EWIDS: Uma Extensão para Arquiteturas de Sistemas de Detecção de Intrusos para Redes Sem Fio Metropolitanas

Nilson Rocha Vianna[1,2], Reinaldo de B. Correia[1], Luci Pirmez[1]

[1]Universidade Federal do Rio de Janeiro - Núcleo de Computação Eletrônica
Prédio do CCMN - Bloco C, Caixa Postal: 2324 - CEP: 20.010-974
Cidade Universitária - Ilha do Fundão, Rio de Janeiro, RJ

[2]Diretoria de Telecomunicações da Marinha (DTM)
Rua 1º de março, 118 – 3º, 4º e 5º andares
centro – Rio de Janeiro, RJ – CEP: 20.090-070

nilsonrv@posgrad.nce.ufrj.br, luci@nce.ufrj.br

Abstract. *The increasing use of wireless networks and its vulnerabilities stimulate the inclusion of more robust security requirements in the standards. The IDS proposals found in literature depend on constant updates in bases of signatures and/or normal activities in a network. This work presents a proposal of an architecture extension for IDS based on fuzzy logic, incorporating authentication processes based on transmitter fingerprinting and by a mobility kinematics analysis. Tests in the archetype present resulted promising in scenes of metropolitan wireless network.*

Resumo. *O crescente uso de redes sem fio e as suas vulnerabilidades incentivam a inclusão de requisitos de segurança mais robustos nos padrões. As propostas de IDS encontradas na literatura dependem de constantes atualizações em bases de assinaturas e/ou atividades normais nas redes. Este trabalho apresenta uma proposta de extensão de uma arquitetura para IDS baseada em lógica nebulosa, incorporando processos de autenticação fundamentados em assinatura de transmissão rádio e em uma análise cinemática da mobilidade. Testes no protótipo apresentam resultados promissores em cenários de rede sem fio metropolitana.*

1. Introdução

A crescente necessidade de mobilidade associada aos avanços tecnológicos das redes sem fio popularizou o seu uso. Além disso, o baixo custo de instalação e as facilidades de configurações fazem com que as redes sem fio sejam cada vez mais utilizadas em empresas, escritórios e residências. Apesar dessas vantagens existem desafios intrínsecos a este tipo de ambiente que propiciam um vasto campo para pesquisa.

Os atuais desafios estão relacionados principalmente ao fato do meio ser de difusão. As interferências na transmissão via rádio, a atenuação do sinal em relação à distância e a presença de obstáculos provocam uma alta taxa de erros, perdas de QoS e interrupções da conexão. Já o compartilhamento do mesmo meio por diferentes tipos de usuários, autorizados ou não, possibilita a escuta do tráfego e transmissões ilegítimas no canal [Boom 2004].

Para minimizar estes problemas e viabilizar a interoperabilidade entre equipamentos de diversos fabricantes, surgem os padrões que, geralmente, carecem de definições mais completas que contemplem as reais exigências e atendam aos aspectos

de QoS e Mobilidade [Johnston e Walker 2004]. Entre eles estão os IEEE 802.11 (Redes Locais Sem Fio) e o IEEE 802.16 (Redes Metropolitanas Sem Fio) [IEEE 2004][IEEE 2005].

No tocante ao requisito segurança, foco do presente trabalho, tê-lo garantido já é uma tarefa complexa para redes que adotam infra-estruturas cabeadas, onde o meio de transmissão é naturalmente protegido. Nas redes sem fio, o meio de difusão estabelece novas vulnerabilidades oriundas da possibilidade de interceptação do sinal por usuários não autorizados [Stallings 2002].

Diversas soluções clássicas de segurança [Crothers 2002] são adaptadas ao meio sem fio tais como *Firewalls* e IDS (*Intrusion Detection System*) [Zhang et al 2003]. Porém, o procedimento de adaptação não é suficiente para conter um "mau uso" destas redes, pois o meio sem fio introduziu uma diversidade de novas vulnerabilidades. Na taxonomia de um IDS surgem os WIDS (*Wireless Intrusion Detection System*) [Schmoyer et al 2004] [Zhang et al 2003], que se propõem a incrementar os níveis de segurança nas redes sem fio, em face das vulnerabilidades existentes nos protocolos e padrões.

O presente trabalho apresenta uma proposta de extensão da arquitetura clássica de um IDS [Crothers 2002] que não impacte os requisitos de QoS e Mobilidade. A arquitetura proposta atua de forma independente dos algoritmos de criptografia utilizados. Esta incorpora em um único sistema os processos de autenticação baseados em ***assinatura de transmissão rádio*** do dispositivo [Hall et al 2004], assim como os baseados em uma ***análise cinemática da mobilidade*** do mesmo, implementados neste trabalho. Como contribuições do presente trabalho estão: **(i)** a possibilidade de detecção de intrusos independentemente de atualizações em bases de assinaturas de ataques e/ou anomalias; **(ii)** a possibilidade de detecção de ataques do "dia zero" (ataques sem assinatura conhecida); **(iii)** a não interferência nos requisitos de QoS e Mobilidade, fundamentais nos cenários aplicados e **(iv)** redução significativa de falsos positivos e negativos, limitando a liberdade de posicionamento dos atacantes. Para a validação da proposta, cenários de uma rede sem fio metropolitana foram gerados e as simulações demonstraram a eficácia do protótipo implementado quanto à identificação dos atacantes.

O restante deste trabalho está estruturado em sete seções. Na segunda seção são apresentados os conceitos básicos relacionados ao trabalho. Na terceira seção são descritos os trabalhos relacionados. Na quarta seção é apresentada uma descrição da arquitetura EWIDS (*Extended Wireless Intrusion Detection System)* proposta. Na quinta seção é descrita a implementação do protótipo. Na sexta seção são apresentados os resultados das simulações realizadas. O trabalho é finalizado na sétima seção com a apresentação da conclusão e os possíveis trabalhos futuros.

2. Conceitos básicos

Nesta seção, são abordados os conceitos básicos relacionados com o presente trabalho, entre eles: o padrão IEEE 802.16, requisitos de segurança em redes sem fio e lógica nebulosa.

2.1 Padrão IEEE 802.16

O padrão IEEE 802.16-2004 [IEEE 2004] especifica a interface aérea de sistemas fixos de acesso sem fio de banda larga (BWA - Broadband Wireless Access) com suporte a serviços multimídia. O padrão foi criado para operar com estações fixas: estação base (BS) e estações assinantes (SS). Permite arquiteturas ponto-multiponto (PMP) e em malha (*Mesh*). Na topologia PMP, as SS se comunicam apenas com as Estações Bases, formando uma estrutura hierárquica semelhante às das redes celulares. Na topologia *mesh*, cada nó possui uma vizinhança e circunvizinhança por onde são "roteados" os fluxos de entrada e saída. Opera nas faixas de freqüência de 10 a 66 GHz ou abaixo de 11GHz.

O novo padrão IEEE 802.16e [IEEE 2005] adiciona mobilidade ao padrão de IEEE 802.16-2004, permitindo que as estações assinantes, agora nomeadas de *Mobile Station* (MS), se movimentem livremente na área de cobertura, realizando os procedimentos de *handoff* entre as células.

2.2 Segurança em Redes sem Fio

Um requisito de segurança é uma funcionalidade que um componente de software pode vir a oferecer. Os principais requisitos ou serviços de segurança são [Stallings 2002]: confidencialidade, autenticação, integridade, irretratabilidade ou não repúdio, disponibilidade, controle de acesso e auditoria.

Ferramentas são construídas visando a prevenção ou minimização de ataques contra esses requisitos de segurança. Ataques [Stallings 2002][Schmoyer et al 2004] como *MAC spoofing*; *Man-in-the-middle* (*MiTM*); e *Session Hijack* (Roubo de sessão) são muito comuns em redes sem fio e proporcionam ao atacante a possibilidade de obter informações privadas de outros usuários ou de realizar atividades maliciosas usando a identidade de terceiros. Sua detecção é vital no tempo de resposta a incidentes de segurança.

Quanto à origem do ataque, é considerado que os mesmos podem ter duas origens: **externos**, que são os realizados de fora das fronteiras da instituição a que pertence; e **internos**, que são os praticados de dentro das fronteiras da instituição, geralmente por pessoas que possuem privilégios de acesso como funcionários mal intencionados, insatisfeitos e/ou pessoas infiltradas que, através de técnicas de engenharia social, obtiveram acesso.

Em relação às fronteiras de uma instituição, estas são muito mais complexas de definir no universo da transmissão sem fio. Nas redes cabeadas, os dados trafegam em um ambiente confinado e fisicamente controlado, o que facilita o controle de acesso aos mesmos. Nas transmissões rádio, o sinal da rede ultrapassa os limites físicos da instituição, possibilitando que um usuário indesejado possa acessar a mesma. Em outras palavras, nas redes sem fio não existem fronteiras físicas e sim fronteiras lógicas, referentes aos domínios onde estão inseridas as entidades usuárias do sistema. Por exemplo, um provedor de serviços de banda larga sem fio e móvel possui diversas empresas/instituições como usuário (cliente) em um dado centro urbano. Todos estes usuários passam a pertencer a um mesmo domínio de rede: o provedor de serviços. Entretanto, esses usuários pertencentes a diferentes instituições são usuários "internos" de um mesmo domínio lógico de controle de acesso, que compartilham a infra-estrutura sem fio desse provedor. Esta descrição torna o componente segurança muito mais

desafiador, principalmente quando existe a possibilidade de instituições concorrentes estarem compartilhando o mesmo domínio sem fio metropolitano.

Quase sempre, um ataque é precedido de uma atividade suspeita. Para tal, existem ferramentas auxiliares que podem ser classificadas conforme seu objetivo em [Crothers 2002]: analisadores de vulnerabilidades; monitores de rede; protetores de integridade; controladores de acesso; e finalmente, os sistemas de detecção de intrusos (IDS).

Quanto aos IDS, foco deste trabalho, suas principais funções são: alarmar o administrador de rede ou do sistema em tempo real e disparar automaticamente mecanismos de segurança contra essa suspeita. As ferramentas de detecção de intrusos procuram por padrões de anormalidades nos fluxos de informação. Portanto, existem dois enfoques de detecção: por anomalia (*anomaly detection*) e por padrões de ataque (*misuse detection*). No primeiro caso, a ferramenta estabelece um padrão de normalidade e classifica como ataque ou intrusão qualquer atividade que se afaste significativamente desse padrão. No segundo caso, a ferramenta é alimentada com padrões que identificam atividades consideradas impróprias, gerando um alarme a cada vez que os padrões procurados sejam encontrados no fluxo de informação. A arquitetura clássica de um IDS é ilustrada na Figura 1.

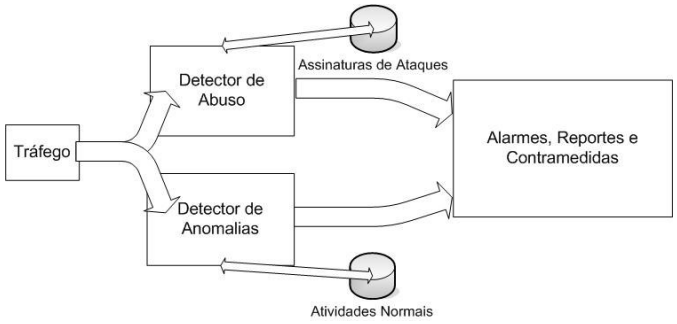

Figura 1. Arquitetura clássica de um IDS [Crothers 2002].

Porém, a criatividade dos atacantes, as constantes descobertas de vulnerabilidades nos protocolos e a divulgação de métodos de exploração pela Internet (*exploits*) incentivam a busca por soluções que sejam independentes de protocolos. Além disto, as soluções procuram evitar as constantes atualizações nas bases de assinaturas e/ou atividades normais. Outro problema é a existência dos ataques do dia "zero", que são aqueles tão novos que ainda são desconhecidos ou não existe uma "vacina" para tal.

2.3 Lógica Nebulosa

Os dois principais aspectos da imperfeição da informação são a imprecisão e a incerteza. Estas duas características estão intrinsecamente ligadas e opostas entre si: quanto mais se aumenta a incerteza mais se diminui a imprecisão e vice-versa. A teoria dos conjuntos nebulosos foi desenvolvida por Lotfi Zadeh a partir de 1965, para tratar do aspecto vago da informação [Zadeh 1965][Klir et al 1997]. Esta teoria, quando utilizada em um contexto lógico, como o de sistemas baseados em conhecimento, é conhecida como lógica "fuzzy", lógica nebulosa ou lógica difusa.

A lógica nebulosa é uma das tecnologias atuais mais bem sucedidas para o desenvolvimento de sistemas de controle complexos que podem ser implementados em

Máquinas de Inferência simples, de baixo custo e fácil manutenção. O uso de *Máquinas de Inferência Nebulosas* é especialmente conveniente quando o modelo matemático está sujeito a incertezas. Esta máquina é um sistema nebuloso com base em regras, formado por um grupo de condições do tipo Se <*premissa*> Então<*conclusão*>, que determinam as ações de controle em função das várias faixas de valores que as variáveis de estado do problema podem assumir. Estas faixas de valores são modeladas por conjuntos nebulosos que são nomeados através de rótulos.

Para descrever a medida de um fenômeno do mundo real, precisamos agrupar vários conjuntos nebulosos. Uma variável nebulosa é definida pela quádrupla: {*X, R, U, M*}, onde *X* é o nome simbólico da variável, *R* é o conjunto de rótulos, *U* é o Universo de Discurso e *M* são as regras semânticas que indicam o significado de cada rótulo em *R.* As bases do pensamento nebuloso são as regras que estabelecem relações entre diversas variáveis nebulosas e uma ou mais conjuntos nebulosos.

Em geral, um sistema nebuloso é composto por 3 componentes, conforme ilustrado na Figura 2.

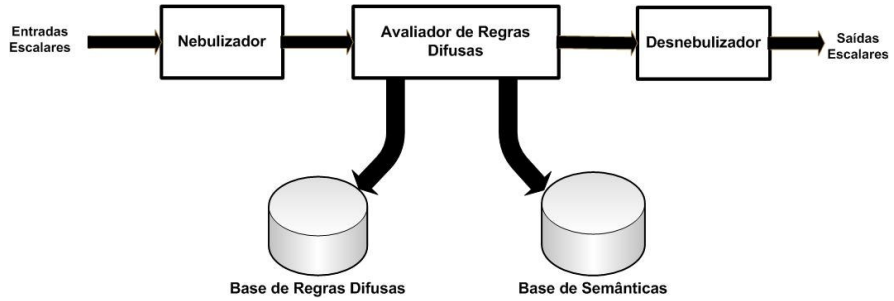

Figura 2. Diagrama de um sistema nebuloso.

O componente *nebulizador* recebe as entradas escalares ou *crisp* e as converte em variáveis nebulosas ou lingüísticas definidas pelos conjuntos nebulosos (Base de Semânticas). Após este passo, estas entradas convertidas são submetidas pelo Avaliador de Regras Difusas a um conjunto de regras (Base de Regras Difusas), obtendo-se as saídas nebulosas. Por fim, estas saídas sofrem um processo de *desnebulização*, onde são novamente transformadas em valores escalares.

3. Trabalhos Relacionados

A detecção de intrusos tem sido foco de inúmeras pesquisas. Em [Estevez et al 2004] foram apresentados IDS baseados em detecção de anomalias no tráfego observado. Em [Zamboni 2000], foi explorado o uso de agentes móveis para a concepção de sistemas de detecção de intruso do tipo distribuído. Em [Dickerson et al 2001], foi apresentada uma proposta de IDS nebuloso baseado em uma infra-estrutura de agentes móveis. Porém, esses três trabalhos continuam sendo IDS fundamentados em detecção de anomalia no tráfego.

Em [Gomez 2002] foi proposto um IDS que busca por padrões de ataques em uma massa de dados de *logs* de eventos, através de um algoritmo de classificação nebuloso. Tais trabalhos carecem de constantes atualizações em suas bases de dados de ataques conhecidos e/ou de bases de normalidade na rede, não sendo totalmente eficazes contra ataques do "dia zero" (ataques novos).

Recentemente, a proposta de [Hall et al 2004], diferentemente dos trabalhos tradicionais, apresenta como solução para o problema da detecção de intruso a possibilidade de identificação unívoca dos transceptores pela assinatura de transmissão (camada física), com um desempenho de 94%. Porém, tal trabalho não é integrado a outros sistemas de detecção de intrusos baseados em anomalia (*anomaly detection*) e em padrões de ataque (*misuse detection*). Adicionalmente, este trabalho também não é eficaz na detecção de atacantes que possuam dispositivos autorizados.

No presente trabalho, a arquitetura proposta busca integrar o trabalho apresentado por [Hall et al 2004] com processos de autenticação baseados em uma ***análise cinemática da mobilidade*** do dispositivo, com o intuito de aumentar ainda mais o desempenho de detecção de intrusos, inclusive para atacantes internos. Para tal, o protótipo proposto agrega à arquitetura clássica de um IDS tais funcionalidades, garantindo uma boa taxa de detecção em redes sem fio metropolitanas. Diferentemente dos trabalhos tradicionais, o EWIDS independe do tipo de ataque que está sendo executado, não impactando os requisitos de QoS e Mobilidade nas redes sem fio.

4. Descrição do EWIDS

No presente trabalho, são acrescentados à arquitetura clássica de um IDS novos componentes, conforme ilustrado na Figura 3. A integração desses novos elementos resulta na arquitetura estendida EWIDS

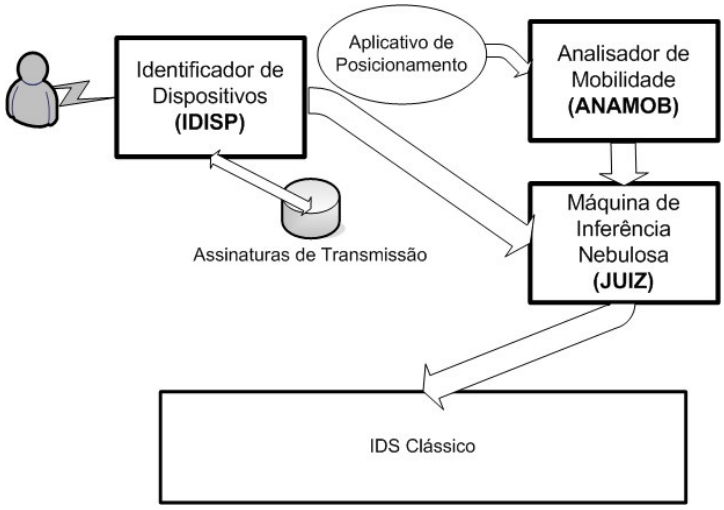

Figura 3. Arquitetura EWIDS proposta.

O EWIDS é capaz de detectar de forma ***integrada e híbrida*** as ocorrências anômalas quanto ao uso de dispositivos não autorizados (assinatura de transmissão) e quanto à localização incoerente de usuários (analise cinemática). É ***reativo***, pois, após a identificação de uma anomalia ou ataque, o sistema reage reportando tal ocorrência ao componente responsável por realizar as contramedidas na arquitetura clássica. É de ***monitoração contínua e de tempo real***, pois se propõe a identificar e informar o evento anômalo antes do ataque obter sucesso. Possível de ser usado como ***instrumento de auditoria e análise forense***, a partir do fato que pode armazenar e correlacionar os eventos em uma massa *logs*.

Os novos componentes da arquitetura EWIDS proposta são: Identificador de DISPositivos (IDISP), ANAlisador de MOBilidade (ANAMOB) e uma Máquina de Inferência Nebulosa (JUIZ), conforme ilustrado na Figura 3.

O primeiro componente – **IDISP** – é um autenticador baseado em assinatura de transmissão do dispositivo, proposto por [Hall et al 2004], que verifica a autenticidade do transceptor rádio utilizado na conexão sem fio. A autenticidade do transceptor rádio é baseada na assinatura de transmissão do equipamento. Esta é usada para identificar de forma única o dispositivo, através de uma análise comparativa com uma base de dados de assinaturas autorizadas. O componente IDISP é especialmente importante quando um atacante tenta se passar por um usuário legítimo, utilizando-se de um dispositivo não reconhecido pela rede. Para tal, um atacante pode inicialmente, por exemplo, realizar um "MAC *spoofing*" ou efetuar ataques mais elaborados [Schmoyer et al 2004] [Stallings 2002] como o *man-in-the-midle* ou *hijacking*. Este componente é um detector de intrusos que atua exclusivamente na camada física, criando uma separação (divisor de águas) entre os dispositivos autorizados e os intrusos.

O segundo componente – **ANAMOB** – é um analisador da mobilidade dos usuários em uma rede metropolitana, e é proposto nesse trabalho. Ele é baseado em uma análise cinemática do movimento dos mesmos. Em outras palavras, este componente é adequado para redes onde os usuários podem se mover dentro da cobertura de um determinado provedor de acesso sem fio metropolitano (Ex. Redes WiMax, 3G, WLAN estendidas). O princípio de funcionamento desse componente é baseado no fato de que cada usuário é único e não pode ser "clonado". Este princípio está fundamentado nas seguintes premissas: **(i)** um usuário somente ocupa um lugar no espaço; **(ii)** um usuário pode estar autenticado em um ou mais dispositivos móveis; **(iii)** os dispositivos móveis por "*default"*, devem estar próximos do usuário; **(iv)** a(s) posição(ões) do(s) dispositivo(s) determina(m) indiretamente a localização do usuário; **(v)** sendo pelo menos dois dispositivos autenticados, estes possuem posições próximas entre si; **(vi)** a posição de um dispositivo respeita a evolução cinemática do movimento do usuário; e **(vii)** as autenticações de dispositivos devem ocorrer em posições conhecidas do usuário ou dentro de uma área provável para a sua localização.

Quanto ao seu objetivo, o ANAMOB é responsável, em ambientes de mobilidade, por monitorar o posicionamento geográfico do usuário que acessa a rede através de um ou mais dispositivos móveis (*palm, notebook*, celular, etc.). Vale ressaltar que o monitoramento é de fato do(s) equipamento(s) que está(ão) sendo usado(s) pelo usuário e que, por conseguinte e indiretamente, determina a posição do mesmo (usuário). A informação de posição (fora do escopo deste trabalho) é dada em Latitude e Longitude, que pode ser obtida através de GPS ou algoritmos de triangulação [Gwon et al 2004][Hightower 2001]. Ressalta-se que para o emprego do GPS (dados com origem no dispositivo), requisitos de integridade deverão existir, a fim de impedir o forjamento de posições. Contudo, outros sistemas por triangulação podem ser usados, evitando esse problema. Assim, qualquer movimentação do usuário é monitorada através dos dispositivos em que estiver "autenticado" e os dados de movimento (posições históricas) são armazenados em uma base de dados. As posições históricas do percurso, em função do tempo, permitem calcular a velocidade do dispositivo e suas respectivas variações, através de cálculos cinemáticos. Essas posições dos usuários são analisadas segundo uma avaliação do movimento de cada dispositivo e são classificadas como posições esperadas ou não, dentro de um determinado grau de anormalidade. A última

posição conhecida do dispositivo, dentro do seu histórico, recebe a designação DATUM. A partir desta referência, diversos círculos de distância concêntricos são criados com centro em DATUM e raios variáveis, em função do tempo e velocidade estimada do usuário. Uma nova transmissão ou uma nova autenticação para este usuário, no caso de uma desconexão, somente será considerada normal caso a sua localização esteja contida no círculo de posição esperada/provável do mesmo e/ou esteja compatível com as posições dos outros dispositivos em uso pelo mesmo usuário.

O terceiro componente – **JUIZ** -, também proposto neste trabalho, é responsável por correlacionar os reportes oriundos dos outros dois, sendo, portanto, o elo de integração do EWIDS. Basicamente possui as tarefas de receber os dados originados em IDISP e ANAMOB, correlacioná-los e disparar alarmes associados a um Grau de Anormalidade (GA) que pode ser Normal, Baixo, Médio ou Alto. Conseqüentemente, este componente contribui com a possibilidade de uso em conjunto das duas abordagens (assinatura de transmissão e análise cinemática), melhorando a eficácia do IDS. A gradação de alarmes indica o grau de comprometimento da rede e podem gerar ações de contramedidas defensivas no componente específico da arquitetura clássica (fora do escopo deste trabalho). Em suma, como as entradas de JUIZ possuem abordagens distintas na determinação de anormalidades, a integração das informações fornecidas por tais componentes "purifica" a análise, aumentando a confiabilidade do sistema. Outra característica é a utilização de conceitos de inteligência computacional na implementação do componente através de uma máquina de inferência nebulosa.

Os componentes da arquitetura proposta devem ser inseridos nos elementos de concentração de tráfego da rede, para permitir a aquisição dos dados necessários ao sistema. Outro aspecto importante consiste em que os componentes principais do EWIDS devem ser processados em máquinas independentes dos concentradores de tráfego, não impactando o desempenho das tarefas principais dos elementos centrais (estação base) e, ao mesmo tempo, aumentando a performance do IDS.

5. Implementação

O ambiente de simulação escolhido foi o *MatLab* e as ferramentas relacionadas: *Simulink* e *Fuzzy Logic Toolbox*. Para o protótipo do EWIDS foram implementados: os componentes da arquitetura utilizando o *Simulink*; a máquina de inferência nebulosa como mecanismo de decisão do EWIDS e um *script MatLab*. A função principal do *script* é instanciar o gerador de cenários, o modelo *simulink*, a máquina de inferência nebulosa e gerar os relatórios estatísticos em função do número de rodadas.

A escolha do *MatLab* permitiu a integração, em um só ambiente, de todos os módulos implementados, inclusive a utilização do *FIS* (*Fuzzy Inference System) Editor* para a implementação da máquina nebulosa. Esta opção possibilitou a otimização da simulação do protótipo e viabilizou a realização de cálculos matriciais e vetoriais.

Os dois primeiros módulos implementados no *Simulink* foram: **Cenário** e **EWIDS**. O módulo **Cenário** trata cada transmissão de dados simulada, introduzindo um erro de precisão na posição reportada do dispositivo. Isto possibilita medir a acurácia do EWIDS, quanto às métricas escolhidas na fase de simulação, em uma situação mais próxima do mundo real.

O módulo **EWIDS** possui todos os três novos componentes que deram origem a arquitetura estendida proposta, que são: ***IDISP, ANAMOB e JUIZ***. Os dois primeiros

implementam as duas funcionalidades de verificação da autenticação: aquelas baseadas em assinatura de transmissão do transceptor do dispositivo e aquelas baseadas na análise cinemática da mobilidade do mesmo. O terceiro integra as informações geradas pelos anteriores e determina a avaliação final do EWIDS.

5.1 Componentes IDISP e ANAMOB

O primeiro componente ***IDISP*** é simulado e baseia-se no desempenho do algoritmo, medido em [Hall et al 2004], atribuindo-se um erro de 6% nas avaliações. Em outras palavras, o componente IDISP possui uma precisão de 94%.

O segundo componente ***ANAMOB*** foi todo implementado, possuindo, entre outros, três módulos principais: ***PMA*** (Perfil de Mobilidade Absoluto), ***PMR*** (Perfil de Mobilidade Relativo) e ***Avaliador***. Os demais módulos são auxiliares.

O módulo ***PMA*** é responsável por avaliar a última posição do dispositivo, dentro do histórico de movimento do mesmo. Esse histórico é definido pelos parâmetros da evolução cinemática do dispositivo. As posições discrepantes são reportadas como anormais e atribuída um valor GA_PMA (Grau de Anormalidade do PMA). Quanto maior for o GA_PMA, mais fora de uma posição esperada o dispositivo está. Ou seja, o GA_PMA é uma medida de quanto discrepante está a posição do dispositivo. Este módulo é composto por diversos sub-módulos. Dentre eles estão: "Calc_CDP", que é responsável pelo cálculo do círculo de distância provável (CDP) e "juízo_PMA", que realiza a avaliação dos parâmetros atuais do movimento do dispositivo, verificando se são anormais ou normais e atribuindo um valor ao GA_PMA. O "juízo_PMA" é composto pelos sub-módulos: "Promotor", "Defensor" e "Juiz_PMA". O primeiro compara a distância percorrida com o raio do CDP. O segundo verifica se as variações de velocidade e de precisão do posicionamento podem ser consideradas normais. Já o terceiro decide, se a posição é normal ou não, baseado nas entradas de "Promotor" e "Defensor", atribuindo-se um valor GA_PMA ao evento.

O módulo ***PMR*** é usado quando há mais de um dispositivo relacionado ao mesmo usuário. Ele é responsável por comparar as informações do movimento atual do dispositivo com as de seus dispositivos "irmãos", isto é, outros dispositivos do mesmo usuário. As distâncias relativas entre eles são calculadas a fim de se verificar o percentual de proximidade de um em relação ao outro. A distância aceitável é função de um raio de proximidade em torno do usuário acrescida da imprecisão máxima do sistema de posicionamento. Este módulo agrega confiabilidade ao mecanismo de decisão do ANAMOB (Avaliador). Em suma, não basta possuir coerência no movimento, mas deve-se respeitar a proximidade relativa entre os dispositivos "irmãos".

O módulo ***Avaliador*** correlaciona as duas análises, PMA e PMR, gerando uma decisão final do ANAMOB e um Grau de Anormalidade do componente.

5.2 Componente JUIZ

O componente ***JUIZ*** correlaciona às entradas de IDISP e ANAMOB, gerando entradas no Sistema de Inferência Nebuloso, chamado de "Juiz Nebuloso" do EWIDS.

O "Juiz Nebuloso" foi implementado no ambiente *MatLab*, utilizando-se o *FIS editor.* A primeira etapa na construção do "Juiz Nebuloso" compreende a definição das

variáveis nebulosas como também dos conjuntos nebulosos referentes a cada uma dessas variáveis consideradas. No presente trabalho, as definições tanto das variáveis como dos conjuntos nebulosos foram feitas a partir de um refinamento do próprio sistema, obtidas na fase de testes. Estes testes visaram um aperfeiçoamento das saídas quanto a sua correção e quantidades de falsos positivos. A máquina de inferência resultante do processo de refinamento possui um total de sete variáveis de entrada e duas de saída descritas, respectivamente, a seguir.

- ***V/F_IDISP***, indicando a análise da transmissão rádio recebida (verdadeira ou falsa);
- ***V/F_ANAMOB***, representando a análise cinemática recebida (verdadeira ou falsa);
- ***GA_ANAMOB***, representando o valor do Grau de Anormalidade (Normal, Baixo, Média e Alta) atribuído pelo componente ANAMOB;
- ***ind_alarmes_IDI***, sendo o índice de alarmes (Normal, Anormal e Mui-Anormal) que o dispositivo em avaliação gerou historicamente em IDISP;
- ***ind_alarmes_ANAM***, como o índice de alarmes (Normal, Anormal e Mui-Anormal) que o dispositivo também gerou historicamente em ANAMOB. É utilizado para se ter a medida da reincidência de alarmes em ANAMOB, que implicará em um aumento gradativo no GA;
- ***media_GA_ANAM***, sendo a média dos GA´s reportados por ANAMOB (Normal, Baixo, Média e Alta), considerada como uma outra medida da tendência dos reportes sucessivos, podendo atenuar ou agravar os alarmes;
- ***nr_transm***, indicando o total de transmissões realizadas pelo transceptor rádio do dispositivo (Baixo e Não-Baixo), que objetiva reduzir os falsos positivos causados por falsos alarmes no início das transmissões. Estes eventos, por ocorrerem na fase inicial (transiente estatístico), podem interferir nos índices calculados;
- **Julgamento,** indicando a avaliação final do EWIDS (Normal ou Anormal) que determina a geração de um alarme, em caso de julgamento anormal; e
- **Sentença,** indicando o Grau de Anormalidade (GA) (Normal, Baixa, Média e Alta) associado ao julgamento.

A forma gráfica dos conjuntos nebulosos (trapezoidal, triangular, etc.) representa a função de pertinência do conjunto, sendo o seu rótulo o indicativo da semântica a este associada. No presente trabalho, a construção da semântica dos conjuntos nebulosos foi efetuada a partir, como já mencionado, da fase de testes. Assim, cada conjunto nebuloso é representado graficamente por um trapézio ou triângulo cujos valores limites, à esquerda e à direita, coincidem com o último e com o primeiro valor dos conjuntos adjacentes respectivos, que possuem grau de inclusão 1. A Figura 4 ilustra a forma dos conjuntos nebulosos pertencentes às variáveis "ind_alarmes_IDI" e "Sentença".

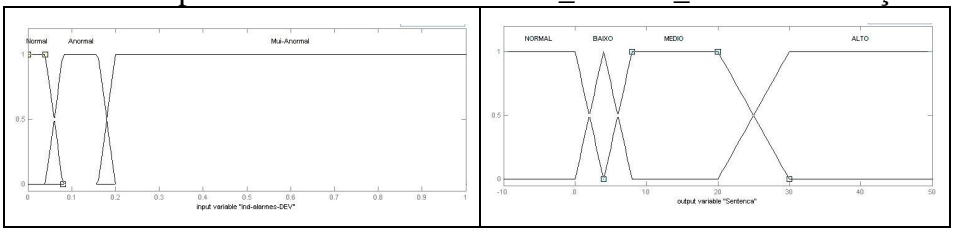

Figura 4. Variáveis Nebulosas "ind_alarmes_IDI" e "Sentença".

Assim, é garantido que cada conjunto nebuloso de uma mesma variável possui uma interseção com seu próximo conjunto, de tal forma que não haja qualquer valor pertencente ao seu Universo de Discurso que não esteja contido em, pelo menos, um de seus conjuntos nebulosos. Desta forma, foram definidas todas as variáveis nebulosas, com seus conjuntos e regras semânticas. Após a conclusão desta etapa, foram construídas as regras de inferência, que completam a construção do sistema nebuloso.

O método de construção das regras de inferência consiste em se determinar as regras de implicação que relacionam os conjuntos nebulosos das variáveis de entrada citadas, através do uso de operadores lógicos "e" (and) e "ou" (or), resultando como saídas a determinação de um alarme associado a um Grau de Anormalidade.

A combinação de todas as variáveis nebulosas, resultado do processo de *nebulização* das entradas, pode gerar até 1152 regras possíveis na base de regras difusas. Contudo, várias regras podem ser agrupadas de forma genérica através do uso do operando "none", quando não é necessário incluir determinada condição estabelecida em um rótulo, e "not", quando se pode agrupar vários rótulos adjacentes em uma mesma situação. Desta forma, o número de regras foi otimizado para um total de 110.

Os parâmetros selecionados para a *Máquina de Inferência Nebulosa, isto é, para o juiz_nebuloso,* foram: sistema tipo *mamdani* e métodos: (i) *And* - min; e (ii) *Or* - max; (iii) *Implication* - min e (iv) *Aggregation* - max. [Klir et al 1997]

O processo de *Desnebulização* escolhido foi o *mom* (média dos máximos), por apresentar os melhores resultados e uma coerência com o tipo de saída. Este método escolhe como saída escalar o valor médio de todas as possíveis saídas que possuam grau de inclusão um.

Finalizando o processo, a máquina de regras difusas determina quais regras serão ativadas pelos valores de entrada (variáveis nebulosas citadas) a fim de determinar quais conjuntos nebulosos de saída sofrerão o processo de "desnebulização". O exemplo a seguir ilustra uma regra da base:

If (VF-IDISP is Verdadeiro) and (VF-ANAMOB is Falso) and (GA-ANAMOB is Baixo) and (ind-alarmes-IDI is Normal) and (ind-alarmes-ANAM is Anormal) and (media-GA-ANAMOB is baixo) and (nr-transm is não-baixo) then (Sentenca is BAIXO)(Julgamento is ANORMAL).

Este processo é o responsável por determinar o resultado escalar de saída e, no mecanismo proposto, consiste em verificar se o evento analisado é normal ou anormal, associando-se um Grau de Anormalidade, para aquele conjunto de dados de entrada.

Logo, a saída do componente JUIZ é de fato a resposta do EWIDS ao evento de entrada na simulação. Tal saída, pode ser considerada Normal ou Anormal e, neste caso, atribuído um Grau de Anormalidade que pode ser Normal, Baixo, Médio ou Alto.

6. Simulações e Resultados

Com o intuito de validar o protótipo implementado, se fez necessário a criação de cenários apropriados para testar os componentes da arquitetura EWIDS, através de simulações. Todos os cenários usados neste trabalho são os de uma rede móvel metropolitana, como, por exemplo, a do padrão IEEE 802.16e (*full mobility*) [IEEE 2005] e com topologia PMP. O cenário é composto por diversas estações bases

distribuídas pela área de cobertura e um conjunto de estações móveis assinantes. Quanto ao cenário de simulação exemplificado, o padrão 802.16e – PMP representa uma rede metropolitana sem fio, onde há usuários internos ao provedor, pertencentes a instituições distintas, exemplificando a situação mais crítica de detecção. A topologia PMP permite que os sistemas de posicionamento sejam centralizados.

Inicialmente, foram realizados testes com o gerador de posicionamento de nós móveis sem fio do *Network Simulator* (NS): o *setdest.* Contudo, o mesmo não se mostrou totalmente adequado ao presente trabalho, pois (i) não engloba todos os parâmetros exigidos para o trabalho, como, por exemplo, a presença de atacantes e (ii) gera *waypoints* (pontos intermediários no percurso) muito distantes quando em cenários metropolitanos. Logo, se tornou necessário a criação de um gerador de cenários adequado para esse trabalho e que foi implementado em *MatLab Script*.

Os cenários gerados são compostos por dois atores: os usuários legítimos e os atacantes. Tais atores podem ser estáticos ou podem se movimentar segundo dois tipos de perfis de velocidade: a pé ou automotivo. Um ator do tipo usuário legítimo pode estar conectado à rede através de um ou mais dispositivos móveis. Esses usuários se movimentam no interior da rede sem fio metropolitana. Por outro lado, os atores do tipo atacante podem ser internos ou externos ao provedor de serviços, conforme já descrito.

Nos cenários gerados, cada atacante escolhe uma vítima diferente (um dispositivo pertencente a determinado usuário), segundo três ***padrões de distâncias*** definidas: Curta (1 a 100m), Média (500 a 1000m) ou Longa (1500 a 2500m). O momento do início do ataque é escolhido aleatoriamente. Em geral, o comportamento de um atacante real é o de não revelar a sua identidade quando executa um ataque. Portanto, o atacante procura se passar por outros usuários através da interceptação do sinal de transmissão do dispositivo legítimo e sua substituição pelo sinal do atacante.

Este tipo de ataque pode ser impedido se duas características importantes forem exploradas pelo IDS: a assinatura de transmissão do dispositivo e a posição do transmissor. É importante ressaltar que um aplicativo de posicionamento real possui erros de precisão, sendo estes considerados nas informações de entrada do EWIDS. Assim, no presente trabalho, foi inserido o erro de precisão do sistema GPS comercial comum que varia de 0 a 15 metros [Hightower 2001]. Outra observação é que o módulo identificador da assinatura de transmissão possui uma precisão de 94% na identificação dos dispositivos, de acordo com [Hall et al 2004]. Em suma, durante um ataque as posições do usuário legítimo são substituídas pelas posições dos atacantes na matriz de entrada do EWIDS. As intenções finais dos atacantes são indiferentes ao sistema.

O ***gerador de cenários*** implementado faz uso dos seguintes parâmetros de entrada: número de usuários, número de dispositivos relacionados a cada usuário, área geográfica do cenário (cobertura), número de atacantes, perfis de velocidade (a pé ou automotivo) e proximidade da vítima. Após a definição destes parâmetros, o algoritmo escolhe aleatoriamente as posições iniciais dos usuários e dos atacantes e gera o movimento dos mesmos dentro da área criada.

A saída do gerador é de fato o cenário a ser introduzido na simulação. Na prática, a saída é uma variável "cenário.mat", do tipo matriz Nx6, sendo "N" o número de eventos do cenário. As colunas desta matriz contêm as seguintes informações, respectivamente: Assinatura de Transmissão (0–Falso e 1–Verdadeiro), *timestamp*,

número do usuário/dispositivo, coordenadas cartesianas do dispositivo na rede (x,y) e gabarito para verificações estatísticas (0-transmissão legítima e 1-ataque).

Para o teste e validação do protótipo do EWIDS, foram criados oito tipos de cenários. Esse grupo de cenários possui as seguintes características: **(i)** área de cobertura metropolitana; **(ii)** proximidade das vítimas (CURTA e MÉDIA); **(iii)** Perfil de Velocidade (a pé – 1 a 3m/s ou automotivo urbano – 7 a 17m/s); **(iv)** tipo de atacantes (internos) e **(v)** número de dispositivos relacionados com cada usuário (1 ou 2).

Com o aumento da adoção de ferramentas de proteção de perímetro (*firewalls*), os ataques com origem interna passaram a crescer percentualmente em relação aos externos. Além disso, os ataques internos são potencialmente mais perigosos. Logo, foram escolhidos cenários com a presença desse tipo de atacante, ou seja, internos. Logo, nesses cenários, o componente IDISP, baseado em [Hall et al 2004], identifica como verdadeiras as assinaturas dos dispositivos atacantes em 94% das vezes. Este é o pior caso, cabendo ao componente JUIZ avaliar as anomalias pelos reportes de ANAMOB.

Foram executadas 50 rodadas de simulação para cada cenário com o intuito de obter intervalos de confiança aceitáveis, observando um limite de confiança de 95% e seguindo o mesmo número de iterações realizadas em [Hall et al 2004]. As métricas [Olson 1965] escolhidas foram: **(i) Percentual de Alarmes Corretos –** número de alarmes corretos sobre o total de transmissões atacantes; **(ii) Índice de Falsos Positivos –** totais de alarmes falsos sobre o total de alarmes e **(iii) – Percentual de Atacantes Descobertos –** número de atacantes descobertos sobre o total de atacantes no cenário. Considera-se um atacante descoberto quando pelo menos uma de suas transmissões foi alarmada pelo EWIDS. As Tabelas 1 e 2 trazem os resultados obtidos nas simulações para cada cenário.

Tabela 1 e 2. Resultados obtidos para atacantes internos – Perfis: a pé e automotivo.

	Perfil de Mobilidade a Pé			
Distância Atacante-Vítima	**Curta**		**Média**	
Dispositivos / Usuário	**1**	**2**	**1**	**2**
% Atacantes Descobertos (AD)	90	93,6	100	100
% Alarmes Corretos (AC)	80,8	88,2	100	100
% Falsos Negativos (FN)	19,2	11,8	0	0
% Falsos Positivos (FP)	0,5	1,5	0,3	0,3

	Perfil de Mobilidade Automotivo			
Distância Atacante-Vítima	**Curta**		**Média**	
Dispositivos / Usuários	**1**	**2**	**1**	**2**
% Atacantes Descobertos (AD)	70,9	82,2	100	100
% Alarmes Corretos (AC)	40,7	72,8	100	100
% Falsos Negativos (FN)	59,3	27,2	0	0
% Falsos Positivos (FP)	10	20,2	5,9	7,2

Para facilitar a análise dos resultados, a Figura 5 apresenta de forma gráfica os resultados obtidos nas simulações, com os seus respectivos intervalos de confiança. Em alguns pontos, esses intervalos, por serem pequenos, se confundem com a marca escolhida para a legenda. Na parte da Figura 5(a), o eixo "y" indica o percentual medido em cada métrica escolhida: AD – atacantes descobertos; AC – alarmes corretos e FN – falsos negativos. O eixo "x" indica, em ordem crescente de distância, os cenários-tipos que foram simulados. Na parte "b", foram plotadas duas curvas representativas dos falsos positivos nos cenários selecionados, sendo que uma (FP-15m) considera o erro do mecanismo de posicionamento do GPS de até 15m e a outra (FP-1m) de até 1m (Ex.aplicações militares). Comparando ambas, nota-se uma queda nos índices de Falsos Positivos quando o erro de posição é menor.

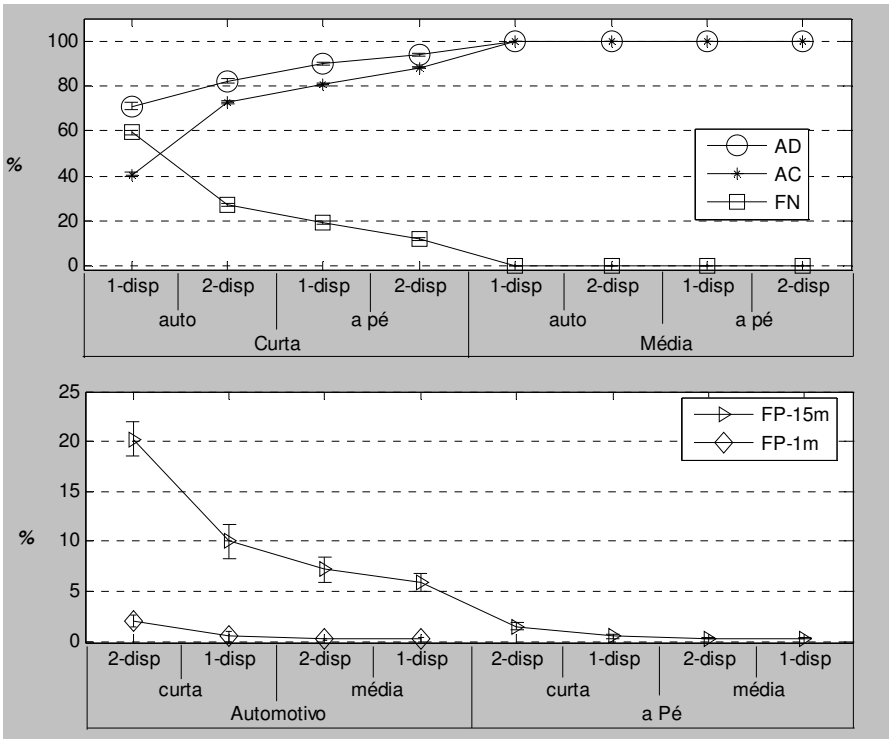

Figura 5. a) Resultados obtidos para Atacantes Descobertos (AD), Alarmes Corretos (AC) e Falsos Negativos (FN); b) Resultados obtidos para Falsos Positivos com erro de posicionamento de até 15m e até 1m.

Analisando os resultados, verifica-se um melhor desempenho do protótipo em distâncias médias entre o atacante e a vítima (Figura 5a), demonstrando que quanto maior for essa distância, mais fácil se torna para o EWIDS distinguir entre uma posição esperada ou não. Em distâncias curtas, algumas posições dos atacantes podem ser confundidas com as localizações dos usuários legítimos devido à suas proximidades.

Quanto aos Falsos Negativos, observa-se nos cenários com distâncias curtas que o perfil a pé possui um desempenho superior ao perfil automotivo, nas métricas medidas (Figura 5a), tanto para um ou dois dispositivos por usuário. Tal fato ocorre pois quanto maior a velocidade, maior é a área onde um dispositivo pode ser considerado legítimo.

No tocante aos Falsos Positivos (Figura 5b), constata-se, nos cenários cujo perfil é automotivo, principalmente com distâncias curtas e com dois dispositivos, um maior índice de Falsos Positivos em relação ao perfil a pé. As variações de velocidades no perfil automotivo, associadas ao erro do mecanismo de posicionamento, influenciam

estes valores. Na Figura 5(b), a curva com medições feitas com erro de posicionamento menor que 1 (FP-1m) revelam o grau de influência desse erro. A razão para o aumento dos Falsos Positivos em cenários que usam dois dispositivos por usuário é devida a adição da avaliação do módulo PMR (Perfil de Mobilidade Relativo), onde os acertos e erros deste componente passam a integrar a estatística.

7. Conclusões e Trabalhos futuros

Este trabalho apresentou uma proposta de extensão de uma arquitetura para Sistemas de Detecção de Intrusos cujo principal objetivo é o de aumentar a taxa de detecção de invasores em uma rede sem fio metropolitana, incorporando os processos de autenticação baseados em ***assinatura de transmissão rádio*** do dispositivo [Hall et al 2004], assim como os baseados em uma ***análise cinemática da mobilidade.*** Em topologias PMP, o EWIDS pode rodar próximos dos concentradores de tráfego, não competindo com o processamento normal e não interferindo nos requisitos de QoS e Mobilidade.

Quanto aos resultados de simulações em um cenário de rede sem fio metropolitana, estes foram promissores, comprovando a eficácia do algoritmo empregado no EWIDS. A análise dos resultados demonstra que a proposta de extensão impõe uma limitação de distância ao atacante, forçando o mesmo a estar mais próximo possível da vítima, caso pretenda atacar com alguma chance de sucesso. Ou seja, a liberdade de posicionamento fica restringida a uma área menor que 100 metros (no pior caso – atacante interno) ao redor da vítima, em uma escala metropolitana de vários Km^2. Portanto, o EWIDS contribui com a minimização do impacto de uma das principais vulnerabilidades inerentes ao meio sem fio: a utilização maliciosa do sinal rádio interceptado em uma distância conveniente para o atacante.

Quanto aos trabalhos futuros, serão investigadas soluções para aperfeiçoar o protótipo nos cenários onde a distância atacante-vítima é curta e para reduzir o índice de Falsos Positivos nos perfis automotivos, de forma independente da precisão dos mecanismos de posicionamento. Outro trabalho futuro que visa investigar a robustez do EWIDS, em um cenário real, está relacionado à criação de novos cenários que vislumbrem a inclusão de um percentual de impossibilidades momentâneas de localização e/ou de dispositivos que opere em modo ocioso (*idle*).

Outra linha de pesquisa é adequar a proposta desse trabalho para redes com topologia *mesh.* Neste caso, a proposta deve ser distribuída e a referência no controle de nós invasores passa a ser a vizinhança de cada nó.

Referências

Boom, Derrick D. (2004), "Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks" **-** Master Thesis - Naval Postgraduate School. California.

Crothers, Tim (2002)**, "**Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network**".** Ed. Wiley.

Dickerson, J.E., J. Juslin, O. Koukousoula, J.A. Dickerson (2001), "Fuzzy intrusion detection", IFSA World Congress and 20th North American Fuzzy Information Processing Society (NAFIPS) International Conference, Vancouver, *British Columbia*, Volume 3, p. 1506-1510.

Estevez, Juan M., Pedro Garcıa-Teodoro, Jesus E. Dıaz-Verdejo (2004), "Measuring normality in HTTP traffic for anomaly-based intrusion detection". *Computer Networks* 45, p. 175–193.

Gomez, Jonatan and Dipankar Dasgupta (2002), "Evolving fuzzy Classifiers for Intrusion Detection"**,** *Proceedings of the IEEE Workshop on Information Assurance United States Military Academy*, West Point, NY.

Gwon, Youngjune, Ravi Jain and Toshiro Kawahara (2004), **"**Robust Indoor Location Estimation of Stationary and Mobile Users"**.** IEEE INFOCOM.

Hall, Jeyanthi, Michel Barbeau and Evangelos Kranakis (2004), "Enhancing Intrusion Detection In Wireless Networks Using Radio Frequency Fingerprinting"**.** *Proceeding (433) Communications, Internet, and Information Technology*.

Hightower, Jeffrey and Gaetano Borriello (2001), "Location Systems for Ubiquitous Computing"**,** *IEEE Computer*, p. 57-66**.**

IEEE Draft 802.16e-D9 (2005), "Air Interface for Fixed and Mobile Broadband Wireless Access Systems".

IEEE Std. 802.16 (2004), "Air Interface for Fixed Broadband Wireless Access Systems".

Johnston, David and Jesse Walker (2004), "Overview of IEEE 802.16 security", *IEEE Security & Privacy, IEEE Computer Society*.

Klir. G.J., U. St.Clair, and B.Yuan (1997), "Fuzzy Set Theory: Foundations and Applications", Prentice Hall.

Olson, Roger H. (1965), "On the use of Bayes' Theorem in estimating False Alarm Rates". *Monthly Weather Review* 93, p. 557-558

Schmoyer, Timothy R. et al (2004), "Wireless Intrusion Detection and Response. A case study using the classic man-in-the-middle attack". WCNC.

Stallings, William (2002), "Network Security Essentials". Ed. Prentice Hall.

Zadeh L. (1965), "Fuzzy Sets", *Information and Control*, vol. 8, p. 338–353.

Zamboni, Diego, Eugene H. Spafford (2000), "Intrusion detection using autonomous agents". *Computer Networks* 34, p. 547±570.

Zhang, Yongguang, Wenke Lee and Yi-an Huang (2003), "Intrusion Detection Techniques for Mobile Wireless Networks". *Wireless Networks* 9, p. 545–556.