

SISMA - SISTEMA DE MONITORAMENTO E AUDITORIA HOSPITALAR UTILIZANDO CRIPTOGRAFIA NEURAL

Macêdo Firmino*, Gláucio B. Brandão*, Ana Maria G. Guerreiro*

*Departamento de Engenharia de Computação e Automação
Universidade Federal do Rio Grande do Norte
Natal - RN, Brasil

Emails: macedofirmino@dca.ufrn.br, glaucio@dca.ufrn.br, anamaria@dca.ufrn.br

Abstract— Medical errors may result in loss of life and increase the costs of the healthcare system. Researchers has shown great potential of RFID (Radio Frequency Identification) technology in healthcare to prevent medical errors. However, existing international RFID standards do not include security specifications, which resulted in appearance of security threats. Actually, privacy issues are major obstacle to use this technology in hospital environments. This paper presents a novel approach of security for RFID systems based on a neural network, called tree parity machine. Moreover, we proposed a monitoring and audit system in the healthcare. This system is responsible for real-time patients monitoring and provide an audit in case of medical errors.

Keywords— Monitoring and Audit System in the Healthcare, RFID Security and Privacy.

Resumo— Organizações e universidades vêm pesquisado medidas para combater erros médicos e melhorar a qualidade na prestação dos serviços. Uma das tecnologias que vem se destacando é a RFID (*Radio Frequency Identification*). Porém, os padrões internacionais relacionados com esta tecnologia não abrangem especificações de segurança, o que acarretou no surgimento de vulnerabilidades de segurança. Estas vulnerabilidades se tornaram um obstáculo para a utilização desta tecnologia em ambientes hospitalares. Neste artigo, é proposta uma solução para a segurança em sistemas RFID, baseada na geração de chaves criptográficas através de uma rede neural artificial chamada *tree parity machine*. Além disso, é apresentado um sistema, chamado SISMA (Sistema de Monitoramento e Auditoria Hospitalar), que é responsável pelo monitoramento em tempo real dos pacientes e por prover suporte a auditoria em caso de denúncia de erros médicos.

Palavras-chave— Monitoramento e Auditoria Hospitalar, Segurança em sistemas RFID.

1 Introdução

Hospitais necessitam de uma boa infra-estrutura de comunicação e armazenamento de dados para prover suporte às tomadas de decisões. A complexidade dos hospitais revela-se nas: funções e serviços diversificados, na escassez de seus recursos e na urgência das ações. O gerenciamento dos dados em ambientes hospitalares é um processo difícil devido ao grande volume de informações geradas. Além disso, hospitais ainda continuam a armazenar a informações em papeis e processá-las manualmente, apesar de décadas de experiência na aplicação bem sucedida da tecnologia da informação em outros setores da indústria e prestadoras de serviços.

Um relatório do *Institute of Medicine* (*To Err Is Human: Building a Safer Health System*, 1999) relatou que morrem de 44.000 a 98.000 pessoas anualmente em hospitais americanos devido a erros médicos. Além do risco de vida dos pacientes, os erros médicos apresentam um elevado custo financeiro aos hospitais. O relatório (*To Err Is Human: Building a Safer Health System*, 1999) estima que os custos diretos provocado por erros médicos, que podem ser evitados, nos Estados Unidos são de aproximadamente $17 bilhões por ano.

Pesquisas (Florentino et al., 2008) (Wang et al., 2006) vêm demonstrando o potencial da utilização da tecnologia RFID em ambientes hospitalares, principalmente em prontos socorros, maternidades e centros cirúrgicos onde há uma grande quantidade de pacientes e, conseqüentemente, maiores riscos de erros médicos. A tecnologia RFID pode auxiliar na gestão hospitalar de várias maneiras, por exemplo: na identificação de recém nascidos, identificação e localização de pacientes e membros da equipe hospitalar, armazenamento de prontuários médicos, localização de equipamentos médicos e identificação de remédios.

RFID representa uma tecnologia de identificação sem fio que pode ser incorporado a produtos, animais ou pessoas. A utilização desta tecnologia tem a finalidade de permitir a identificação automática. Os sistemas RFID são compostos por dispositivos eletrônicos chamados de *tag* e leitor. A *tag* é o componente responsável pelo armazenamento dos dados de identificação. O leitor tem a finalidade de obter os dados das *tags* e disponibilizá-los em uma interface gráfica ou sistemas de processamento de dados.

Um obstáculo para a adoção desta tecnologia em ambientes hospitalares é a questão da privacidade das informações dos pacientes. As instituições internacionais ISO (*International Organization for Standardization*) e EPCGlobal vêm desenvolvendo padrões, porém estes padrões não abrangem especificações de segurança. Este fato acarretou no surgimento de falhas de segurança (Juels, 2006).

Para a criação de um sistema RFID seguro se faz necessário a utilização de: algoritmos criptográficos, protocolo de autenticação e protocolo de gerenciamento de chaves. Pesquisas (Juels, 2005) (Feldhofer et al., 2004) apresentaram algoritmos criptográficos para sistemas RFID. Estes algoritmos ainda não apresentaram nenhuma vulnerabilidade de segurança. Conseqüentimente, o desafio de segurança em sistemas RFID atualmente se encontra em protocolo de autenticação e protocolo de gerenciamento de chaves.

Com relação ao gerenciamento de chaves, Kinzel e Kanter (Kinzel and Kanter, 2002) definiram uma rede neural (chamada de *tree parity machine*) e seu respectivo algoritmo de aprendizado. Duas *tree parity machines* após o período de treinamento alcançam a sincronização dos seus pesos. A sincronização por aprendizado mútuo desta estrutura neural pode ser aplicada no gerenciamento de chaves secretas sobre um canal público.

Existem trabalhos que visam prover tecnologias para dar suporte à infra-estrutura de hospitais. Murakami et al. (Murakami et al., 2006) desenvolveu um sistema de monitoramento contínuo de glicose em pacientes críticos em UTIs (Unidades de Terapia Intensiva) e Varady et al (Várady et al., 2002) desenvolveram um sistema de monitoramento de pacientes com redes *Profibus*. Porém, ambos os trabalhos não abordaram a questão da segurança da informação, redes sem fio e um sistema de auditoria.

Florentino et al. (Florentino et al., 2008) apresentou um sistema de informação, baseado na tecnologia RFID, com o objetivo de aperfeiçoar o funcionamento de um laboratório de análises clínicas. O sistema não apresentou requisitos de segurança da informação e nem abordou sistema de auditoria.

O presente trabalho descreve como redes neurais artificiais podem ser utilizadas em protocolos de segurança para sistemas RFID. Outra contribuição é a proposta de um sistema de monitoramento e auditoria hospitalar. Na seqüência, apresentaremos como a *tree parity machine* pode produzir chaves secretas, apenas trocando alguns *bits* sobre um canal público, e propor um sistema de monitoramento e auditoria hospitalar que faz uso desta rede neural para a geração de chaves secretas em algoritmos de criptografia simétrica.

2 *Tree Parity Machine*

A *tree parity machine* corresponde a uma arquitetura em duas camadas, conforme mostrada na Figura 1. A camada escondida é formada por k neurônios e a camada de saída por apenas um neurônio. Cada neurônio da camada escondida possui n valores de entrada, sendo cada entrada associada a um peso.

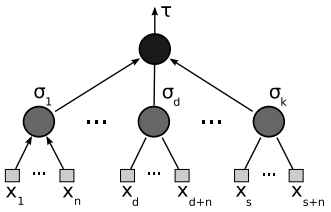

Figura 1: A arquitetura *tree parity machine*.

Os possíveis valores da entrada da rede são: $x_i \in \{-1, 1\}$. Os pesos deverão apresentar valores discretos entre o intervalo de $-l$ a l, ou seja, $w_{i,j} \in \{-l, -l+1, ..., l\}$ onde o índice $i = 1, ..., k$ representa o neurônio da camada escondida e o $j = 1, ..., n$ indica o elemento do vetor de entrada.

A saída do neurônio da camada escondida é dada pela equação:

$$\sigma_i = sgn\left(\sum_{j=1}^{n} w_{i,j} x_j\right) \tag{1}$$

A saída da rede neural é obtida pela multiplicação das saídas dos neurônios da camada escondida:

$$\tau = \prod_{i=1}^{k} \sigma_i. \tag{2}$$

Considere dois dispositivos A e B que desejam se comunicar. Cada dispositivo deverá possuir uma *tree parity machine*, com a mesma arquitetura. As duas redes iniciam o processo de sincronização escolhendo aleatoriamente os seus pesos. A utilização de valores discretos para os pesos e as entradas levará a sincronização das duas redes neurais, ou seja, os pesos das duas redes serão iguais após um número finito de passos (Kinzel and Kanter, 2002).

Uma vez iniciado com valores aleatórios para os seus pesos, a cada instante de tempo, um vetor de entrada X é criado aleatoriamente e apresentado as redes, para obtermos suas respectivas saídas τ_A e τ_B. Se as saídas forem diferentes ($\tau_A \neq \tau_B$) os pesos não deverão ser ajustados. Caso contrário deverá ser utilizada à regra de aprendizado: somente os pesos do neurônio da camada escondida que possui a sua saída (σ_i) igual à saída da rede (τ) serão ajustados. A equação de atualização dos pesos é:

$$w_{i,j} = g(w_{i,j} + x_j), \tag{3}$$

onde:

$$g(\zeta) = \begin{cases} sgn(\zeta)l & \text{se } |\zeta| > l \\ \zeta & \text{caso contrário.} \end{cases} \quad (4)$$

A função $g(\zeta)$ possui o objetivo de garantir que os valores dos pesos se mantenham na faixa $[-l, l]$, ou seja, se o valor de um determinado peso em módulo for maior que o módulo de l, deverá ser atribuído ao mesmo o valor limite $(\pm l)$.

A arquitetura *tree parity machine* apresenta algumas peculiaridades, por exemplo, para $k \leq 3$, o tempo de sincronização é diretamente proporcional a l^2, enquanto que o tempo de sincronização de um atacante é proporcional a e^l, o que não ocorre para $k > 3$ (Ruttor, 2007). Outra característica é que para $k \leq 2$ o sistema é vulnerável a um ataque chamado de *geometric attack* (Ruttor, 2007). Conseqüentemente pode-se atribuir o nível de segurança desejável através da escolha do parâmetro l, com $k = 3$. O sistema é seguro se $l \to \infty$. Na prática é atribuído um valor suficientemente grande para garantir o nível de segurança desejado.

O processo de sincronização das redes neurais pode ser utilizado em algoritmos criptográficos em protocolos de autenticação e na geração de chaves em protocolos de gerenciamento de chaves.

Comparado com os algoritmos baseados em teoria dos números, as redes neurais apresentam algumas vantagens: o algoritmo é de baixa complexidade e proporciona a criação de novas chaves para cada bloco de mensagem (Kinzel and Kanter, 2002).

3 SISMA - Sistema de Monitoramento e Auditoria Hospitalar

Nos hospitais é comum o uso de prontuários médicos manuscritos em papel. O prontuário médico é o conjunto de documentos (tais como, ficha clínica, exames complementares, prescrição médica e folha de evolução clínica), onde devem ser registrados todos os cuidados profissionais prestados aos pacientes (*Manual de Orientação ética e Disciplinar*, 2000). O preenchimento do prontuário médico é obrigação e responsabilidade do médico. O que acarreta no gasto de uma grande quantidade de tempo na interpretação e atualização da documentação manuscrita. Porém, não existe nenhum obstáculo para a utilização da informática na elaboração de prontuários médicos, desde que seja garantido o respeito ao sigilo profissional (*Manual de Orientação ética e Disciplinar*, 2000). Estes fatos motivaram a avaliação do potencial da tecnologia RFID em hospitais.

Recentemente, foram encontradas várias vulnerabilidades de segurança presentes na tecnologia RFID (Juels, 2006). Resultando na falta de privacidade nas informações dos pacientes quando utilizado em ambientes hospitalares. Porém, redes neurais artificiais podem ser utilizadas na geração de chaves criptográficas em sistemas RFID. Portanto, se utilizarmos redes neurais, algoritmos criptográficos simétricos e um protocolo de autenticação é possível propiciar requisitos de segurança da informação em ambientes hospitalares. Baseado nestes mecanismos é proposto um sistema chamado SISMA (Sistema de Monitoramento e Auditoria Hospitalar). Este sistema é composto por cinco unidades: UIMP (Unidade de Identificação e Monitoramento do Paciente), UIM (Unidade de Identificação dos Medicamentos), UIEH (Unidade de Identificação da Equipe Hospitalar), URM (Unidade Remota de Monitoramento) e a UCP (Unidade Central de Processamento). O sistema é mostrado na Figura 2.

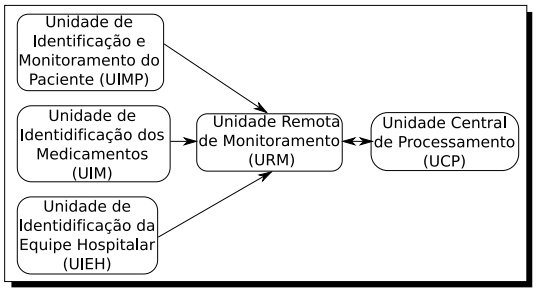

Figura 2: Componentes do SISMA.

O SISMA tem a finalidade de monitorar algumas variáveis fisiológicas dos pacientes. O sistema corresponde ainda a uma ferramenta de auditoria na defesa dos médicos nos casos de denúncias por mau atendimento com indícios de imperícia, imprudência ou negligência, ou seja, na presunção da existência de erro médico. Os auditores obterão informações sobre que medicamento foi ministrado a um determinado paciente, que estava sobre um determinado quadro clínico, por um determinado membro da equipe médica em uma data e horário discriminado.

O SISMA faz uso de pulseiras RFID para os pacientes. As pulseiras contêm o que chamamos de UIMP (Unidade de Identificação e Monitoramento dos Pacientes). Esta pulseira é colocada em cada paciente na chegada do mesmo e removida na sua saída. Os identificadores utilizados pelo SISMA são usados como índices em um banco de dados na Unidade Central de Processamento. As pulseiras são usadas para identificar o paciente durante todo o período de internação, sendo utilizadas ainda para armazenar alguns dados importantes do paciente (tais como: sintomas, alergias e grupo sangüíneo). As UIMP podem ser lidas por leitores RFID mesmo quando os pacientes estão desacordados, evitando acordá-los para obter as informações ou erros de

comunicação entre funcionários da equipe hospitalar.

A UIMP é responsável pelo monitoramento de algumas variáveis fisiológicas e identificação dos pacientes. O monitoramento realizado pela UIMP é opcional e sua utilização deverá ser avaliada para cada paciente. A UIMP é composta por um microprocessador, um módulo de criptografia neural, uma *tag* RFID, uma unidade de memória e opcionalmente sensores fisiológicos (mostrada na Figura 3). O microprocessador é responsável por: obtér os dados dos sensores, extrair a chave de criptografia do módulo de criptografia neural, obtér o identificador do paciente armazenado na unidade de memória, realizar a criptografia dos dados (variáveis monitoradas e identificador do paciente) e inserir estes dados na *tag* RFID.

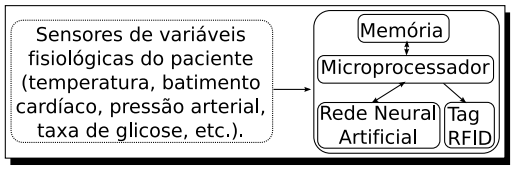

Figura 3: UIMP - Unidade de Identificação e Monitoramento do Paciente.

O módulo de criptografia neural é formado por uma rede neural artificial e tem a finalidade de gerar as chaves de criptografia necessárias para comunicação segura entre a UIMP e URM. A unidade de memória contém o identificador único do paciente. A memória não deverá conter informações confidenciais do paciente, como nome e endereço. Isso se faz necessário para diminuir os danos causados em uma possível quebra de privacidade do sistema.

Médicos, enfermeiros e demais profissionais da equipe hospitalar deverão utilizar crachás RFID. Estes crachás contêm a UIEH (Unidade de Identificação da Equipe Hospitalar). Este componente contém um identificador único do funcionário da equipe hospitalar. O UIEH é utilizado para a identificação do funcionário do hospital no sistema de auditoria médica, podendo ainda ser utilizado para obter acesso a ambientes restritos. A UIEH não deverá conter informações confidenciais do funcionário.

Medicamentos também deverão apresentar *tags* RFID únicas. Estas *tags* contém a UIM (Unidade de Identificação de Medicamentos). As UIMs serão utilizadas no sistema de auditoria hospitalar, podendo ainda serem utilizadas em sistemas de gestão de medicamentos. Um sistema de gestão de medicamentos se faz necessário para impedir o furto. A UIM pode opcionalmente conter outros dados pertinentes, por exemplo, validade do medicamento e local de armazenamento.

O SISMA define ainda dois *hardwares*, são eles: URM (Unidade de Remota de Monitoramento) e UCP (Unidade Central de Processamento). A URM é responsável por realizar a leitura das *tags* da UIMP, UIM e UIEH e disponibilizar estes dados a UCP. A URM tem acesso à base de dados da UCP para obter prontuário dos pacientes, permitindo que os pacientes tenham acesso as suas informações clínicas através de uma interface gráfica. A URM tem ainda a função de gerar avisos de alertas, por exemplo, quando estiver sendo ministrado um medicamento que não está na prescrição médica ou quando alguma variável fisiológica do paciente se encontra em um estado crítico.

A URM é formada por um leitor RFID, microprocessador, um módulo de criptografia neural, interface de rede, interface gráfica e opcionalmente um módulo de proteção contra interferências (observe a Figura 4). O leitor é responsável por realizar a leitura das UIMP, UIM e UIEH. O microprocessador tem a função de obter os dados do leitor e a chave de criptografia do módulo de criptografia neural para realizar a decriptação e obter as informações. Uma vez obtida às informações, a URM irá enviar estas informações a UCP através da interface de rede. A interface gráfica é utilizada na comunicação do sistema com o paciente e funcionários da equipe hospitalar. A comunicação entre a URM e a UCP poderá utilizar o protocolo PM-AH (de M. Valentim et al., 2008), *Profibus* (Várady et al., 2002) ou outros protocolos de tempo real que possam ser utilizados em ambientes hospitalares. O módulo de proteção contra interferência poderá fazer uso de filtros dinâmicos ou de técnicas como FHSS *(Frequency Hopping Spread Spectrum)*.

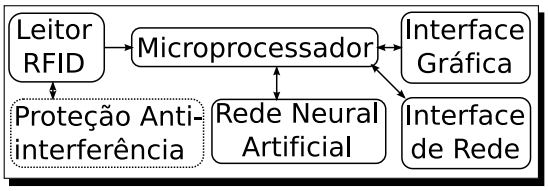

Figura 4: URM - Unidade Remote de Monitoramento.

A UCP é responsável pelo armazenamento dos dados e a geração de relatórios de auditoria. A UCP é formado por uma interface de rede, processador, gerenciador de banco de dados e um servidor *web* (conforme mostrada na Figura 5). A interface de rede se faz necessário para realizar a comunicação entre UCP e as URMs. O banco de dados tem a finalidade de armazenar os dados dos pacientes, medicamentos e funcionários da equipe hospitalar. Os relatórios de auditoria e demais dados serão disponíveis ao usuário do sistema através do servidor *web* e um programa aplicativo.

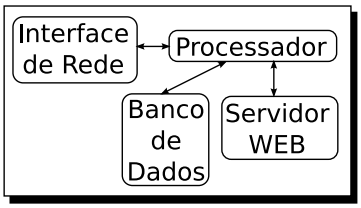

Figura 5: UCP - Unidade Central de Processamento.

4 Conclusões e Trabalhos Futuros

Este artigo mostra como redes neurais artificiais podem ser utilizadas em protocolos de segurança para sistemas RFID. Outra contribuição é a proposta de um sistema de monitoramento e auditoria hospitalar baseado na tecnologia RFID. O sistema denominado SISMA (Sistema de Monitoramento e Auditoria Hospitalar) trata do monitoramento em tempo real dos pacientes e do suporte aos médicos nos casos de denúncias de erros, através de relatórios de auditoria. O sistema proporciona a identificação rápida e precisa dos pacientes, medicamentos e membros da equipe hospitalar. Além de informar alguns sintomas clínicos que os pacientes apresentam. A identificação automática irá evitar ou reduzir erros médicos, aumentar a eficiência e produtividade. Os hospitais que implantarem o SISMA apresentarão uma melhor troca de informações entre os diversos setores do hospital, tais como as enfermarias, almoxarifado, laboratorial e financeiro.

Têm-se como trabalhos futuros: construir uma prova de conceito utilizando FPGA (*Field Programmable Gate Array*) para verificar a viabilidade técnica da utilização do sistema em *tags* RFID comerciais, realização de um estudo de caso em hospitais, implementação do módulo de anti-interferência e expansão do sistema da identificação para equipamentos hospitalares, criando assim um sistema de inventário de equipamentos.

Referências

de M. Valentim, R. A., Morais, A. H. F., Guerreiro, A. M. G., Brandão, G. B. and de Araújo, C. A. P. (2008). MP-HA: Multicycles Protocol for Hospital Automation over multicast with IEEE 802.3, *Industrial Informatics* pp. 979–984.

Feldhofer, M., Dominikus, S. and Wolkerstorfer, J. (2004). Strong Authentication for RFID Systems Using the AES Algorithm, pp. 357–370.

Florentino, G. H. P., Bezerra, H. U., de A. Júnior, H. B., Araújo, M. X., de M. Valentim, R. A., Morais, A. H. F., Jesus, T. O., Guerreiro, A. M. G., Brandão, G. B. and de Araújo, C. A. P. (2008). Hospital automation RFID-based, *Industrial Informatics* pp. 1534–1538.

Juels, A. (2005). Minimalist Cryptography for Low-Cost RFID Tags, pp. 149–164.

Juels, A. (2006). Rfid security and privacy: a research survey, *Selected Areas in Communications, IEEE Journal on* **24**(2): 381–394.

Kinzel, W. and Kanter, I. (2002). Neural cryptography, *in Proc. of the 9th International Conference on Neural Information Processing*, pp. 18–22.

Manual de Orientação ética e Disciplinar (2000). CRM - Conselho Regional de Medicina do Estado de Santa Catarina, Volume 1 - 2. Comissão de Divulgação de Assuntos Médicos.

Murakami, A., Gutierrez, M., Lage, S., Rebelo, M., Guiraldelli, R. and Ramires, J. (2006). A Continuous glucose monitoring system in critical cardiac patients in the Intensive Care Unit, *Computers in Cardiology* pp. 233–236.

Ruttor, A. (2007). Neural Synchronization and Cryptography.

To Err Is Human: Building a Safer Health System (1999). Institute of Medicine.

Várady, P., Benyó, Z. and Benyó, B. (2002). An open architecture patient monitoring system using standard technologies, *Information Technology in Biomedicine* pp. 95–98.

Wang, S.-W., Chen, W.-H., Ong, C.-S., Liu, L. and Chuang, Y.-W. (2006). RFID Application in Hospitals: A Case Study on a Demonstration RFID Project in a Taiwan Hospital, *Hawaii International Conference on System Sciences* **8**: 184a.