Sistema de Detecção de Intrusão Imuno-inspirado customizado para Redes de Sensores Sem Fio*

Helio M. Salmon[1], Claudio M. de Farias[1], Luci Pirmez[1], Silvana Rossetto[1], Paulo H. de A. Rodrigues[1], Rodrigo Pirmez[2], Flávia C. Delicato[4], Luiz F. R. da C. Carmo[3]

[1]Programa de Pós-Graduação em Informática - Universidade Federal do Rio de Janeiro
[2]Faculdade de Medicina - Universidade Federal do Rio de Janeiro
Cidade Universitária – 21.941-901 – Rio de Janeiro – RJ – Brasil

[3]Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - Av. N. S. das Graças, 50 – 25.250-020 - Xerém - Duque de Caxias – Rio de Janeiro

[4]Departamento de Informática e Matemática Aplicada – Universidade Federal do Rio Grande do Norte - Campus Universitário Lagoa Nova – 59.078-970 - Natal - RN

{helio.salmon, luci.pirmez, cmicelifarias, Silvana.rosseto, rodrigopirmez, pauloaguiar.ufrj, fdelicato, lfrust}@gmail.com

Abstract*. In this work we propose an IDS framework inspired in the Human Immune System and a decentralized and customized version of the dendritic cell algorithm to be applied in the wireless sensor network context. Its basic feature is the nodes neighborhood monitoring and collaboration to identify an intruder. The work was experimentally evaluated in order to demonstrate its efficiency in detecting a denial-of-sleep attack.*

Resumo*. Neste artigo são propostas uma arquitetura de Sistema de Detecção de Intrusão inspirado no Sistema Imunológico Humano e uma versão descentralizada e customizada do algoritmo das células dendríticas para o contexto das redes de sensores sem fio. Sua característica básica é que os nós monitoram sua vizinhança e colaboram entre si para a identificação de um intruso. A proposta foi avaliada experimentalmente para demonstrar sua eficiência na detecção de um ataque do tipo denial-of-sleep.*

1. Introdução

Os recentes avanços nas tecnologias de sistemas micro-eletromecânicos e nas comunicações sem fio possibilitaram a construção de sensores dotados de capacidade de processamento e comunicação, com baixo custo e tamanho reduzido. Redes de Sensores Sem Fio (RSSFs) são constituídas por dezenas, centenas ou milhares destes equipamentos e utilizadas para monitorar variáveis físicas e ambientais como temperatura, umidade, níveis de ruído e movimento de objetos. As RSSFs são usadas por diversas aplicações, como: monitoramento de estruturas, rastreamento e monitoramento de alvos militares [Yick *et al.* 2008].

Se por um lado RSSFs trazem novas e amplas perspectivas para várias aplicações, por outro trazem uma série de desafios, relacionados à limitação de recursos e às vulnerabilidades associadas à comunicação sem fio e à organização *ad-hoc*, características inerentes dessas redes. Aliado a isso, os sensores podem ser depositados em áreas abertas, desprotegidas e às vezes hostis, tornando as RSSFs alvo de ataques, os

*Artigo financiado com recursos da FINEP (01.10.0064.00), CNPq (309270/2009-0, 481638/2007-5, 477226/2007-8, 477229/2009-3, 306938/2008-1 e 481638/2007-5) e FAPERJ (E-26/101.360/2010).

quais podem comprometer a confiabilidade, integridade e disponibilidade dos dados trafegados nestas redes e a vida útil dos sensores [Yick *et al.* 2008].

Uma das formas de lidar com as vulnerabilidades associadas às RSSFs é adotando um Sistema de Detecção de Intrusão (SDI). SDIs em geral possuem algumas limitações como, por exemplo, as falhas na detecção e os alarmes falsos que podem ocorrer com certa frequência, comprometendo o seu uso com sucesso [García-Teodoro *et al.* 2008]. Uma forma de contornar tais limitações é empregando métodos de Inteligência Computacional (IC) de forma a tornar o SDI mais eficaz [Silva 2009]. As técnicas de IC adicionam características de aprendizado, evolução e adaptação que possibilitam a construção de SDIs mais eficazes, robustos e capazes de tratar ataques desconhecidos, adaptando-se mais facilmente a diferentes cenários de aplicação. Neste trabalho, adotamos um Sistema Imunológico Artificial (SIA), aplicando os conceitos do Sistema Imunológico Humano (SIH) na construção de um SDI para RSSFs [Greensmith 2007].

Os SIAs estão sendo vistos como abordagens promissoras para a implementação de SDIs, pois os problemas encontrados nas áreas de segurança de redes, incluindo-se as RSSFs, possuem grandes semelhanças com os SIAs no que se refere à manutenção da estabilidade do sistema em um meio em constante mudança [Silva 2009]. Algumas das características principais do SIH, tais como a auto-organização, adaptação, robustez e tolerância a falhas, são análogas as das RSSFs. Estas redes devem ser capazes de se adaptar a mudanças contínuas do meio ambiente e dos requisitos da própria aplicação, e ser tolerantes a falhas, uma vez que os nós sensores utilizam um meio de comunicação não confiável e instável. Além disso, mecanismos e/ou algoritmos para RSSFs devem ser distribuídos e auto-organizáveis, uma vez que a existência de mecanismos centralizados não é adequada para essas redes, dados os seus recursos limitados.

Este trabalho apresenta uma proposta de arquitetura de um SDI para RSSF que utiliza técnicas imuno-inspiradas baseadas na Teoria do Perigo (TP). A TP utiliza um sinal de perigo para considerar como anômalo um antígeno (invasor) que esteja causando danos ao organismo, não levando em conta se o mesmo pertence (próprio) ou não (não-próprio) ao referido organismo. As células conhecidas como células dendríticas (CDs) detectam e processam diferentes sinais, incluindo o sinal de perigo, para classificar os antígenos coletados por elas mesmas como normais ou anômalos. Estas células podem ser vistas como sendo o mecanismo de controle do SIA, capaz de determinar se a RSSF está sofrendo um ataque. O SDI proposto foi concebido de forma a ser ativado ou desativado de acordo com os requisitos de segurança das aplicações sendo executadas na RSSF, atendendo as limitações de recursos das RSSFs. Neste trabalho foi proposta também uma versão descentralizada e customizada do algoritmo original de CDs para o contexto de RSSF, onde os procedimentos relacionados ao algoritmo original foram adaptados de forma a melhor explorar a característica de densidade dessas redes e reduzir o processamento e as estruturas de dados existentes em cada nó sensor. O algoritmo proposto foi concebido de forma a: (i) ser genérico no sentido de ser independente do tipo de ataque; (ii) permitir a reutilização dos seus componentes em várias aplicações de RSSF; e (iii) tornar seu código independente do código das aplicações e protocolos de RSSF.

Como estudo de caso, nesse trabalho considera-se uma aplicação onde os sensores capturam e enviam seus dados para um nó ligado a um computador (estação base - EB) em intervalos de tempo regulares. Em cada um desses nós é instalado um SDI

programado para detectar ataques do tipo *denial-of-sleep* e acionar contramedidas adequadas. Esse tipo de ataque visa acelerar o esgotamento das fontes de energia de um ou mais sensores e, por fim, inutilizá-los. O ataque ocupa o meio e aumenta a possibilidade de colisões de pacotes dentro da área de alcance do sinal de interferência. Esse ataque pode exigir que o nó afetado permaneça por um tempo maior acordado tentando transmitir (o meio está ocupado pelo nó atacante) ou retransmitir um pacote (a aplicação solicita a retransmissão de pacotes não recebidos), causando em ambos os casos um gasto adicional de energia do nó sensor.

Este artigo está organizado em seis seções. A Seção 2 apresenta os conceitos básicos do trabalho e a Seção 3 os trabalhos relacionados. Na Seção 4 é descrito o SDI proposto e na Seção 5 os experimentos realizados e a análise de seus resultados. Por fim, a Seção 6 contém as conclusões deste trabalho.

2. Conceitos Básicos

Greensmith *et al.* (2005) introduziram o algoritmo das células dendríticas (ACD), o qual é dividido em três fases: inicialização, atualização e agregação. Na fase de inicialização, os parâmetros do algoritmo são configurados e inicializados e o estado imaturo é atribuído às CDs. Na fase de atualização, um processo contínuo de atualização das estruturas de dados a partir dos sinais de entrada e dos antígenos é realizado. Ao final desta fase, os sinais de saída são gerados, alterando o estado das CDs para semi-madura (normal) ou madura (anômala). A fase de agregação ocorre no linfonodo, que é um gânglio encontrado por toda a extensão do sistema linfático e tem a função de receber as CDs. Nesta fase os antígenos apresentados pelas CDs maduras ou semi-maduras são analisados e o índice de anomalia dos antígenos, conhecido pela sigla MCAV (*Mature Context Antigen Value*), é calculado. O MCAV varia entre zero e um e representa o quão anômalo é um antígeno, sendo calculado pela fórmula: MCAV = (M)/(SM+M). Onde “M” representa a quantidade de um determinado antígeno em células maduras e “SM” a quantidade do mesmo antígeno em células semi-maduras. Caso o índice esteja acima de um valor pré-determinado (limiar de anomalia), os anticorpos são acionados, iniciando o combate aos invasores. O processo de avaliação de antígenos é repetido um determinado número de ciclos (eventos) ou até que todos os antígenos tenham sido avaliados [Silva 2009].

No ACD, os sinais de entrada são classificados como: (i) sinais de perigo, quando as células sofrem necrose (morte celular não programada); (ii) sinais seguros, quando as células sofrem apoptose (morte celular programada); (iii) sinais de PAMP, substâncias que indicam a presença de entidade extra-organismo; e (iv) inflamação, que indica o aumento do fluxo de sangue e da temperatura em uma área afetada por uma invasão, cujo efeito amplifica os efeitos dos 3 sinais anteriores [Greensmith 2007]. As CDs processam os sinais de entrada de forma a gerar os sinais de saída de acordo com a Equação 1. A Equação é executada uma vez para cada um dos sinais de saída: (i) sinal de migração (*Costimulatory Molecules* - CSM); (ii) semi-maduro; e (iii) maduro. Cada CD permanece armazenando os sinais de saída enquanto o sinal de migração não atingir um limite pré-determinado (limiar de migração). Quando o sinal de migração atingir tal limite, a CD compara os valores armazenados para os sinais semi-maduro e maduro. O sinal de maior valor define o estado de maturação daquela CD. Em seguida, esta CD migra para o linfonodo. Na Equação 1, “P*i*” representa o sinal de PAMP, “D*i*” o sinal de

perigo, “S*i*” o sinal seguro e “IC” o sinal de inflamação. O somatório de cada um desses sinais é multiplicado pelos seus respectivos pesos “W*p*”, “W*d*” e “W*s*”.

$$Saída_{\left[\begin{array}{l} csm \\ semi-madura \\ madura \end{array}\right]} = \left(W_P \sum_{i=0}^{I} P_i + W_D \sum_{i=0}^{I} D_i + W_S \sum_{i=0}^{I} S_i \right) * (1 + IC) \qquad \text{Equação 1}$$

No SIH, existe uma população de CDs capturando antígenos e sinais de entrada. A multiplicidade de CDs é fundamental, pois são necessárias várias CDs apresentando análises sobre um mesmo tipo de antígeno para causar uma resposta do SIH. Assim, o ACD torna-se tolerante a erros, pois a classificação errônea feita por uma CD não é suficiente para estimular um erro de falso positivo do SIH. Uma vez que as CDs informam ao linfonodo sobre a presença de um invasor, as células B e T são ativadas, ficando responsáveis pela produção de anticorpos específicos para aquele patógeno.

3. Trabalhos Relacionados

Constatou-se que são poucos os trabalhos [Lebbe *et al.* (2008), Becker (2009), Liu e Yu (2008) e Kim *et al.* (2006)] que apresentam propostas de SDI inspirados no SIH e voltados especificamente para redes *ad-hoc* sem fio e RSSFs. Lebbe *et al.* (2008) apresentam uma proposta de SDI baseado na TP para redes *mesh* sem fio. Nessas redes, o perigo foi medido em termos de nós que “morriam”. Os autores propõem a realização de dois passos: (i) reconhecer o sinal de perigo; e (ii) classificar o sinal de perigo em diferentes níveis. Para tal, foi usada uma rede neural (*self-organizing maps* - SOMs) como um classificador dos níveis de perigo. Diferentemente desse trabalho, nossa proposta prevê o uso de mais do que um tipo de sinal (seguro, PAMP e perigo) para identificação de um intruso na RSSF e não faz uso de redes neurais. A utilização de mais de um tipo de sinal torna mais precisa a avaliação da presença de uma anomalia.

Nos trabalhos de Becker (2009) e Liu e Yu (2008), os autores apresentam propostas de SDI por anomalia usando a seleção negativa para detecção de intrusos. A seleção negativa considera antígenos próprios como normais e não-próprios anômalos, dependendo de uma base de dados que contenha os próprios. Diferentemente de ambos os trabalhos, nossa proposta não utiliza o algoritmo de seleção negativa e sim a TP, em particular, o ACD. A escolha da TP em detrimento de outras teorias do SIH se deve ao fato de que naquelas teorias assume-se que os antígenos classificados como não-próprios devem ser combatidos e os próprios não, necessitando de uma base de dados em constante atualização, sob pena de sofrer ataques do dia zero caso esteja desatualizada. A TP considera um “sinal de perigo” ao invés das características próprias e não-próprias na identificação de um elemento invasor possibilitando que o sistema seja capaz de detectar novos tipos de ataques. O emprego da TP é mais adequado do que a da seleção negativa para a detecção de intrusos em RSSF uma vez que uma base de dados com informações que identificarão os ataques é necessária na seleção negativa, mas não na TP, resultando em um menor consumo de memória. Adicionalmente, na seleção negativa somente os antígenos registrados na base de dados são identificáveis, enquanto que a TP classifica os antígenos como normais ou anômalos a partir da observação de sinais de perigo. Por fim, em nossa proposta existe cooperação por parte dos nós sensores, ou seja, existe avaliação coletiva de mau comportamento, aumentando a chance de acerto quanto à decisão de existir ou não um ataque, o que difere da proposta de Becker (2009).

Kim *et al.* (2006) propuseram a primeira implementação de um ACD aplicado a RSSF para a detecção de um novo tipo de ataque, que pode ocorrer especificamente quando o protocolo de difusão direcionada é usado. Diferentemente de Kim *et al.* (2006), onde os procedimentos do ACD e do protocolo de difusão direcionada estão entrelaçados, no presente trabalho o algoritmo proposto foi concebido de forma que seu código seja independente do código das aplicações e protocolos de RSSF, permitindo a reutilização dos seus componentes em diferentes cenários de aplicação.

4. SDI Imuno-inspirado customizado para RSSF

Nesta seção são descritos: (i) a arquitetura lógica do SDI proposto; (ii) o mapeamento dos elementos computacionais nos elementos imuno-inspirados; (iii) o ACD customizado para RSSFs; e (iv) estudo de caso.

4.1. Arquitetura Lógica do SDI

A arquitetura lógica do SDI para RSSF proposto (Figura 1) consiste dos seguintes componentes: Monitoramento, Gestor de Detecção de Intrusão, Gestor de Contexto, Gestor de Decisão, Bases de Parâmetros, Base de Regras e Contramedidas. Tais componentes foram agrupados em quatro subsistemas: (i) Ambiente Monitorado (E-BOX); (ii) Detector de Intrusos (A-BOX); (iii) Armazenador (D-BOX); e (iv) Contramedidas (C-BOX). A divisão do SDI em quatro subsistemas segue a arquitetura proposta pelo *Common Intrusion Detection Framework* [García-Teodoro *et al.* 2008].

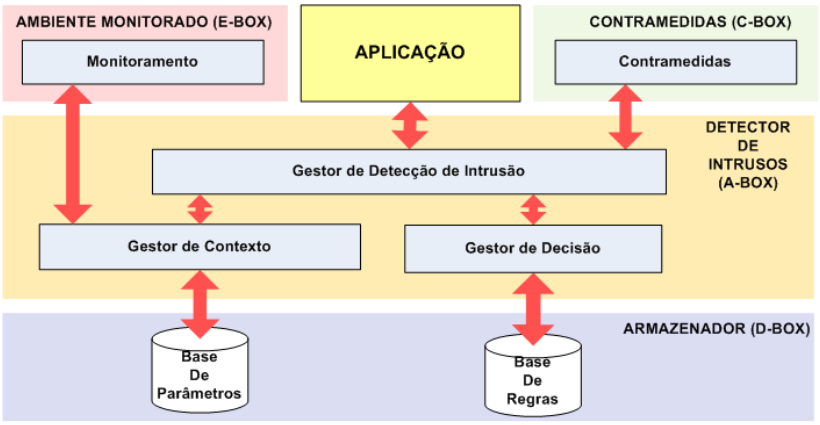

Figura 1. Arquitetura Lógica do SDI.

O subsistema **Ambiente Monitorado**, composto pelo componente Monitoramento, é responsável pela captura dos valores dos parâmetros de monitoramento definidos pelo Gestor de Contexto. No subsistema **Detector de Intrusos** são feitas as análises das informações coletadas para que seja tomada uma decisão referente à presença ou não de um intruso no ambiente onde se localiza o nó. Este subsistema é composto pelos componentes: Gestor de Detecção de Intrusão, Gestor de Contexto e Gestor de Decisão. O Gestor de Detecção de Intrusão, componente central na arquitetura, é o responsável por organizar as tarefas e coordenar as ações e respostas dos outros gestores. Durante a execução do sistema, o Gestor de Detecção de Intrusão informa ao Gestor de Contexto quais parâmetros devem ser monitorados. Os valores dos parâmetros recebidos do Gestor de Contexto são repassados pelo Gestor de Detecção de Intrusão para o Gestor de Decisão a fim de identificar a existência ou não de ataque, e, em caso de ataque, o seu tipo e o grau de anomalia. Essas informações são retornadas

para o Gestor de Detecção de Intrusão, que as encaminha para o componente de Contramedidas para decidir sobre a ação a ser executada. O Gestor de Contexto é responsável por duas funcionalidades: (i) gerenciar o monitoramento (solicitar a leitura de parâmetros ao componente de Monitoramento); e (ii) gerenciar a base de parâmetros (comparar os valores dos parâmetros recebidos do componente de Monitoramento com os valores mantidos na Base de Parâmetros e armazenar os novos valores coletados). O Gestor de Decisão é responsável por três funcionalidades: (i) executar o ACD customizado para RSSF; (ii) identificar um ataque por meio do processamento das informações geradas pelo algoritmo imuno-inspirado; e (iii) gerenciar a base de regras. O Gestor de Decisão necessita consultar no repositório Base de Regras as regras estabelecidas para cada tipo de ataque. Uma vez identificada uma possibilidade de ataque, o Gestor de Detecção de Intrusão é avisado. A detecção de diferentes ataques pode ser feita com a aplicação de um conjunto de regras distintas. O subsistema **Armazenador** representa a parte do sistema onde são armazenadas: (i) a Base de Parâmetros, que contém o histórico dos valores dos parâmetros coletados; e a (ii) Base de Regras, que contém as regras que identificam os tipos de ataques que o sistema é capaz de identificar. Já o de **Contramedidas** contém o componente de Contramedidas, responsável por executar ações de combate aos ataques identificados. As contramedidas podem ser ações diretas, executadas no próprio nó, ou o envio de informações de alerta ao administrador para que o mesmo tome alguma medida cabível.

4.2. Mapeamento dos elementos computacionais em imuno-inspirados

Os **antígenos** são representados como identificadores de um ataque específico sendo compostos por informações retiradas de mensagens enviadas ou recebidas pelos nós. Por exemplo, estas mensagens podem ser consideradas próprias ou não-próprias, ou seja, geradas por um nó legítimo ou não, sendo avaliadas quanto ao perigo que representam ao sistema. Os **patógenos** são tratados como sendo os ataques e os **anticorpos** as contramedidas. As **células dendríticas** são representadas pelo componente Gestor de Detecção de Intrusão e pela funcionalidade de gerenciar a base de parâmetros do Gestor de Contexto. O **linfonodo** é representado pelo mecanismo de decisão do Gestor de Decisão e as **células B** e **T** pelo componente de Contramedidas. Os sensores poderão assumir dois papéis diferentes: CDs e linfonodo. O sensor que assume o papel de CD (linfonodo) é chamado de sensor-cd (sensor-linfo). Os componentes Monitoramento, Gestor de Detecção de Intrusão, Gestor de Contexto e Bases de Parâmetros e de Regras estão localizados no sensor-cd. Gestor de Decisão e Contramedidas estão localizados no sensor-linfo. Os sinais de perigo, seguro e PAMP (**sinais de entrada**) são parâmetros variáveis e diferentes para cada tipo de ataque e serão discutidos nas próximas seções. As **Base de Parâmetros** e **de Regras** foram modeladas para disponibilizar a funcionalidade computacional de armazenamento de dados, sem buscar inspiração no sistema biológico.

4.3. Algoritmo das células dendríticas customizado para RSSF

A Figura 2 apresenta o pseudocódigo do ACD original, proposto por Greensmith (2007). Neste trabalho, o algoritmo ACD original foi adaptado de forma a melhor explorar a característica de densidade das RSSFs e reduzir o processamento e as estruturas de dados existentes em cada nó sensor. Os procedimentos do algoritmo foram divididos entre o sensor-cd e o sensor-linfo. Cada sensor-cd é responsável pelo procedimento de uma CD apenas. Assim, o *loop* da linha 8 foi excluído dos nós sensor-

cd. Além disso, o teste condicional da linha 14 e as linhas 15, 16 e 17 foram deslocadas para fora do *loop* da linha 5. Ao término de um ciclo de execução, o sensor-cd envia uma mensagem (de controle 1) para o sensor-linfo, indicando seu estado final e quais antígenos foram processados, e reinicia o ciclo de execução. As linhas 18 e 19, referentes ao cálculo do índice de anomalia, são executadas apenas pelo nó sensor-linfo, que usa como informação de entrada as mensagens recebidas dos nós sensores-cd, enviando para a EB uma mensagem (de controle 2) informando o MCAV obtido.

```
1.  //entradas: Sinais de Entrada e Antígenos
2.  //saídas: Antígenos e Estado da célula
3.  Inicializar Células_Dendríticas;
4.  Inicializar Parâmetros;
5.  Enquanto (Número_de_ciclos_da_Célula_Dendrítica < Limite_de_Ciclos) faça
6.      Coletar Antígenos;
7.      Atualizar Sinais_de_Entrada;
8.      Para (todas as Células_Dendríticas da População) faça
9.          Para (Antígenos_amostrados_pela_Célula_Dendrítica_no_Ciclo) faça
10.             Célula_Dendrítica amostra Antígenos;
11.         Para (todos os Sinais_de_Entrada) faça Preencher Matriz_de_Sinais_de_Entrada;
12.          Para (todos os itens do Vetor_de_Antígenos) faça Célula_Dendrítica processa Antígeno_do_Vetor;
13.         Para (todos os Sinais_de_Saída) faça Calcular Sinal_de_Saída_Temporário;
14.         Se (Sinal_de_Migração > Limiar_de_Migração) então
15.             Remover Célula_Dendrítica da População;
16.             Calcula Estado da célula e migra Célula para o linfonodo;
17.             Resetar Vetor_de_Antígenos e todos os sinais;
18. Calcular o índice de anomalia (MCAV);
19. Se (MCAV maior do que limite) então Enviar Alerta;
```

Figura 2. Pseudocódigo do ACD [Greensmith 2007].

É importante mencionar que no algoritmo original o aumento de confiabilidade quanto à decisão de existir ou não um ataque era obtido pela existência de um conjunto de CDs em um único dispositivo. Em nossa proposta, essa confiabilidade é obtida fazendo com que existam vários nós com a funcionalidade de sensor-cd e um sensor-linfo (para cada grupo de sensores sensor-cd) que reúne as avaliações sobre a existência ou não de ataque provenientes desses nós sensor-cd. Essa decisão visa explorar o fato das RSSFs serem constituídas por vários pequenos nós dispostos próximos uns dos outros, o que permite ter diferentes ângulos de visão sobre um mesmo ponto de ataque.

4.4. Funcionamento do SDI e Estudo de Caso

A fim de melhorar a compreensão, é importante mencionar que o procedimento do SDI proposto é dividido em quatro fases: (i) Fase de Coleta, (ii) Fase de Análise, (iii) Fase de Decisão e (iv) Fase de Reação. No contexto biológico, os procedimentos relativos à primeira e a segunda fase estão relacionados com os procedimentos das CDs, enquanto que a terceira fase está relacionada com os procedimentos associado ao linfonodo. A quarta fase representa as reações contra os invasores que são tomadas pelo SDI. No contexto computacional, os procedimentos relativos à primeira fase estão relacionados com os componentes de Monitoramento e Gestor de Contexto (tarefa de gerenciar o monitoramento). Os procedimentos relativos à segunda fase estão relacionados com o Gestor de Contexto (gerenciar base de parâmetros) e o Gestor de Decisão (gerenciar base de regras e algoritmo imuno-inspirado). Os procedimentos relativos à terceira fase relacionam-se com o Gestor de Contexto (gerenciar base de parâmetros) e o Gestor de Decisão (identificar ataque). Os procedimentos relativos à fase de reação estão relacionados com o componente Contramedidas.

Para descrever com mais detalhe cada uma dessas fases e como elas se aplicam no cenário de uma RSSF, considera-se como caso de uso uma aplicação de monitoramento de temperatura em uma área de preservação florestal. Nessa aplicação, os nós sensores são dispostos de forma aleatória em uma região aberta e são programados para realizar coletas periódicas de temperatura e enviá-las a uma EB. Nesse tipo de aplicação, os sensores podem ser configurados para intercalarem períodos de ativação (onde capturam dados e trocam mensagens) e períodos de dormência (onde são desligados para economizar energia). Nessa aplicação, o tempo de vida da rede é de crucial importância em detrimento do atraso de detecção de uma anomalia. Nesse estudo de caso, considera-se a possibilidade de ataques do tipo *denial-of-sleep*. Esse ataque pode ser feito inserindo na rede um sensor malicioso que gera mensagens aleatórias com potência de sinal elevada. Essas mensagens ocupam o meio fazendo com que os sensores permaneçam acordados por um período maior de tempo esperando que o meio fique livre para então enviar as mensagens para a EB. Nesse estudo de caso, a primeira questão a tratar é determinar quais elementos devem ser usados como antígeno para o tipo de ataque *denial-of-sleep* e quais parâmetros deverão ser usados como sinais de entrada. Como esse tipo de ataque está diretamente relacionado com as mensagens que são trocadas na rede, uma alternativa é considerar as mensagens recebidas em cada nó sensor como sendo um antígeno. Para os sinais de entrada, pode-se considerar, por exemplo, a potência do sinal recebido com cada mensagem (RSSI) e a taxa de mensagens recebidas e enviadas pelo nó sensor.

A **fase de coleta** tem início com a execução do ACD nos sensores com o papel de sensor-cd. O sensor pode operar no modo promíscuo, capturando todas as mensagens trocadas na rede, ou no modo normal, capturando apenas as mensagens destinadas àquele nó. Para cada mensagem recebida, o sensor coleta os sinais de entrada definidos e o antígeno. A **fase de análise** é responsável pela identificação do ataque. A análise é baseada na comparação de parâmetros e regras previamente definidos e armazenados nas Bases de Parâmetros e de Regras. O Gestor de Contexto, na sua funcionalidade de gerenciamento da base de parâmetros, avalia o valor de um parâmetro recebido do Monitoramento (taxa de mensagens recebidas, RSSI e o inverso da variação da taxa de mensagens recebidas) comparando-o com um limiar. Caso o parâmetro esteja dentro do limiar de operação, seu valor será armazenado em um histórico na Base de Parâmetros; em seguida, o Gestor de Detecção de Intrusão será avisado e o sistema continuará operando normalmente. Caso contrário, o Gestor de Contexto passa esta informação ao Gestor de Detecção de Intrusão, que a repassa para o Gestor de Decisão. No Gestor de Decisão esta informação serve de entrada para o ACD. Este procedimento é repetido até que o número de mensagens recebidas atinja o valor do limiar de migração fazendo com que o sensor-cd envie uma mensagem de controle contendo as informações de antígenos e estado de maturação para o sensor-linfo. A fase de análise do algoritmo original foi concebida para ser executada 3 vezes, segundo a Equação 1, uma para cada sinal de saída. Neste trabalho, optamos por eliminar a execução da fase de análise para o sinal de saída CSM. O sinal de saída CSM era utilizado no algoritmo original com o intuito de obter uma maior confiabilidade no resultado da avaliação, uma vez que forçava que cada CD avaliasse os sinais de entrada durante um determinado tempo (limiar de migração). Na RSSF, tal confiabilidade é garantida quando o procedimento do algoritmo proposto neste trabalho é executado até o recebimento de um número pré-determinado de mensagens (limiar de migração). A **fase de decisão** é realizada no sensor-linfo (Gestor de Decisão), onde as mensagens recebidas dos nós sensor-cd são

contabilizadas e os antígenos apresentados por elas são classificados como normais ou anômalos, gerando o índice MCAV para cada um deles. Este índice é passado para o Gestor de Detecção de Intrusão, que o repassa para o componente de Contramedidas, dando início a quarta e última fase. No cenário de aplicação que estamos considerando, temos apenas um tipo de antígeno, o qual está implicitamente associado ao ataque do tipo *denial-of-sleep*. Na **fase de reação**, o componente de Contramedidas recebe informações do tipo e intensidade do ataque (índice MCAV) que está ocorrendo na rede e dá às ações de combate aos invasores, lançando anticorpos que irão combater a invasão. A execução das contramedidas pode ser feita no próprio sensor-linfo onde a reação básica pode ser o envio de uma mensagem especial para a EB ou para outros sensores, alertando sobre o ataque.

5. Experimentos com o SDI Imuno-Inspirado para RSSFs

No primeiro e segundo experimentos aqui descritos, simulações foram realizadas com o intuito de calibrar o SDI proposto. No primeiro busca-se determinar o valor mais adequado para o limiar de migração em termos de número de mensagens recebidas. Já no segundo busca-se determinar o número de sensor-cd por sensor-linfo em termos de taxa de acerto na detecção de um ataque e taxa de acerto em relação a uma situação normal de forma a detectar com precisão e exatidão o ataque *denial-of-sleep* por parte de um único linfonodo. No terceiro experimento, as três primeiras fases do fluxo de execução do SDI proposto (coleta, análise e decisão) foram implementadas em sensores reais com o objetivo de avaliar a eficiência do algoritmo e impacto do SDI na RSSF.

5.1. Ambiente de experimento

Nos experimentos reais e simulados, a RSSF foi composta por sensores da plataforma MICAz, comercializados pela *Crossbow Technology* [Crossbow 2010]. Os sensores foram programados dentro do ambiente de desenvolvimento TinyOS [Levis e Gay 2009], versão 2.1.0, usando a linguagem nesC [Levis e Gay 2009], uma extensão da linguagem C, que implementa um modelo de programação orientado a eventos. O TinyOS é um framework baseado em componentes, projetado especificamente para o desenvolvimento de soluções para RSSFs. Os experimentos reais foram realizados em ambiente fechado (laboratório).

Os cenários simulados foram realizados com o simulador TOSSIM [Levis e Gay 2009], próprio do TinyOS. O TinyOS disponibiliza diversos componentes de software, incluindo os componentes que implementam a pilha de protocolos de comunicação. Cada componente TinyOS possui uma interface bem definida, implementada por meio de funções que são caracterizadas como tratadores de eventos ou comandos. O SDI proposto foi implementado definindo-se dois novos componentes para o TinyOS: o *SDICelulaDendriticaC*, com a funcionalidade de CD, implementado nos nós sensores-cd; e o SDILinfonodoC, com a funcionalidade de linfonodo, implementado nos nós sensores-linfo. O componente *SDICelulaDendriticaC* foi projetado de modo a ser usado pelas aplicações no lugar do componente padrão *AMReceiverC*. Este último faz o recebimento de mensagens do TinyOS. Desta forma, todas as mensagens que chegam ao nó sensor são avaliadas pelo componente *SDICelulaDendriticaC* e repassadas de forma transparente para a aplicação em execução no sensor. Este componente disponibiliza interfaces que permitem: (i) ativar e desativar o rádio do sensor; (ii) obter os valores RSSI (potência do sinal recebido) no momento da recepção de cada

mensagem; (iii) calcular a taxa de mensagens recebidas pelo nó sensor; (iv) executar o ACD. O componente *SDILinfonodoC* também foi projetado de modo a ser usado pelas aplicações no lugar do componente TinyOS padrão de recebimento de mensagens *AMReceiverC*. Sua função adicional consiste em receber e tratar as mensagens especiais enviadas pelos sensores-cd. As outras mensagens recebidas são repassadas de forma transparente para a aplicação. Este componente disponibiliza interfaces com as seguintes funcionalidades: (i) ativar ou desativar o rádio do sensor; (ii) receber dos sensores com o componente *SDICelulaDendriticaC* as mensagens contendo as informações das CDs, contabilizando a quantidade de vezes que os estados maduro e semi-maduro foram recebidos; (iii) controlar, segundo uma periodicidade determinada pelo administrador da rede, quando o linfonodo deverá calcular o índice MCAV; (iv) ativar os elementos responsáveis pelas contramedidas (para efeito dos experimentos realizados nessa etapa, essa funcionalidade não foi implementada, uma vez que espera-se medir apenas os índices de acertos e erros na detecção dos ataques).

O nó malicioso (*Jammer*) foi implementado como uma aplicação que utiliza os componentes de comunicação padrão do TinyOS, gerando mensagens na rede a uma taxa determinada, intercalando períodos de ativação e de desativação.

5.2. Descrição do cenário, experimentos, e métricas

Para os experimentos, adotou-se uma rede de topologia plana e com nós fixos tanto para a implementação real quanto para as simulações. Foi considerado apenas o ataque de interferência (*jamming*), um tipo de ataque *denial-of-sleep*, que se caracteriza por causar um ruído no meio, atrapalhando a comunicação entre os nós. Foi deixada como trabalho futuro a análise da detecção de outros tipos de ataques em RSSFs.

A RSSF foi composta por: (i) nós sensores-cd, com o componente *SDICelulaDendriticaC*; (ii) um nó sensor-linfo, com o componente *SDILinfonodoC*; e (iii) um nó sensor *Jammer*. Foi utilizado um intervalo de 100 ms para o envio das mensagens do *Jammer*. O *Jammer* foi posicionado a 1 metro do sensor-linfo. Para aplicar o ACD customizado para RSSFs para a detecção do ataque de *denial-of-sleep*, os sinais de entrada foram definidos e mensurados a partir das mensagens recebidas pelos sensores-cd da seguinte forma: (i) sinal de PAMP, definido como sendo o nível do RSSI presente no meio quando o sensor-cd recebe uma mensagem; (ii) sinal de perigo, obtido calculando a taxa das mensagens recebidas pelo sensor-cd; e (iii) sinal seguro, definido como sendo o inverso da variação da taxa das mensagens recebidas pelo sensor-cd.

Na equação 1, os pesos foram definidos empiricamente a partir de experimentos imunológicos conduzidos por imunologistas do "*The Danger Project*" [Silva (2009)]. Assim, para o sinal de saída semi-maduro os pesos W*p*, W*d* e W*s* assumem, respectivamente, os valores 0, 0 e 1. Por fim, para o sinal de saída maduro, os pesos W*p*, W*d* e W*s* assumem, respectivamente, os valores 2, 1 e -3. A inflamação não será considerada neste trabalho.

No algoritmo proposto, a ativação de um dado sensor-cd para que seja iniciada a avaliação das CDs ocorre apenas quando há o recebimento de mensagens por parte do sensor-cd em questão. No algoritmo original ocorre uma coleta contínua de antígenos e de sinais, levando a um processamento também contínuo. Tal simplificação visa à redução no gasto de energia e no tempo de processamento dos sensores.

5.3. Simulações

Para as simulações, a quantidade de sensores-cd foi variada entre 1, 2, 3, 5, 7 e 10 sensores, tendo os mesmos sido dispostos ao longo de um círculo de três metros de diâmetro de forma a permanecerem eqüidistantes do sensor-linfo, o qual foi posicionado no centro desta circunferência. Cada nó foi programado de forma a possuir uma identificação única e um alcance de rádio omnidirecional fixo de 15 metros. Foram realizados dois experimentos a fim de escolher os melhores parâmetros a serem utilizados pelo algoritmo proposto. Em cada um destes experimentos foi variada uma das características do algoritmo: (i) o limiar de migração das células, que é controlado pela quantidade de mensagens a serem recebidas por um sensor-cd de forma a serem extraídos os antígenos; e (ii) o número de sensores-cd por linfonodo, representando a quantidade de CDs que informam a um determinado linfonodo sobre a situação do ambiente em que se encontram. Cada teste foi repetido 30 vezes, permitindo obter resultados com um intervalo de confiança de 95%.

5.3.1. Variando o limiar de migração

Neste experimento foram realizadas variações para o limiar de migração utilizado pela CD com intuito de determinar a quantidade de mensagens que o sensor-cd deveria analisar antes de definir o estado de maturação da CD. Após receber a quantidade determinada de mensagens, o sensor-cd define o estado de maturação da CD e envia essa informação para o sensor-linfo. Foi utilizado apenas um sensor-cd e o limiar do MCAV no sensor-linfo foi fixado em 50% (100% de acerto [Silva 2009]). Ou seja, para todos os MCAV maiores ou iguais a 50%, o algoritmo proposto indica a presença de intruso. Em cada rodada foram realizadas 30 avaliações do MCAV, sendo que o sensor-linfo realiza esta avaliação em intervalos regulares de 10 segundos. A Tabela 1 apresenta os resultados obtidos nesse experimento. Os valores são: (i) falsos positivos (FP), que indicam a quantidade de alarmes falsos; (ii) falsos negativos (FN), que indicam uma condição de normalidade quando na verdade está ocorrendo um ataque; (iii) verdadeiros positivos (VP), que indicam que está ocorrendo um ataque durante um ataque; e (iv) verdadeiros negativos (VN), que indicam uma condição de normalidade quando não está ocorrendo nenhum ataque.

Tabela 1. Variação do limiar de migração para 1 sensor-cd.

Limiar de Migração	1	3	5	7	8	9	10	20	25
VP	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%	50,00%	48,92%	41,57%
VN	50,00%	50,00%	50,00%	50,00%	49,90%	49,61%	49,41%	48,53%	48,33%
FP	0,00%	0,00%	0,00%	0,00%	0,10%	0,39%	0,59%	1,47%	1,67%
FN	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	1,08%	8,43%

Observa-se que com o aumento do limiar de migração ocorre aumento nos valores de FP e FN. Com o limiar de migração na faixa de 1 a 7, obtemos os melhores valores de FP e FN. A atribuição de um valor alto para o referido limiar ocasiona uma detecção tardia de um evento de anomalia, tornando a detecção ineficiente. Porém, a atribuição de um valor baixo implica um número maior de mensagens de controle enviadas do sensor-cd para o sensor-linfo, gerando um maior gasto de energia. Como nosso estudo de caso prioriza o tempo de vida da rede em detrimento do atraso da detecção de anomalias, optamos por trabalhar com um número de limiar de migração igual a 7.

5.3.2. Quantidade de células dendríticas por linfonodo

Neste experimento variamos o número de sensores-cd que enviam informações para um mesmo sensor-linfo de forma a identificar o número ideal de sensores-cd por sensor-linfo. Cada sensor-cd foi configurado com limiar de migração igual a 7. A Tabela 2 mostra os valores de VP, VN, FP e FN em percentuais, variando a quantidade de sensores-cd e observando os MCAV informados pelo sensor-linfo. Podemos observar que o aumento do número de sensores-cd por sensor-linfo torna o sistema mais preciso (taxas de VP e VN iguais a 100%), uma vez que obtém-se índices de MCAV maiores. De acordo com a Tabela 2, os melhores resultados de VP e FN são obtidos para 5 ou 7 sensores-cd por sensor-linfo. Apesar de 10 sensores-cd, não ilustrado na tabela, também apresentarem altas taxas de VP e FN, estes apresentam baixas taxas de VN e FP.

Tabela 2. Variação do número de sensores-cd por linfonodo e limiar MCAV.

Sensores	MCAV (%)											
	0		10	20	30	40	50	60	70	80	90	100
5	VP	50,00	50,00	50,00	50,00	50,00	50,00	50,00	50,00	44,51	7,45	0,00
	VN	0,00	39,71	47,94	49,41	50,00	50,00	50,00	50,00	50,00	50,00	50,00
	FP	50,00	10,29	2,06	0,59	0,00	0,00	0,00	0,00	0,00	0,00	0,00
	FN	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	5,49	42,55	50,00
7	VP	50,00	50,00	50,00	50,00	50,00	50,00	50,00	50,00	44,81	8,04	0,00
	VN	0,00	41,57	48,43	49,90	50,00	50,00	50,00	50,00	50,00	50,00	50,00
	FP	50,00	8,43	1,57	0,10	0,00	0,00	0,00	0,00	0,00	0,00	0,00
	FN	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	5,19	41,96	50,00

A fim de extrair informações qualitativas a respeito do ACD proposto neste trabalho, foram utilizados os resultados obtidos no experimento anterior para a elaboração das curvas ROC (*Receiver Operating Characteristics*). Estas curvas são uma técnica de medição de efetividade para detectores de intrusos baseados em anomalias [Silva 2009]. Os valores medianos de VP, VN, FP e FN foram usados na extração dos valores das medidas de sensibilidade e especificidade. A sensibilidade é calculada pela razão entre a quantidade de VP dividido pela soma de VP e FP, ou seja, Sensibilidade=VP/(VP+FN). A especificidade é calculada pela razão entre a quantidade de VN dividida pela soma dos VN e FP, ou seja, Especificidade=VN/(VN+FP). A partir dos valores de especificidade e sensibilidade, os melhores valores para o MCAV foram encontrados. Por questões de espaço, os valores da sensibilidade e da especificidade são representados na Figura 3 apenas para 2 e 5 sensores-cd. Observa-se que a taxa de especificidade cresce com o aumento do valor do limiar de anomalia, significando que um limiar baixo pode ocasionar FP. Por outro lado, a taxa de sensibilidade começa com um valor igual a 1 e decresce com o aumento do MCAV, causando aumento nos FN.

A melhor configuração de parâmetros em termos de detecção de intrusos é aquela que apresenta os valores mais altos, tanto da sensibilidade quanto da especificidade, ou seja, quando ambos os valores são iguais a 1, ocasionando uma interseção entre as curvas. No que concerne à sensibilidade, pode-se observar que conforme o número de sensores-cd por sensor-linfo aumenta, a faixa de valores de limiar de anomalia que tem valor igual a 1 passa a ser maior. Por exemplo, para 2 sensores-cd, os valores de MCAV que se encontram no intervalo de 0 a 60% possuem valor igual a 1 para sensibilidade. Já para 5 sensores-cd, os valores de MCAV que se encontram no intervalo de 0 a 70% possuem valor igual a 1 para sensibilidade. Quanto à especificidade, a Figura 3 mostra que alcançamos especificidade igual a 1 para valores de MCAV acima de 30%, para o

caso de 2, 5 e 7 sensores-cd. Já para o caso de 10 sensores-cd, o MCAV deve ser maior que 50% para um valor de especificidade igual a 1. Sabe-se que quanto maior o número de sensores por linfonodo maior será o número de colisões. Portanto, levando em consideração as informações: (i) aumento do número de colisões quando se aumenta a quantidade de sensores; (ii) curva de sensibilidade; e (iii) curva de especificidade; podemos concluir que 5 sensores-cd por sensor-linfo é um número adequado para ser usado na configuração dos parâmetros do algoritmo.

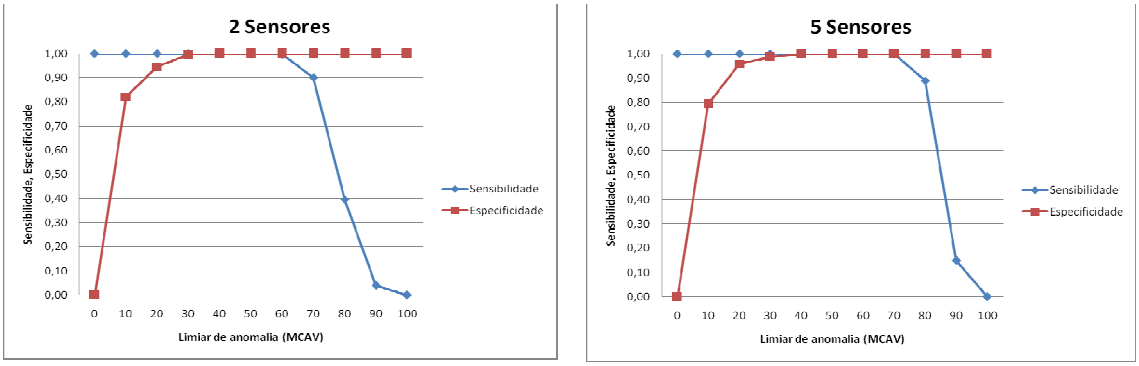

Figura 3. Curvas ROC para os 2 e 5 sensores-cd.

5.4. Experimento com sensores reais

Para o experimento real, estavam disponíveis 30 sensores. Foram usados 6 sensores-linfo com 3 sensores-cd cada; 4 sensores fontes responsáveis por transmitir mensagens de 1 em 1 segundo aos sensores-cd; um sensor atacante e uma EB. A EB ficou responsável por receber as mensagens contendo as avaliações dos sensores-linfo assim como as mensagens de dados sensoriados a partir de um único sensor-linfo. Os sensores foram dispostos em uma topologia de grade, em um esquema fixo e determinístico. Na grade a escala utilizada foi de 0,5 m de distância entre os sensores-linfo e todos os nós foram dispostos no solo, ou seja, suas posições serão descritas em um plano 2D.

Os sensores foram dispostos da seguinte forma: (i) a EB foi posicionada nas coordenadas (0,3) do plano 2D, recebendo todas as mensagens de dados e controle emitidas pelo sensor-linfo, posicionado nas coordenadas (2,4); (ii) 6 sensores-linfo foram posicionados em (2,4), (6,4), (10,4), (2,2), (6,2) e (10,2); (iii) 18 sensores-cd foram dispostos a 10 cm de seu respectivo sensor-linfo; (iv) 4 sensores fonte de mensagens foram posicionados entre os sensores-cd; (v) o *Jammer* foi posicionado em (12,3), de forma a ficar próximo dos sensores-linfo localizados em (10,4) e (10,2) e sua interferência foi especificada de modo a afetar todos os sensores.

Os resultados dos experimentos foram como segue. Para os dois sensores-linfo mais próximos do *Jammer*, foram obtidos os valores: (i) FN:0,52% e 2,28%; (ii) VN: 45,50% e 45,94%; (iii) FP: 4,78% e 5,00%; e (iv) VP: 49,21% e 46,77%. Para os dois sensores-linfo localizados entre a EB e o *Jammer*, foram obtidos os valores: (i) FN: 14,87% e 6,68%; (ii) VN: 48,53% e 45,91%; (iii) FP: 1,76% e 4,48%; e (iv) VP: 34,84% e 42,92%. Para os dois sensores-linfo mais distantes do *Jammer*, foram obtidos os valores: (i) FN: 44,37% e 35,72%; (ii) VN: 49,88% e 48,46%; (iii) FP: 0,22% e 2,76%; e (iv) VP: 5,53% e 13,06%. Com estes resultados observamos que o *Jammer* pode ser identificado eficientemente pelos dois sensores-linfo mais próximos e, à medida que a distância entre os sensores-linfo e o *Jammer* aumentava esta eficiência diminuiu em decorrência da atenuação do sinal do *Jammer*, conforme era esperado.

6. Conclusões

Este trabalho teve como objetivos apresentar um estudo sobre a detecção de intrusos e propor um SDI baseado em anomalias e customizado para RSSFs. Tal SDI foi programado de forma a atender às demandas e restrições deste tipo de rede. Nos experimentos realizados, a detecção descentralizada mostrou-se eficaz na detecção de um ataque. Com o uso da TP, além da detecção propriamente dita, conseguiu-se mostrar também, em cada sensor no papel de linfonodo, um valor qualitativo do ataque impetrado pelo invasor na RSSF (índice de anomalia).

Em trabalhos futuros serão investigadas outras opções de cálculo do limiar de migração, com o intuito de analisar a relação entre o gasto de energia e a eficiência na detecção do intruso. Pretende-se também realizar testes para averiguar o impacto computacional do SDI quanto ao consumo de recursos dos sensores. Por fim, será realizada a comparação dos resultados obtidos neste trabalho com outros da literatura.

Referências

Aickelin, U. *et al.* (2003) "Danger Theory: The Link between AIS and IDS?", Lecture Notes in Computer Science, v. 2787, páginas 147-155.

Becker M. *et al.* (2009) "On Classification Approaches for Misbehavior Detection in Wireless Sensor Networks", Journal of Computers, v. 4, número 5, Maio.

Crossbow (2010) "Crossbow Technology", http://www.xbow.com/. Acessado em 2010.

García-Teodoro, P. *et al*. (2008) "Anomaly-based network intrusion detection: Techniques, systems and challenges", Computers & Security, v. 28, páginas 18-28.

Greensmith, J. (2007) "The Dendritic Cell Algorithm", PhD Thesis, University of Nottingham.

Greensmith, J. *et al.* (2005) "Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection", 4th International Conference on Artificial Immune Systems, Canada.

Kim, J. *et al.* (2006) "Danger Is Ubiquitous: Detecting Malicious Activities in Sensor Networks Using the Dendritic Cell Algorithm", Artificial Immune Systems, Springer Berlin, v. 4163/2006, páginas 390-403.

Lebbe, M. *et al*. (2008) "Artificial Immune System inspired danger modelling in Wireless Mesh Networks", Proceedings of the International Conference on Computer and Communication Engineering, Kuala Lumpur, páginas 984-988, Kuala Lumpur.

Liu, Y. e Yu, F. (2008) "Immunity-Based Intrusion Detection for Wireless Sensor Networks", Neural Networks, IJCNN, páginas 439-444, 2008.

Matzinger, P. (2002) "The Danger Model: A Renewed Sense of Self", Science, v. 296, número 5566, páginas 301-305,2002.

Silva, G. (2009). "Detecção de Intrusão em Redes de Computadores: Algoritmo Imunoinspirado Baseado na Teoria do Perigo e Células Dendríticas", Tese de Mestrado, Programa de Pós-Graduação da Engenharia Elétrica, UFMG, 2009.

Yick, J. *et al.* (2008) "Wireless sensor network survey", Computer Networks, número 52, p. 2292-2330.