensores são iguais em termos de precisão uma vez que dependendo da localização, um sensor específico pode ter uma melhor qualidade de dados ou uma combinação de sensores pode prover uma precisão maior do que outra.

Da perspectiva da rede a precisão depende de fatores como localizações geográficas dos sensores que geram relatórios, tamanho do *buffer* e tempo de processamento de pacotes. Em relação à perspectiva da aplicação o valor da informação monitorada pelo sensor precisa, também, ser considerada. Se um sensor está fornecendo alguma informação única sobre alguma característica do fenômeno, então a aplicação deve requerer que o sensor reporte-a independentemente da sua localização. Em redes de sensores, a infra-estrutura em termos de capacidade de detecção do sensor, número de sensores e estratégia de uso eficiente mostram uma significante influência na determinação do desempenho da rede. Em redes de sensores são estudados os efeitos de infraestrutura de dois tipos de modelos de envio da rede (fenômeno contínuo e controlado) e diferentes protocolos de rede (*DSR – Dynamic Source Routing*, *DSDV – Destination Sequenced Distance Vector* e *AODV – Ad Hoc On Demand Distance Vector*). É comum mostrar o desempenho em termos da eficiência da rede, precisão da aplicação e demandas de latência.

## 4. IMPORTÂNCIA DA REDE DE SENSORES SEM FIO

As redes de sensores formam um campo que está sendo muito pesquisado atualmente. Utilizando redes de sensores é possível monitorar ambientes de difícil acesso tais como campos de batalha, regiões do oceano, florestas. Além disso, podem ser utilizados na área biomédica, na monitoração de tráfego, enfim, pode ser utilizada nos mais diversos campos de atividades.

## 5. CONCLUSÕES

As redes de sensores formam um campo que está sendo muito pesquisado atualmente. Utilizando redes de sensores é possível monitorar ambientes de difícil acesso, como campos de batalha, regiões do oceano, florestas. Além disso, podem ser utilizados na área biomédica, na monitoração de tráfego, enfim, pode ser utilizada pelos mais diversos campos de atividades. Os sensores podem ser móveis ou imóveis, sendo que no segundo caso as redes apresentam características de redes móveis *ad hoc*. Portanto, em redes de sensores, problemas como segurança e tolerância a falhas devem ser observados. Para resolver, ou pelo menos amenizar estes problemas, uma fonte de pesquisa são os protocolos de comunicação que prevêem falhas e tentam evitá-las. Além disso, existem protocolos que tentam evitar que inimigos coloquem informações incorretas na rede de sensores. Uma rede de sensores pode ser vista como um caso especial de redes móveis, onde os nós têm baixa capacidade de energia e disponibilidade de memória. Porém, os protocolos de roteamento utilizados para redes *ad hoc* não são apropriados para redes de sensores, porque podem gerar tabelas de roteamento muito grandes. Elas exigem uma capacidade de memória que não existe em um sensor, não suportam agregação ou fusão de dados, nem a criação e manutenção de rotas. Os protocolos precisam ser adaptados. As redes de sensores auto-organizáveis propõem uma outra forma de funcionamento de uma rede composta de sensores, pois os sensores por si próprios formam a rede. Este tipo de rede deve ser capaz de se adaptar para problemas como falhas de dispositivos. Além disso, devem gerenciar os movimentos dos nós sensores e atender a consultas na rede. O desafio físico encontra-se em se ter um sensor com capacidade de

armazenamento de tamanho razoável e que a rede funcione sem falhas, fornecendo informações atuais e corretas do fenômeno observado. Desta forma, podemos dizer que as redes de sensores possuem características próprias relevantes que devem ser cuidadosamente observadas. Isto para que sejam propostos novos protocolos de comunicação, de gerenciamento de tolerância a falhas, entre outros pontos, para tornar mais concreto e viável a utilização destas redes. É importante a segurança em rede de sensores utilizando criptografia já que a rede de sensores estão se tornando comuns, é necessário segurança para evitar que um nó intruso de sensor possa entrar na rede de sensores e prejudicar a rede, o uso de criptografia deve se levar em conta o tempo de vida do sensor e a limitação para processar algoritmos criptográficos grandes, para os uso em sensores deve ser um algoritmo pequeno e seguro para evitar gargalo e consumo alto de bateria.

## 6. REFERÊNCIAS BIBLIOGRÁFICAS


BLUETOOTH, special interest group, disponível em (2003) http://www.bluetooth.com.

BROADWELL, P., Polastre, J., and Rubin, R. Geomote: Geographic multicast for networked sensors. Disponível em: http://www.cs.berkeley.edu/~pbwell/, 2001 (acessado em 28 de setembro de 2005).

CULLER, D, J. Hill, N. Lee, P. Levis, S. Madden, J.Polastre, R. Szewczyk, K. Whitehouse e A. Woo, “TinyOS Project”, University Berkeley, disponível em (2003) http://webs.cs.berkeley.edu/tos.

DEMERS, A., J. Gehrke, J. Shanmungasundaram, M.Calimlim, M. Riedewald e N. Trigoni, Cournel Database Group, disponível em (2003) http://www.cs.cornell.edu/database/cougar/index.htm.

ELSON, J. e D. Estrin, “Time Synchronization for Wireless Sensor Networks”, University of California, Los Angeles; and USC/Information Sciences Institute, disponível em (2003) http://www.circlemud.org/~Ejelson/writings/timesync.

EVANS, D., “Programming the Swarm”, Department of Computer Science, University of Virginia, disponível em (2003) http://swarm.cs.virginia.edu.

ESTRIN, D., R. Govindan, J. Heidemann e S. Kumar, “Next century challenges: scalable coordination in sensor networks”, In Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Seattle, Washington, USA, ACM Press, ISBN 1-58113-142-9, 1999, pp 263-270, disponível em (2003) http://doi.acm.org/10.1145/313451.313556.

GANESAN, D., R. Govindan, S. Shenker e D. Estrin, “High-resilient, energy-efficient multipath routing in wireless

HEINZELMAN, W. R., Chandrakasan, A., and Balakrishnan, H. *Energy-efficient communication protocol for wireless microsensor networks.* In Proceedings of the Hawaii International Conference on System Sciences, Maui, Hawaii, USA, 2000.

KARLOF, Chris and WAGNER, David – Secure Routing in Wireless Sensor Networks: Attacks and *Countermeasures* – University of California at Berkeley – IEEE, 2003. LEACH code for NS2 http://www-mtl. mit.edu/researchgroups/icsystems/cad/ (acessado em 28 de setembro de 2005).

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

MANJESHWAR, A. and AGRAWAL, D. *Teen: A routing protocol for enhanced effeciency in wireless sensor networks.* In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, 2001.

MIT - Massachussets Institute of Technology - http://web.mit.edu/ (acessado em 28 de setembro de 2005).

NEWSOME, James et al. – *The Sybil Attack in Sensor Networks: Analysis & Defenses* – IPSN´04, Berkeley California – USA, 2004. NS-2, The network Simulator ns-2. http://www.isi.edu/nsnam/ns/

SANCAK, Serdan et al. – *Sensor Wars: Detecting and Defending Against Spam Attacks in WSNs* – IEEE Communication Society, 2004.

WOOD, Antony D. and STANKOVIC, John A. – *Denial of Service in Sensor Networks* – University of Virginia, IEEE, 2002.