Instituto de Matemática / Núcleo de Computação Eletrônica
Universidade Federal do Rio de Janeiro

Nilson Rocha Vianna

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

Rio de Janeiro
2006

NILSON ROCHA VIANNA

EWIDS: UMA EXTENSÃO PARA ARQUITETURAS DE SISTEMAS DE DETECÇÃO DE INTRUSOS PARA REDES SEM FIO METROPOLITANAS

IM/NCE-UFRJ

Nilson Rocha Vianna

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

Dissertação submetida ao corpo docente do Núcleo de Computação Eletrônica / Instituto de Matemática da Universidade Federal do Rio de Janeiro – UFRJ, como parte dos requisitos necessários à obtenção do grau de Mestre em Ciências em Informática.

Rio de Janeiro

2006

FICHA CATALOGRÁFICA

VIANNA, NILSON ROCHA

EWIDS: Uma Extensão para Arquiteturas de Sistemas de Detecção de Intrusos para Redes Sem Fio Metropolitanas, [Rio de Janeiro], 2006.

XII, 89 p., 29,7 cm (IM/NCE/UFRJ), MSc., Informática, 2006)

Dissertação (Mestrado) – Universidade Federal do Rio de Janeiro, IM/NCE

1. Redes Sem Fio Metropolitanas 2. Segurança em Redes

3. Sistemas de Detecção de Intrusos 4. Lógica Nebulosa

NILSON ROCHA VIANNA

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

Dissertação submetida ao corpo docente do Núcleo de Computação Eletrônica / Instituto de Matemática da Universidade Federal do Rio de Janeiro – UFRJ, como parte dos requisitos necessários à obtenção do grau de Mestre em Ciências em Informática.

Aprovada em

_____

Prof[a]. Luci Pirmez - Orientador
D.Sc., COPPE/UFRJ, Brasil

_____

Prof[o]. Julius César Barreto Leite
Ph.D. UMIST , Inglaterra

_____

Prof[o] Adriano Joaquim de Oliveira Cruz
Ph.D, Southampton University, Inglaterra

_____

Prof[a]. Flávia Coimbra Delicato
D.Sc., COPPE/UFRJ, Brasil

DEDICATÓRIAS

À Deus, autor da vida, da minha fé e Amigo sempre presente.

"Ele é o que está assentado sobre a redondeza da terra, cujos moradores são como gafanhotos; é ele quem estende os céus como cortina e os desenrola como tenda para neles habitar"

Isaías 40:22

"... não temas, porque eu sou contigo; não te assombres, porque eu sou o teu Deus; eu te fortaleço, e te ajudo, e te sustento com a minha destra fiel."

Isaías 41:10

À minha esposa Jamyle, mulher virtuosa, guerreira, companheira....

Ao meu filho Isaac, um presente muito especial que recebi durante essa jornada.

Ao meu pai pelos bons conselhos de professor.

À minha mãe pelo apoio incondicional e amor.

À minha irmã pelo seu carinho especial.

AGRADECIMENTOS

À Deus pela minha vida, saúde e pela direção correta que me fez caminhar.

À minha esposa Jamyle por todo o incentivo, apoio e pela compreensão durante esses dois anos de dedicação intensa a atividade acadêmica. Ao meu filho Isaac pela alegria que me deu no seu nascimento e de ver o seu sorriso a cada dia. Aos meus pais Nilson e Geovanina e a minha irmã Márcia, por todo apoio dispensado durante o meu curso.

Aos amigos do mestrado Anderson, Cássio, Luciana, Mostardinha, Nelson, Fred, Gustavo, Daniela e Erica pelo companheirismo e amizade dispensadas a mim ao longo desses dois anos. Aos também amigos do Laboratório de Redes e Multimídia Edson, André e em especial ao Alexandre por toda a ajuda técnica fornecida no nosso dia a dia.

Ao grande amigo Reinaldo, companheiro do dia a dia, pessoa de caráter, amigo valoroso, obrigado por tudo que fez em prol do meu trabalho, em especial a revisão da minha dissertação o que contribuiu decisivamente para a qualidade do trabalho final.

Aos professores Paulo Aguiar, Adriano, Osvaldo Vernet e Rust pela disponibilidade em sempre atender as solicitações de um mestrando com dúvidas.

Em especial, à Profª Luci Pirmez, pessoa de grande coração, obrigado pela orientação segura que sempre suas palavras me transmitiram, pelo acompanhamento zeloso de todo o trabalho e pela amizade desenvolvida ao longo do curso. Agradeço à Deus pela oportunidade que me deu de ser orientado por ti, pois, sem dúvida, o sucesso obtido jamais teria sido o mesmo sem a sua participação.

Ao apoio recebido dos Comandantes Márcio Moreira da Silva e Valter Monteiro Júnior (Diretoria de Telecomunicações da Marinha) durante o período que estive afastado de minhas funções.

À Marinha do Brasil, pela oportunidade concedida de aprimorar os meus conhecimentos e pela visão estratégica que possui no aperfeiçoamento de seu pessoal.

RESUMO

VIANNA, Nilson Rocha. EWIDS: Uma Extensão para Arquiteturas de Sistemas de Detecção de Intrusos para Redes Sem Fio Metropolitanas**.** Rio de Janeiro, 2006. Dissertação (Mestrado em Informática) - Instituto de Matemática/Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006

A evolução tecnológica vivenciada pela humanidade trouxe consigo soluções para diversos problemas em todas as áreas do conhecimento. Todavia, juntamente com as novas soluções surgem, intrinsecamente, novos problemas a serem resolvidos. No contexto das tecnologias de redes de computadores, o crescente uso de redes sem fio propicia a exploração de vulnerabilidades inerentes ao meio de difusão e incentivam a inclusão de requisitos de segurança mais robustos nos padrões. Contudo, muitas dessas soluções, especialmente as fundamentadas em robustez criptográfica, não atendem as necessidades de equipamentos legados e de dispositivos móveis de baixo poder computacional. Além disso, as propostas de IDS (*Intrusion Detection System*) encontradas na literatura dependem de constantes atualizações em bases de assinaturas e/ou atividades normais nas redes. Este trabalho apresenta uma proposta de extensão para arquiteturas de IDS em redes sem fio metropolitanas, denominada EWIDS (*Extended Wireless Intrusion Detection System*). O EWIDS incorpora, através de uma Máquina de Inferência Nebulosa, os processos de detecção baseados em assinatura de transmissão rádio e em uma análise cinemática da mobilidade dos dispositivos. Uma bateria de testes realizada no protótipo implementado apresentou resultados promissores na detecção de intrusos, que validam a utilização da arquitetura para cenários de redes sem fio metropolitanas.

ABSTRACT

VIANNA, Nilson Rocha. EWIDS: Uma Extensão para Arquiteturas de Sistemas de Detecção de Intrusos para Redes Sem Fio Metropolitanas**.** Rio de Janeiro, 2006. Dissertação (Mestrado em Informática) - Instituto de Matemática/Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006

The technological evolution lived deeply by the humanity brought itself solutions for diverse problems in all the knowledge areas. However, with the new solutions, appear intrinsically, new problems to be solved. In the context of computer networks technologies, the increasing use of wireless networks propitiates the exploration of inherent vulnerabilities in the diffusion media and stimulates the inclusion of more robust security requirements in the standards. However many of these solutions, especially based on cryptographic strength, do not satisfy the needs of legacies equipment and mobile devices with low computational resources. Moreover, the IDS proposals found in literature depend on constant updates in bases of signatures and/or normal activities in their databases. This work presents a proposal of an extension for architectures of IDS (Intrusion Detection System) in metropolitans wireless network, called EWIDS (Extended Wireless Intrusion Detection System). The EWIDS incorporates, through a Fuzzy Inference Machine, the detections processes based on a radio transmitter fingerprinting and by a device mobility kinematics analysis. A battery of tests, carried through in the implemented archetype, presented promising results for intruders detection that validate the use of the architecture for scenes of metropolitans wireless network.

Lista de Abreviaturas e Siglas

AC – Alarmes Corretos
AD – Atacantes Descobertos
AD-AC – Atacantes Descobertos e Alarmes Corretos
ADC – *Analogic Digital Converter*
AES – *Advanced Encryption Standard*
ANAMOB – Analisador de Mobilidade
APRS - *Automatic Position Reporting System*
AS – Associação Segura
ATM - *Asynchronous Transfer Mode*
BPI - *Baseline Privacy Interface*
BS – *Base Station*
BWA - *Broadband Wireless Access*
CBC - *Cipher Block Chaining*
CDPE – Círculo de Distância Padrão/Esperado
CER – *Crossover Error Rate*
CMAC - *Cipher-based MAC*
CPU – *Central Processing Unit*
CRC – *Cyclic Redundancy Check*
DES - *Data Encryption Standard*
DGPS - *Differential Global Position System*
DNS – *Domain Name Service*
DOCSIS - *Data Over Cable Service Interface Specification*
DSL - *Digital Subscriber Line*
EAP - *Extensible Authentication Protocol*
EWIDS – Extended Wireless Intrusion Detection System
FIS – *Fuzzy Inference System*
FN – Falsos Negativos
FP – Falsos Positivos
GA – Grau de Anormalidade
GA-AC – Grau de Anormalidade dos Acertos

Lista de Abreviaturas e Siglas (Continuação)

GE – Guerra Eletrônica
GPS – *Global Position System*
GSM - *Global System for Mobile Communications*
GUI – *Graphical User Interface*
HIDS – *Host Intrusion Detection System*
HMAC – *Keyed-Hash Message Authentication Code*
HTTP – *Hipper Text Transfer Protocol*
IDISP – Identificador de Dispositivos
IDS – Intrusion Detection System
IEEE - *Institute of Electrical and Electronics Engineers*
IP – *Internet Protocol*
MAC - *message authentication code*
MatLab - *MATrix LABoratory*
MiTM – *Man-in-The-Middle*
MS – *Mobile Station*
MSG - Mensagem
NIDS - *Network Intrusion Detection System*
PDU – *Packet Data Unit*
PKM - *Privacy Key Management*
PMA – Perfil de Mobilidade de Absoluto
PMP – *Point Multi Point*
PMR – Perfil de Mobilidade Relativo
QoS – *Quality of Service*
RFC – *Request For Comments*
RFID - *Radio Frequency Identification*
RIA – Raio de Inclusão Aceitável
SS – *Subscriver Station*
SSH – *Secure Shell*
TEK – *Traffic Encryption Key*
TLV – *Type-Length-Value*

Lista de Abreviaturas e Siglas (Continuação)

UMP - *User Mobility Profile*
WIDS – *Wireless Intrusion Detection System*
WLAN – *Wireless Local Area Network*
WMAN - *Wireless Metropolitan Area Network*
WPAN - *Wireless Personal Area Network*

Índice de Figuras

SUMÁRIO

Capítulo 1 - Introdução

A evolução tecnológica vivenciada pela humanidade no último século e principalmente nas últimas décadas, vem possibilitando a descoberta de soluções para diversas áreas do conhecimento. Porém, na mesma medida, surgem novos problemas inerentes às próprias soluções concebidas por, por exemplo, pressões do mercado e lucros financeiros. Como conseqüência, as soluções apresentadas ao longo do tempo carecem muitas das vezes de um amadurecimento, normalmente obtido através de pesquisas. Assim sendo, no contexto das tecnologias de redes de computadores, muitas soluções hoje implementadas são carentes de características essenciais que permitam o seu correto uso. Mesmo assim, observa-se um crescente uso de redes sem fio em empresas, escritórios e residências.

Isso é explicado pois as necessidades de Mobilidade e Qualidade de Serviço (QoS), aliadas ao baixo custo de instalação e às facilidades de configuração, tornam as redes sem fio cada vez mais populares. Apesar dessas vantagens, existem desafios intrínsecos a este tipo de ambiente que propiciam um vasto campo para pesquisa. A tarefa de prover segurança a essas redes é um exemplo de um grande desafio, especialmente quando trata-se de redes sem fio de alcance metropolitano.

Na tentativa de solucionar vários desses problemas para as redes sem fio, novos padrões surgem de forma a atender aos requisitos de Segurança, Qualidade de Serviço (QoS) e Mobilidade das novas aplicações. No entanto, tais requisitos devem ser agrupados e tratados de uma forma única, pois possuem uma relação de dependência mútua. Ou seja, alterações nos requisitos de Segurança interferem diretamente na Mobilidade e QoS ou vice-versa.

O requisito Mobilidade é um dos pilares fundamentais da computação ubíqua e, portanto, está presente nos mais novos padrões IEEE referentes a redes sem fio [1, 2]. A mobilidade ao ser atendida não deve comprometer a segurança e as necessidades de QoS exigidas pelas aplicações e usuários. No que tange à QoS, as aplicações multimídia necessitam de maiores larguras de banda, de menores retardos e suas variações, assim como a sincronização entre as diferentes mídias. Logo, a introdução do requisito segurança, fundamental em várias aplicações, deve também observar as limitações impostas para a exeqüibilidade da mobilidade e QoS necessários. Essa relação é agravada em face da utilização de dispositivos móveis de baixo poder computacional, como PDAs e celulares, tornando ainda mais complexa a tarefa de conceber mecanismos de

segurança, pois além das limitações de processamento e memória, há o problema do consumo de energia de baterias, fundamental para o uso eficiente de tais dispositivos.

Outro aspecto desafiador para prover segurança nas redes sem fio metropolitanas está no fato de que essas redes permitem uma maior liberdade de posicionamento para um atacante, pois possuem uma maior área de cobertura.

1.1 Motivações

A motivação do presente trabalho está diretamente relacionada à proposição de uma solução de segurança para redes móveis sem fio metropolitanas que venha a contribuir com a minimização dos seguintes problemas: **(i)** vulnerabilidades do meio sem fio; **(ii)** vulnerabilidades dos padrões e protocolos para redes sem fio; **(iii)** vulnerabilidades oriundas das políticas de suporte ao uso de equipamentos legados; **(iv)** robustez criptográfica *versus* desempenho dos dispositivos móveis de baixo poder computacional e **(v)** uma nova definição de usuário interno no contexto das redes sem fio metropolitanas.

No tocante às **vulnerabilidades do meio sem fio**, um dos obstáculos para a implementação de serviços de segurança é o meio de transmissão ser por difusão. As interferências na transmissão via rádio, a atenuação do sinal em relação à distância e presença de obstáculos naturalmente 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 [3]. Ressalta-se que a implantação de mecanismos de segurança 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 [4].

Em relação às **vulnerabilidades dos padrões e protocolos para redes sem fio,** os principais problemas estão relacionados à carência de definições que atendam as reais exigências de segurança [5]. A velocidade do surgimento de padrões de redes sem fio, como os do IEEE 802.11 (Redes Locais Sem Fio) e IEEE 802.16 (Redes Metropolitanas Sem Fio) [6, 7], que atenda as novas tendências tecnológicas e, ao mesmo tempo, as exigências das novas aplicações resulta em “brechas” de segurança nesses padrões, que podem ser explorados de forma maliciosa.

Quanto às **vulnerabilidades oriundas das políticas de suporte ao uso de equipamentos legados,** os principais problemas surgem devido a coexistência do parque de equipamentos legados com os equipamentos que são compatíveis com os novos padrões. Para permitir a coexistência desses equipamentos, o padrão IEEE 802.11i, por exemplo, inclui a flexibilidade de conectividade com dispositivos legados. Entretanto, esse mesmo padrão informa que, ao permitir a coexistência, toda a infra-estrutura de segurança no meio sem fio poderá ser comprometida [5]. Por essa razão, torna-se fundamental adicionar mais segurança através de mecanismos adicionais.

O problema da **Robustez criptográfica *versus* desempenho dos dispositivos móveis de baixo poder computacional** está ligado aos aspectos de QoS, Mobilidade e Consumo de Energia das baterias. Geralmente as soluções de segurança propostas nos padrões fundamentam-se na robustez criptográfica. Sabe-se que quanto maior a robustez criptográfica, maior é a sobrecarga computacional gerada. Assim, tal robustez criptográfica inviabiliza, em muitos casos, a utilização de dispositivos móveis de baixo poder computacional [8], pois esses dispositivos possuem baixo poder de processamento, pouca memória e baterias limitadas. Um exemplo seria a limitação do emprego de criptografias robustas em redes celulares GSM [9]. Em suma, prover segurança é fundamental desde que não comprometa os requisitos de QoS, Mobilidade e Consumo de Energia. Portanto, uma das motivações deste trabalho é a de conceber um mecanismo de segurança que contribua com o aumento da segurança nas redes sem fio, sem impactar os requisitos de QoS, Mobilidade e Consumo de Energia dos nós da rede.

Quanto a **uma nova definição de usuário interno no contexto das redes sem fio metropolitanas,** essa definição se faz necessária já que os maiores riscos de segurança em redes corporativas passaram a ser os ocasionados de dentro das próprias instituições, ou seja, de onde os níveis de confiança dos usuários são obviamente maiores. Portanto, os esforços atuais para reforçar os níveis de segurança de redes corporativas devem ter seu foco principal nas ameaças internas, através da implantação de políticas de segurança adequadas ao negócio e a implementação de sistemas de detecção de intrusos (IDS), a fim de se contribuir com o princípio da proteção em camadas, consagrado na literatura [10]. 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 usuários (clientes) 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. Essa descrição torna o componente segurança muito mais desafiador, principalmente quando existe a possibilidade de instituições concorrentes estarem compartilhando o mesmo domínio sem fio metropolitano.

Para adicionar segurança aos protocolos, diversas soluções clássicas de segurança [10] são adaptadas ao meio sem fio tais como *Firewalls* e IDS (*Intrusion Detection System*) [11]. Porém, o procedimento de adaptação não é suficiente para conter um "mau uso" dessas redes, pois o meio sem fio introduz uma diversidade de novas vulnerabilidades. Na taxonomia de um IDS surgem os WIDS (*Wireless Intrusion Detection System*) [11, 12], que incrementam os níveis de segurança nas redes sem fio, em face das vulnerabilidades existentes nos padrões. Especialmente relativo às redes sem fio, ataques [4] como Personificação (*MAC spoofing*), Homem-no-Meio (*Man-in-the-middle - MiTM*) e Roubo de Sessão (*Session Hijack*) são muito comuns e proporcionam ao atacante a possibilidade de obter informações privadas de outros usuários ou de realizar atividades maliciosas usando a identidade de terceiros, de uma posição confortável para o atacante. Essa liberdade de posicionamento é uma das principais características do universo sem fio. Para tal, existem ferramentas auxiliares que podem ser classificadas conforme seu objetivo [10], dentre elas estão os IDS. 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 disso, as soluções para IDS procuram evitar as constantes atualizações nas bases de assinaturas e/ou atividades normais, dependendo da abordagem de detecção. 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. Logo, a tecnologia de detecção de intrusos é imatura e dinâmica, necessitando de constantes evoluções em suas abordagens.

1.2 Objetivos

A fim de incrementar os níveis de segurança nas redes móveis sem fio metropolitanas, o presente trabalho apresenta uma proposta de extensão da arquitetura clássica de um IDS [10] que visa minimizar o efeito das vulnerabilidades inerentes ao meio sem fio, aos padrões e protocolos para redes sem fio e às políticas de suporte ao uso de equipamentos legados. Adicionalmente, a proposta também procura diminuir o impacto nos requisitos de QoS, Mobilidade e Consumo de Energia, especialmente dos dispositivos móveis de baixo poder computacional [8]. Além disso, a proposta busca contribuir com o aumento da detecção de usuários maliciosos que se escondem atrás do privilégio de pertencer a determinado domínio lógico administrativo de um provedor de serviços de rede sem fio metropolitana (atacante interno).

Para tal, a arquitetura proposta [13] atua de forma independente dos mecanismos de segurança empregados nos padrões e protocolos, inclusive de algoritmos de criptografia, caracterizando sua generalidade. Além disso, a arquitetura objetiva utilizar mecanismos que explorem as próprias características das redes sem fio (meio de transmissão e mobilidade), através de um sistema de detecção de intrusos que ofereça baixa carga computacional aos nós da rede, devido ao problema da limitação de recursos dos dispositivos móveis. Com isso, a arquitetura incorpora em um único sistema os processos de detecção baseados em **assinatura de transmissão rádio** do dispositivo [14], assim como os baseados em uma **análise cinemática da mobilidade** [13] do mesmo, implementados neste trabalho, integrando-os através de uma **Máquina de Inferência Nebulosa** [13]. Além dos objetivos já citados, o presente trabalho apresenta as seguintes contribuições: **(i)** a possibilidade de detecção de intrusos independentemente de atualizações em bases de assinaturas de ataques e/ou anomalias, tornando a abordagem mais escalável, característica importante em um ambiente que potencialmente pode possuir um grande número de usuários; **(ii)** a possibilidade de detecção de ataques do “dia zero” (ataques sem assinatura conhecida); **(iii)** a não interferência nos requisitos de QoS, Mobilidade e Consumo de Energia, fundamentais nos cenários aplicados, pois a arquitetura não utiliza o processamento dos nós monitorados; **(iv)** redução de falsos positivos e negativos, através da integração de informações de naturezas distintas (assinatura de transmissão e mobilidade de dispositivos e usuários) empregando técnicas de lógica nebulosa com o objetivo de tornar mais eficiente o mecanismo de decisão; **(v)** minimização do tamanho da informação armazenada em tempo real por usuário, no controle de sua mobilidade, permitindo também uma melhor

escalabilidade e dinamismo em seu perfil de mobilidade e **(vi)** imposição de uma limitação na liberdade de posicionamento dos atacantes, normalmente oferecida pelas redes sem fio, restituindo as redes sem fio uma característica das redes cabeadas.

Para a validação da proposta, cenários de uma rede sem fio metropolitana foram gerados e as simulações demonstraram a eficácia do protótipo implementado quanto às medições estatísticas das diversas métricas de desempenho escolhidas.

O restante deste trabalho está estruturado em seis capítulos. No Capítulo 2 são apresentados os conceitos básicos relacionados à fundamentação da proposta e os trabalhos relacionados. No Capítulo 3, é apresentada uma descrição da arquitetura EWIDS (*Extended Wireless Intrusion Detection System)* proposta. No Capítulo 4, é descrita a implementação do protótipo. No Capítulo 5 são apresentados os resultados das simulações realizadas e suas respectivas análises. O trabalho é finalizado no Capítulo 6 com a apresentação das conclusões e os possíveis trabalhos futuros.

Capítulo 2 - Conceitos Básicos

Este capítulo apresenta os conceitos básicos que fundamentam a Arquitetura **EWIDS** proposta e o desenvolvimento do protótipo para execução dos testes de simulação.

A organização deste capítulo segue uma lógica que parte do tipo de rede sobre a qual a arquitetura de IDS proposta pode ser aplicada, passando pelos princípios teóricos em que se baseiam os componentes da Arquitetura EWIDS até terminar nos trabalhos relacionados. Assim, a Seção 2.1, após introduzir os conceitos gerais sobre Redes sem fio Metropolitanas, descreve sucintamente os objetivos e as principais características do padrão IEEE 802.16, exemplificando, dessa forma, um dos cenários de aplicação da presente proposta. A Seção 2.2 resume os principais conceitos sobre os mecanismos de posicionamento geográfico e os principais sistemas propostos na literatura, pois a EWIDS depende do conhecimento da posição geográfica dos dispositivos. A Seção 2.3 apresenta os conceitos básicos de segurança, especialmente, em redes sem fio, enfatizando os principais mecanismos instituídos pelo padrão IEEE 802.16 assim como os adendos introduzidos no Padrão IEEE 802.16e, além de salientar as vulnerabilidades ainda remanescentes. Estendendo os conceitos de segurança da seção anterior, a Seção 2.4 conceitua os Sistemas de Detecção de Intrusos (*Intrusion Detection Systems-IDS*) além de classificá-los, apresentando as principais abordagens nas suas implementações. Na Seção 2.5 são descritos os conceitos fundamentais sobre Lógica Nebulosa, abordagem escolhida na concepção do componente responsável pelas tomadas de decisões na Arquitetura EWIDS. A Seção 2.6 apresenta os trabalhos relacionados, detalhando as principais arquiteturas de IDS publicadas na literatura acadêmica. A Seção 2.7 descreve o funcionamento de um identificador de dispositivos por assinatura de transmissão, que é essencialmente o componente IDISP da Arquitetura EWIDS, descrita no Capítulo 3. Por fim, a Seção 2.8 finaliza este capítulo, tecendo algumas considerações finais.

2.1 - Redes Sem Fio Metropolitanas

As redes sem fio são sistemas de transmissão de dados que possui, na flexibilidade e no baixo custo de instalação, uma alternativa para redes cabeadas. Outra vantagem intrínseca ao meio sem fio é a possibilidade de mobilidade, utilizando-se equipamentos portáteis. A

padronização dessas redes se deu inicialmente com os padrões IEEE 802.11 [7], para redes locais (WLAN), e Bluetooth IEEE 802.15 [15], para redes pessoais (WPAN).

2.1.1 - Aspectos Gerais

Com o crescimento acelerado das redes sem fio, logo se viu a necessidade de sua utilização para alcances metropolitanos. Isto porque, apesar do acesso em banda larga já estar disponível há um bom tempo, este é ainda limitado. As Conexões DSL ou Cabo-TV são limitadas porque ou os clientes estão fora da área onde os serviços são oferecidos ou não fazem parte de uma infra-estrutura residencial a cabo ou acham que a conexão é muito cara. Por causa da sua natureza sem fio, o serviço de acesso torna-se mais pervasivo, isto é, a sua distribuição é mais rápida, o seu escalonamento é mais fácil e mais flexível, podendo atender aos clientes fora da faixa de serviços cabeados ou aos que não estão satisfeitos com as alternativas de banda larga com fio. Contudo, o vetor determinante para o início do desenvolvimento de tecnologias de rede sem fio de longa abrangência geográfica foi o problema do alto custo da rede cabeada em banda larga entre o provedor de serviços e o usuário (última milha). Assim, surgiu o grupo de trabalho do padrão IEEE 802.16 [6] para redes metropolitanas de banda larga sem fio (WMANs - *Wireless Metropolitan Area Network Working Group*). Porém, o padrão original apenas previa a existência de estações fixas conectadas através de um enlace rádio com linha de visada em uma topologia ponto-multiponto (*point multi point* - PMP). No entanto, a evolução do padrão veio suprir as tendências do mercado e dos usuários que buscavam obter acesso sem fio em estações móveis, através de antenas onidirecionais, operação em baixas freqüências e com a possibilidade de utilização em uma topologia *mesh* (malha). Para tal, surgem os diversos adendos que foram sendo publicados desde então, até chegarmos ao padrão IEEE 802.16e [1], publicado em dezembro de 2005. Esse tipo de rede sem fio se aplica as regiões urbanas, oferecendo uma cobertura geográfica consideravelmente maior que as WLANs, chegando a distâncias de até 50 km [16] e altas taxas de transmissão (até 75 Mbps).

Outro grupo de trabalho em andamento é o referente ao padrão IEEE 802.20, cujo escopo é redes com dispositivos móveis que se movimentam em altas velocidades. O objetivo maior desse padrão é o de estabelecer mecanismos de *handoff* compatíveis com esse cenário, sem a perda da conectividade.

Além dos padrões de redes de dados sem fio, as redes celulares também compõem o conjunto das redes sem fio metropolitanas. Porém os padrões digitais passaram por três gerações distintas [17]: **(i)** Voz analógica (1G), **(ii)** Voz digital (2G) e **(iii)** Voz digital e dados (3G). Atualmente é vivenciado um momento de transição entre celulares 2G e 3G, sendo o primeiro ainda dominante. Contudo, existe a tendência natural para a substituição desses padrões pela tecnologia das redes celulares de terceira geração (3G) que suportam tráfego multimídia. Cabe salientar, que tais dispositivos possuem em geral um baixo poder computacional e limitações de baterias. Essas limitações restringem o uso de aplicações mais robustas, inclusive para o uso de alguns algoritmos de criptografia mais seguros, sem a respectiva perda dos requisitos de QoS.

2.1.2 - O padrão IEEE 802.16

O padrão IEEE 802.16 [2] (WMAN) especifica a interface aérea de sistemas fixos e móveis de acesso sem fio de banda larga (BWA - *Broadband Wireless Access*) com suporte a serviços multimídia, operando nas faixas de freqüência de 10 a 66 GHz ou abaixo de 11GHz. Foi criado inicialmente (IEEE 802.16-2004) para operar com estações fixas (Figura 2.1): Estação Base (*Base Station* - BS) e Estações Assinantes (*Subscriver Station* - SS).

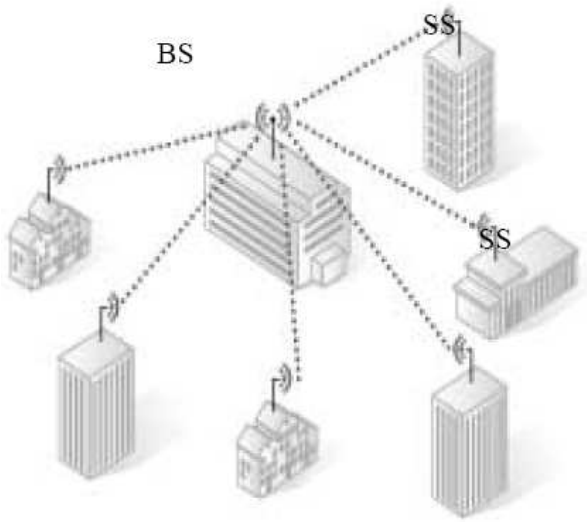


Figura 2.1. Rede Metropolitana Banda Larga Sem Fio – Padrão original - PMP.

Esse Padrão permite arquiteturas ponto-multiponto (PMP) e em malha (*mesh*). Na topologia PMP, os SSs 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.

O novo padrão IEEE 802.16e - 2005 [1] adiciona mobilidade ao padrão 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. A mobilidade provoca a necessidade de uma reserva adicional de recursos para suportar a transferência de conexões ativas entre células (*handoff*). Quanto maior a mobilidade, maior a probabilidade de ocorrência de *handoff* entre células vizinhas e, por conseguinte, maior a quantidade de recursos que devem ser reservados.

Pilha de protocolos

A pilha de protocolos do padrão IEEE 802.16 é ilustrada na Figura 2.2. A estrutura é semelhante à das outras redes IEEE 802, mas tem um número maior de subcamadas. A camada inferior, PHY, lida com aspectos de transmissão.

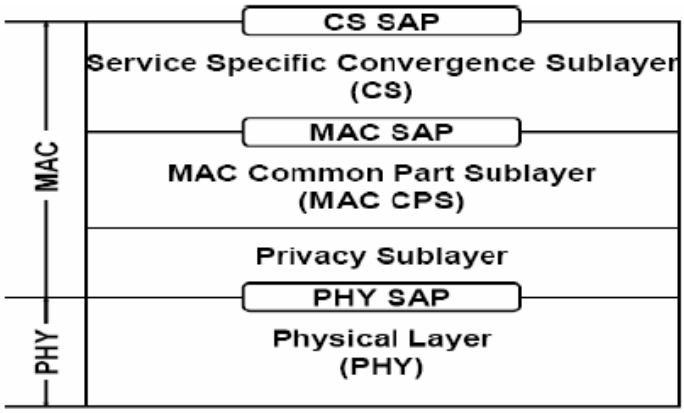


Figura 2.2. Camadas Física e de Acesso ao meio – Padrão IEEE 802.16.

A camada de enlace de dados é composta por três subcamadas. A inferior (*Privacy sublayer*) lida com privacidade e segurança, nos aspectos de criptografia, decriptografia e gerência de chaves. Na parte comum da subcamada MAC (MAC CPS) estão localizados os principais protocolos, como o de gerenciamento de canais, por exemplo. Na camada de convergência é tratado o interfaceamento das várias tecnologias de rede, entre elas as das redes IP e ATM. Um recurso incomum da subcamada MAC é que, diferente do que ocorre nas outras redes IEEE 802, ela é completamente orientada a conexões, a fim de fornecer garantias de qualidade de serviço para fluxos oriundos de aplicações de tempo real, tais como telefonia IP e vídeo sob demanda.

2.2 - Mecanismos de Posicionamento

O advento da computação móvel tem impulsionado a criação de diversas aplicações para preencher as novas necessidades que a mobilidade introduz nesses cenários. A principal necessidade é em se ter o conhecimento onde, fisicamente, estão localizados os elementos de uma rede móvel [18]. Seja para aplicações de usuários, gerenciamento ou segurança, os aplicativos de posicionamento são cada vez mais difundidos para as redes sem fio em geral, através de vários sistemas e tecnologias [18, 19]. Todavia, esses sistemas e tecnologias se baseiam nas Técnicas de Localização por Sensoriamento.

2.2.1 - Técnicas de Localização por Sensoriamento

As principais técnicas usadas para automatizar os mecanismos de posicionamento são [18]: **(i) a Triangulação, (ii) a Análise de Cenários** e **(iii) a Proximidade.** Tais técnicas podem, ainda, ser utilizadas de forma combinada.

A técnica de localização por **Triangulação** utiliza as propriedades geométricas dos triângulos para calcular a posição de objetos. Essa técnica pode, ainda, ser subdividida em duas categorias: **Lateralização** (*Lateration*), que usa medidas de distâncias (Círculos de Distâncias) e **Angulação** (*Angulation*), que utiliza medidas angulares (Linhas de Marcações). A **Lateralização** calcula a posição de um objeto pela medição de sua distância para múltiplas posições de referência. Para possibilitar os cálculos em duas dimensões (Plano) é necessária a medição da distância de três pontos não co-lineares, sendo não co-planares com o objeto quando se desejar obter a posição tridimensional.

Existem três abordagens gerais para a obtenção das distâncias requeridas pela técnica da Lateralização, descritas a seguir. **(i) Direta** (*Direct*) – Medição direta da distância através de um instrumento físico como, por exemplo, uma haste de um robô. **(ii) Tempo-de-vôo** (*Time-of-flight*) **–** Medição da distância de um objeto para algum ponto "*P*", através do tempo que esse objeto leva para ir de sua posição até *"P"* em uma dada velocidade conhecida. Ou seja, calcula-se a diferença entre o momento da transmissão e o de chegada no receptor. Exemplos dessa abordagem são os usos de pulso de ultra-som e de luz assim como de ondas de rádio. **(iii) Atenuação** – (*Attenuation*) – A regra para o cálculo da distância por atenuação está no fato de que a intensidade de um sinal emitido decresce à medida que a distância do emissor aumenta. Dada uma função que correlacione a atenuação e a distância por tipo de emissão e pela potência

inicial da transmissão, é possível estimar a distância de um objeto até algum ponto "*P*" pela medição da potência do sinal no receptor, quando esse chega em "*P*".

A **Angulação,** a outra categoria da técnica de Triangulação**,** é similar a Lateralização, exceto que ao invés de distâncias, são usados ângulos para a determinação da posição de um objeto. Em geral, para a determinação da posição em duas dimensões são necessárias duas medidas de ângulos e uma medida de distância entre os pontos de referência (distância previamente conhecida). A obtenção desses parâmetros, ângulo e distância, se dá com a utilização de múltiplas antenas receptoras, posicionadas a distâncias conhecidas umas das outras.

A segunda técnica de localização**, Análises dos Cenários,** utiliza as observações do cenário em torno do objeto, a fim de se determinar a sua posição. Essas observações, que podem ser feitas por imagens, por exemplo, são comparadas com uma base de dados que é constantemente atualizada. A partir desse processo de comparação e da evolução das observações pode-se determinar a posição e a direção de determinado objeto [18].

A terceira e última técnica, **Proximidade,** determina a posição de dado objeto, quando ele está próximo de uma localização conhecida. A presença do objeto é detectada através de fenômenos físicos com alcance limitado. Um exemplo de aplicação dessa técnica são os detectores de presença, identificadores por códigos de barra, etc.

2.2.2 - Sistemas de Localização

Em [18-20] são descritos diversos sistemas de localização utilizados na computação móvel e ubíqua, fundamentados nas técnicas citadas, e suas respectivas características. O principal e mais popular sistema de localização utilizado atualmente é o **GPS (***Global positioning system*), que utiliza técnicas de triangulação por Lateralização, através do método de Tempo de vôo (*Time-of-flight*). O GPS provê, através de sinais de satélites que podem ser processados em um receptor, a possibilidade de se calcular a posição e velocidade do equipamento. A precisão do GPS varia de acordo com o equipamento em uso. Alguns equipamentos mais baratos podem determinar a posição geográfica com uma precisão de 10 a 15 metros para aproximadamente 95% dos casos [18, 21]. Outros equipamentos mais caros (DGPS – *Differential GPS*) utilizam a informação de estações em terra a fim de corrigir os erros dos sinais do satélite. Desta forma, a precisão pode ser aumentada para a faixa de 1 a 3m, em 99% dos casos [18].

Outros sistemas também são usados. Entre eles está o **VOR** [18], que utiliza a técnica da angulação, é usado em regiões metropolitanas com a disposição de diversas estações com linha de visada para o transmissor e possui uma precisão angular de 1º. O **MSR RADAR** [22], usado para redes sem fio locais, utiliza conjuntamente as técnicas de análise de cenário e triangulação na determinação das posições dos nós da rede, possuindo uma precisão de 3 a 4m. O **PinPoint 3D-iD** [18] utiliza a técnica de Lateralização por atenuação, possuindo uma precisão de 1 a 3m e é usado para redes locais sem fio. Os ***Automatic ID Systems*** [18] são sistemas que se utilizam da técnica da proximidade para a determinação da posição. Podem ser usados em pequenas ou grandes áreas de coberturas, possuindo uma precisão de acordo com o tipo de sensor. Um exemplo dessa aplicação são os **RFID** (*Radio Frequency Identification*), que podem determinar a posição de um objeto com precisão de 1m. O ***Automatic Position Reporting System*** **(APRS)** [23] é um sistema software livre (*open-source*), desenvolvido por Bob Bruninga para a localização de objetos usando rádio amadores. Ele captura e reporta posições geográficas, através de informações trocadas entre várias estações em determinada área de cobertura.

2.3 - Segurança em Redes sem Fio

Em relação ao quesito segurança, foco do presente trabalho, qualquer rede é considerada segura se ela atende a determinados requisitos. Os principais requisitos ou serviços de segurança são [4]:

- **Confidencialidade** - garantia de proteção de uma informação armazenada ou transmitida contra divulgação a uma entidade não autorizada;
- **Autenticação** - método de comprovação da identidade de um parceiro de comunicação ou autor de mensagem;
- **Integridade** - garantia de proteção de informações armazenadas ou em trânsito contra a modificação por uma entidade não autorizada;
- **Irretratabilidade** - garantia de que determinada entidade que tenha transmitido ou recebido uma mensagem não alegue que não a transmitiu ou não a recebeu;
- **Disponibilidade** - garantia de que determinado recurso ou o próprio sistema esteja sempre “disponível” para as entidades autorizadas;
- **Controle de acesso** - garantia que somente as entidades autorizadas tenham acesso a um determinado recurso e que essas “autorizações” não sejam modificadas indevidamente;

- **Auditoria** – garantia do armazenamento de informações sobre a utilização de recursos do sistema.

A aplicação desses quesitos já é uma tarefa complexa para redes que adotam infra-estruturas cabeadas, onde as informações trafegam em meios naturalmente protegidos, tais como cabos coaxiais, pares trançados e fibras óticas. Entretanto, tais quesitos tornam-se mais desafiadores quando são empregados nas redes sem fio.

2.3.1 - Ameaças

Uma ameaça é qualquer situação ou evento que possua um potencial de causar dano a um sistema [10]. As ameaças são classificadas quanto à atividade do atacante em dois tipos: **Passivas**, onde o sistema continua a operação sem a percepção de ter um invasor na rede e, geralmente, acontece roubo de informações; e **Ativas**, onde o invasor prejudica o sistema, atingindo os dados ou degradando os serviços. Quanto à origem, as ameaças também são classificadas em dois tipos: **externas**, quando estão fora das fronteiras da instituição da rede alvo e **internas**, quando provém 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.

2.3.2 - Ataques

Um ataque é uma tentativa intencional de burlar as medidas de segurança adotadas nos sistemas informatizados de alguma forma [10]. Os ataques se classificam em quatros tipos básicos: **(i) interrupção, (ii) interceptação, (iii) modificação e (iv) fabricação**. A Figura 2.3.a ilustra o fluxo normal da informação entre a origem e o destino. A Figura 2.3.b ilustra uma **interrupção** no fluxo de informação, que objetiva interromper o serviço oferecido, ou seja, ataca-se à disponibilidade das informações.

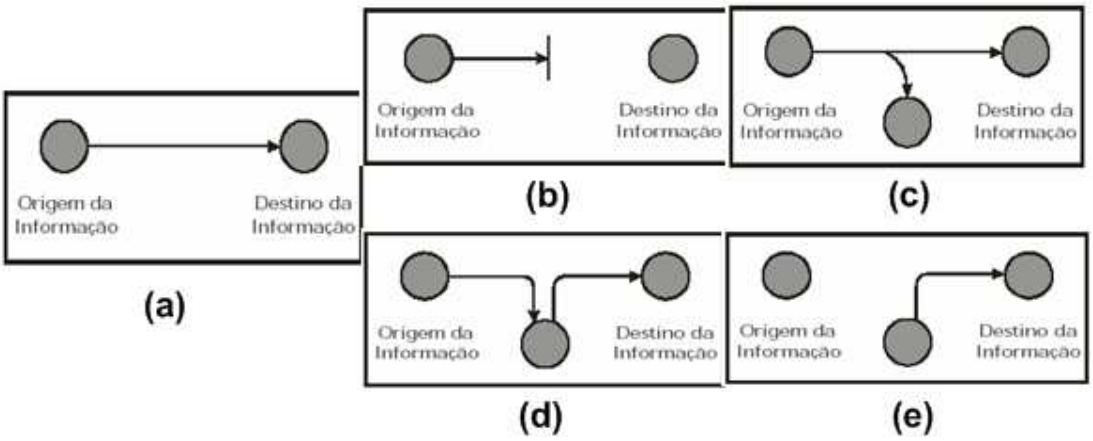


Figura 2.3. (a) Fluxo normal. (b) Fluxo Interrompido. (c) Fluxo interceptado. (d) Fluxo modificado. (e) Fluxo fabricado.

A **interceptação,** Figura 2.3.c, tem por objetivo capturar o que está sendo transmitido sem que o sistema perceba, ou seja, ataca-se a confidencialidade das informações. A **modificação,** Figura 2.3.d, é a ocorrência de uma alteração na informação que está sendo transmitida, ou seja, ataca-se a integridade da mesma. Na **fabricação,** Figura 2.3.e, o atacante tem como finalidade se passar por um usuário do sistema, a fim de obter informações para transmitir dados na rede, ou seja, ataca-se a autenticidade das informações.

Contudo, para se obter o sucesso desejado, um ataque deve explorar as vulnerabilidades existentes no ambiente alvo. Uma **vulnerabilidade** é uma fraqueza ou ponto fraco existente em um sistema que pode ser explorado de forma a violar a política de segurança [10].

2.3.3 - Técnicas de Invasão

O propósito de uma invasão é o de obter um ataque bem sucedido contra um sistema, através da violação intencional de sua política de segurança [10]. Na prática, uma invasão é a entrada em um servidor, computador ou serviço por alguém não autorizado. A seguir são descritas as técnicas de invasão, relevantes a este trabalho.

Personificação (*Spoofing)*

Nessa técnica, o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para acessar o que não deveria ter acesso, falsificando o seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um

usuário externo se faz passar por um usuário ou computador interno ao domínio de controle [4]. Os métodos mais comuns são: o *MAC spoofing*, o IP *spoofing* e o *DNS spoofing*.

Homem no Meio e Roubo de Sessão

Os ataques Homem no Meio (*Man-in-the-Middle – MiTM*) e Roubo de Sessão (*Session Hijacking*) exploram as vulnerabilidades encontradas nos serviços de autenticação, irretratabilidade e controle de acesso. O ataque de MitM, esquematizado na Figura 2.4, é um ataque do tipo *proxy*, onde o atacante, se posicionando entre as duas vítimas (estações 1 e 2 da Figura 2.4), fica apto a monitorar e modificar as transmissões das vítimas.

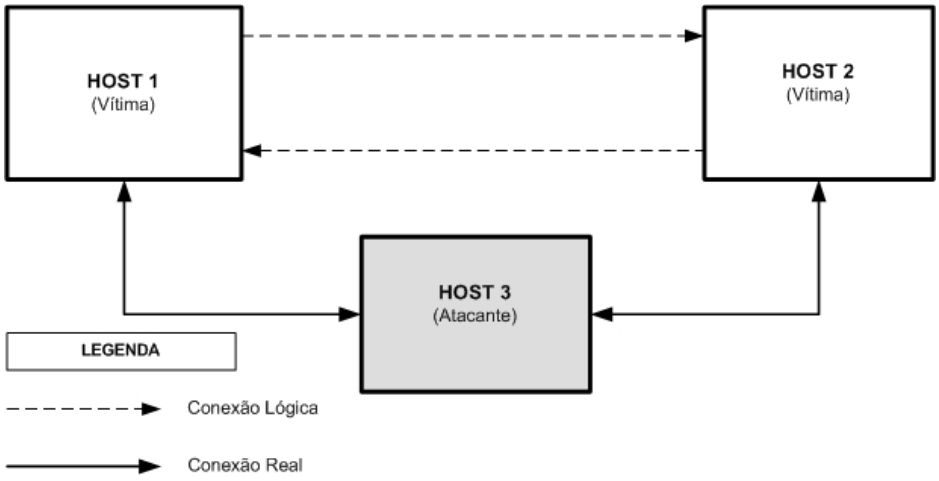


Figura 2.4. Ataque de man-in-the-middle.

A presença do atacante é transparente para as vítimas e, desta forma, as estações 1 e 2 pensam que estão se comunicando normalmente. O MitM pode ser usado contra diversos protocolos vulneráveis a esse tipo de ataque. Para cada protocolo existe uma técnica específica para a sua utilização (MitM-SSHv1, MitM-Ipsec, MitM-HTTPS, etc.).

O ataque de Roubo de Sessão é similar ao homem-no-meio, no que diz respeito à técnica utilizada e à exploração das vulnerabilidades dos protocolos. A diferença está no fato de que no Roubo de Sessão o atacante envia uma mensagem de desautenticação para o usuário legítimo, seqüestrando a sua conexão. Assim, a vítima é desassociada, enquanto a estação base mantém internamente o estado do dispositivo como conectado. O Roubo de Sessão também pode ocorrer quando não há na rede sem fio um mecanismo de autenticação/integridade nos quadros, normalmente existentes nos algoritmos criptográficos mais robustos (HMAC/CMAC TLV).

Assim, o Roubo de Sessão pode ocorrer após uma desautenticação (mensagem de gerência) direta realizada pelo atacante, e o seqüestro da conexão através de técnicas de personificação.

Evasão

A evasão é a arte de não deixar pistas de quem, como e quando foi invadido o sistema. Quando a evasão é realizada com êxito, a descoberta da invasão e das vulnerabilidades causadoras fica muito comprometida. Portanto, é de suma importância a implementação de sistemas de segurança que operem em tempo real, a fim de se evitar que a técnica de evasão apague as pistas porventura deixadas por um invasor.

2.3.4 - Aspectos de segurança do Padrão IEEE 802.16 - 2004

O padrão IEEE 802.16-2004 especifica protocolos para autenticação e privacidade (confidencialidade dos dados) na subcamada de privacidade (*Privacy Subblayer*) conforme desenho da Figura 2.2. Esses protocolos se baseiam no protocolo PKM (*Privacy Key Management*) da especificação DOCSIS BPI [2]. O PKM é construído ao redor de um conceito de associações de segurança (AS). Uma associação de segurança contém informações sobre o algoritmo de criptografia a ser utilizado, o algoritmo de autenticação de dados, e o algoritmo para troca de chaves de criptografia de dados. Cada assinante estabelece pelo menos uma AS durante a inicialização. Cada conexão, com exceção das de gerenciamento básico, é mapeada em uma AS tanto no momento de estabelecimento de conexão como dinamicamente durante a operação. No padrão aprovado em 2004, no momento em que um assinante se conecta a uma Estação Base, ele executa um processo de autenticação com criptografia RSA de chave pública, usando certificados X.509. Nessa fase, o assinante também informa as suas capacidades (*capabilities*) a fim de receber o material criptográfico adequado, e informar as suas limitações de operação. Todavia, apenas os assinantes são autenticados, as Estações Base, não. Além disso, é importante registrar que apenas os dados do usuário são protegidos no padrão IEEE 802.16-2004, os cabeçalhos não são. Ou seja, a criptografia é aplicada apenas sobre a carga útil do MAC PDU (*Package Data Unit*).

Para a criptografia dos dados é usado o DES (*Data Encryptation Standard*) executando em modo CBC (*Cipher Block Chaining*) com chaves de 56 bits. É importante notar que a segurança fornecida pela *privacy sublayer* é baseada em criptografia para a camada 2. Essa

proteção da *privacy sublayer* visa resguardar a carga útil contida nos pacote de dados, somente enquanto ela trafega no meio sem fio.

Vulnerabilidades no protocolo de autenticação do Padrão IEEE 802.16-2004

As vulnerabilidades encontradas no padrão estão contidas em ambas as camadas tratadas pela norma (Física e MAC) [5]. No que diz respeito à camada física, por estar posicionada abaixo da subcamada de privacidade, esta não a protege. Ou seja, o padrão está sujeito a todos os tipos de ataques de camada física, que exploram as características do meio de difusão. Entre eles podemos citar o *Millitar Jamming* e o *Water Torture Attack.* O primeiro é um ataque de negação de serviços que é executado para simplesmente bloquear o canal de comunicação através da emissão de maior potência nas mesmas freqüências da rede sem fio. O segundo ataque (*Water Torture*) é executado através do envio de quadros através de uma técnica chamada de inundação (*flooding*), a fim de se esgotar as baterias dos dispositivos.

No tocante a camada MAC, a própria evolução do padrão de enlace por linha de visada para onidirecionais, utilização de baixas freqüências (10 – 66 Ghz para 2 – 11 GHZ), a inclusão da mobilidade e do modo *mesh* propiciam a exploração de mais vulnerabilidades [5]. Com antenas onidirecionais, o atacante não necessita estar posicionado entre o transmissor e o receptor para efetuar um ataque. Com a utilização de baixas freqüências, os equipamentos são mais baratos, ampliando o universo de atacantes. A mobilidade amplia as possibilidades de busca por vítimas e restringe os níveis de segurança das conexões até os limites mínimos que possibilitem uma troca de célula (*handover*). Nesse caso, os procedimentos de *roaming* devem possuir um baixo custo computacional para atender requisitos de QoS em aplicações de tempo real. Por exemplo, para uma chamada de voz, o limite de 30 ms de atraso (*delay)* no *roaming* não pode ser excedido. Com isto, a robustez criptográfica dos protocolos de autenticação deve respeitar tais limites. O modo *mesh* introduz novos conceitos de segurança que os atuais mecanismos de segurança não tratam adequadamente. É o caso do estabelecimento dos níveis de confiança com os vizinhos e como medir e avaliar o dinamismo desses parâmetros [5].

Contudo, a não autenticação mútua constitui uma das principais vulnerabilidades desse protocolo de autenticação, pois permite que uma Estação Base falsa possa injetar pacotes maliciosos na rede [3]. Essa vulnerabilidade abre as portas para ataques de Roubo de Sessão e Homem no Meio. Além disso, por falta de um algoritmo que proveja autenticidade e integridade

dos dados transmitidos, um usuário malicioso pode injetar, alterar e repetir (*replay attack*) dados na rede [3, 5]. Um ataque possível é a injeção de uma mensagem de desautenticação para uma SS (*Subscriver Station*), feita por um atacante. Por ser uma mensagem de gerência, ela não necessita estar criptografada [3]. Além dessas vulnerabilidades, existem as inerentes aos mecanismos de gerenciamento de chaves e ao tamanho das TEKs (*Traffic Encription Key*).

Novos requisitos de segurança incluídos no padrão IEEE 802.16e

O padrão IEEE 802.16e introduz novos requisitos de segurança, no intuito de minimizar os efeitos das vulnerabilidades que o padrão IEEE 802.16-2004 possui. Entre as principais mudanças, relativas ao quesito segurança, estão: **(i)** a utilização do padrão de criptografia AES (A*dvanced Encryption Standard)*; **(ii)** a introdução de padrões de autenticação mais robustos, com autenticação mútua e a flexibilização da autenticação para mecanismos baseados nos métodos do protocolo EAP (*Extensible Authentication Protocol*) [24] e **(iii)** a permissão para a utilização de processos de reautenticação de baixo custo computacional nos procedimentos de *roaming.*

A primeira mudança visa sanar as vulnerabilidades inseridas pelo uso do algoritmo DES (56 bits), através do aumento da robustez criptográfica oferecida pelo padrão AES (128 bits), produzindo, contudo, sobrecargas computacionais, muitas vezes inadequadas aos dispositivos móveis de baixo poder computacional [8].

A segunda mudança tem o intuito de sanar o problema da autenticação mútua (*Mobile Station* – **MS** e *Base Station* - **BS**) pelo do uso de chaves públicas, previstas no protocolo de certificação digital X.509 [25], por ambas as partes. Todavia, outros métodos de autenticação podem ser escolhidos, desde que baseados no EAP [24]. Essa flexibilização visa não obrigar o uso de certificação digital, possibilitando um menor custo financeiro e um melhor desempenho dos mecanismos de *handoff.* Contudo, o tipo de método EAP a ser usado está fora do escopo da norma IEEE 802.16e, abrindo margem para a implementação de métodos vulneráveis a ataques. A Figura 2.5 mostra a arquitetura da nova subcamada de segurança.

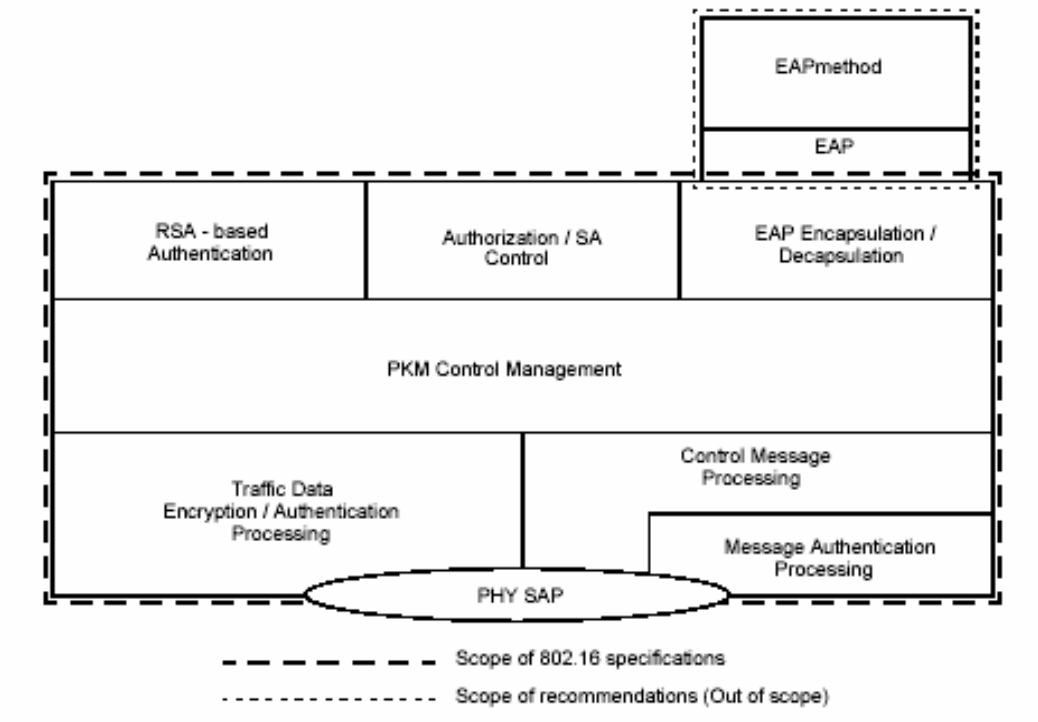


Figura 2.5. Nova Subcamada de Segurança do Padrão IEEE 802.16e [1]

Observa-se, na Figura 2.5, que o bloco "EAP/EAPmethod" está no escopo das recomendações (*out of scope*) e não das especificações.

Em suma, apesar das melhorias introduzidas no padrão 802.16e, as redes metropolitanas não podem prescindir do emprego de sistemas de seguranças adicionais, pois algumas vulnerabilidades ainda persistem, especialmente às tocantes a utilização de métodos EAP inseguros na autenticação dos usuários [26, 27]. Além disso, algumas técnicas previstas nesse padrão, baseadas em robustez criptográfica, são de difícil emprego em face da baixa capacidade computacional [8] de alguns tipos de dispositivos móveis. Para aumentar a segurança são empregados sistemas como *Firewalls*, anti-virus, *anti-spyware* e IDSs, sendo este último abordado na próxima Seção por ser o foco do presente trabalho.

2.4 - Sistemas de Detecção de Intrusos

Um Sistema de Detecção de Intrusos monitora dinamicamente as ações em um dado ambiente e decide quando essas ações constituem um sintoma de ataque ou um uso legítimo do ambiente [28]. Um IDS pode ser definido com um detector que processa informações oriundas de um sistema a ser protegido [28]. A Figura 2.6 ilustra a generalização de um IDS. O **Detector**

utiliza três tipos de informações: as oriundas de uma base de dados, as informações de configurações do sistema e os dados do sistema a proteger.

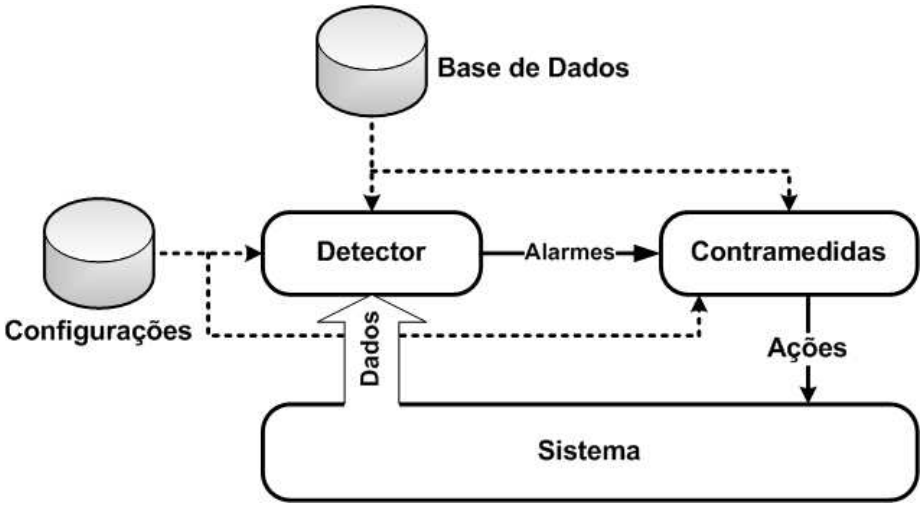


Figura 2.6. Generalização de um IDS [28].

Após o processamento, uma decisão é, então, tomada pelo **Detector** podendo gerar alarmes ao componente de **Contramedidas**. Este, por sua vez, toma as ações necessárias no sistema a proteger, visando corrigir ou prevenir as anomalias.

Na prática, um IDS automatiza a tarefa de analisar dados de auditoria, aumentando a sua rapidez (Tempo Real) e precisão. Além disso, contribui com o paradigma da proteção em camadas, onde se busca a convivência integrada das diversas tecnologias de segurança no intuito de se aumentar a segurança global dos sistemas. Os IDSs são especialmente úteis no monitoramento das atividades dentro das redes. Outrossim, os registros dos IDS podem ser usados para estabelecer a culpabilidade de um atacante e, na maioria das vezes, é o único modo de descobrir uma atividade sem autorização, detectar a extensão dos danos e prevenir tal ataque no futuro.

2.4.1 - Classificação dos IDS

Para classificar os Sistemas de Detecção de Intrusos, diversos conceitos podem ser utilizados. Entre eles estão os [28]: **(i)** Métodos de Detecção**, (ii)** Postura da Detecção**, (iii)** Origem dos Dados**, (iv)** Freqüência de uso**, (v)** Aspectos de tempo **e (vi)** Topologia**.** Os **Métodos de Detecção** descrevem as características do Detector, no tocante à abordagem de monitoramento. Classicamente, há duas formas de identificar ataques: **por anomalia** (*Anomaly*

Detection ou Detector de Anomalias) e por **padrões de ataque** (*misuse detection* ou Detector de Abuso).

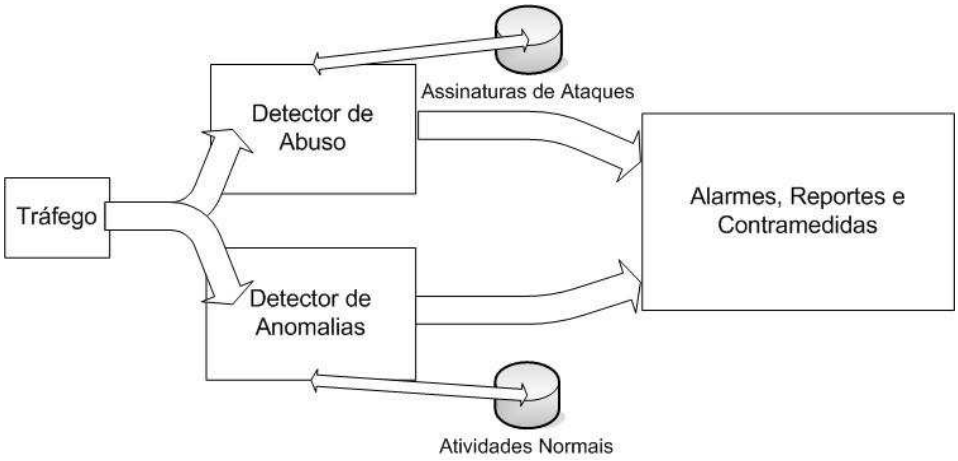


Figura 2.7. Métodos de Detecção contidos em uma Arquitetura clássica de IDS.

No primeiro caso, a ferramenta estabelece um padrão de normalidade e classifica como ataque ou intrusão qualquer atividade que se afaste significativamente desse padrão. Esse método possui a vantagem de possibilitar a detecção de ataques novos (ataques do dia "zero"), ao custo de gerar um índice maior de alarmes falsos. No segundo caso, padrões de ataque, o sistema é alimentado com padrões que identificam atividades consideradas impróprias, gerando um alarme a cada vez que os padrões procurados sejam encontrados no fluxo de informação. Esse método possui índices menores de alarmes falsos, porém necessita de constantes atualizações em suas bases de assinaturas, ocasionando, via de regra, vulnerabilidades a ataques novos. A Figura 2.7 mostra uma arquitetura clássica de um IDS, que ilustra os **Métodos de Detecção** [10].

O segundo conceito, **Postura da Detecção,** descreve o tipo de resposta que o IDS terá diante de um ataque. Quando o IDS reage aos ataques, executando ações corretivas, ou age pró-ativamente [28] (desconectando possíveis atacantes ou encerrando serviços) diante de suspeitas ou sinais de ataques, ele é classificado como **Ativo.** Quando somente dispara alarmes, é classificado como **Passivo.**

O terceiro conceito, **Origem dos Dados,** faz a distinção entre os tipos de entradas que serão analisadas, no tocante a sua localização. Podem, por exemplo, ter origem nos nós da rede, nos registros do sistema, nos pacotes que trafegam na rede, etc. Logo, por esse conceito podemos classificar os IDS em: **(i) HIDS** (*Host Intrusion Detection System*), responsável pela monitoração

de um único nó, geralmente um servidor. **(ii) NIDS** (*Network Intrusion Detection System*), responsável por analisar o tráfego de uma rede ou um trecho específico dessa rede, normalmente instalado em pontos de concentração de tráfego. **(iii) WIDS** (*Wireless Intrusion Detection Systems*), possuindo a origem dos dados nas transmissões sem fio, características dessa tecnologia. Dentro dessa classificação, vêm surgindo novas abordagens, destacando-se as inerentes à própria camada física e às técnicas orientadas à localização dos nós (*located based techniques*). **(iv) Aplicações,** representadas por analisadores de registros (*logs*) do sistema.

O quarto conceito, **Freqüência de Uso,** diz respeito à forma de utilização do IDS, podendo ser dividido em dois casos: **Monitoração Contínua** e **Análises Periódicas.** No primeiro caso, o IDS monitora o sistema em tempo integral, enquanto que no segundo caso em momentos ou situações específicas.

O quinto conceito, **Aspectos de Tempo,** divide os IDS em dois tipos: Tempo Real e Desconectado (*off-line*). O primeiro é executado durante a ocorrência dos eventos e têm como um de seus objetivos detectar invasões durante a ocorrência das mesmas, diminuindo o tempo de resposta aos incidentes. O segundo visa buscar a comprovação de ataques após a ocorrência dos mesmos, como, por exemplo, uma ferramenta de auditoria.

O sexto conceito, **Topologia**, classifica os IDS em dois tipos: Centralizado e Distribuído. Na topologia **Centralizada**, o IDS está localizado em pontos estratégicos da rede de onde pode coletar todos os dados necessários a sua operação. Além disso, esse elemento central concentra todo o processamento do detector de intrusos. Na topologia **Distribuída**, as tarefas do IDS são divididas por vários componentes, localizados em vários locais da rede. O processamento é divido por esses componentes que executam tarefas mais específicas e mais simples. A idéia dessa topologia é exatamente aproveitar os recursos de processamento de uma rede de forma a obter uma melhor eficiência. Um exemplo desse último tipo está no emprego de agentes de *software* na arquitetura.

2.4.2 - Eficiência dos IDS

Para possibilitar a avaliação dos Sistemas de Detecção de Intrusos, são utilizadas algumas medidas que determinam à eficiência de um IDS [28, 29]:

- **Completude** – Mede a capacidade de um IDS em não deixar de detectar um ataque (**Falsos Negativos**);
- **Acurácia** – Mede a capacidade do IDS em não gerar alarmes falsos (**Falsos Positivos**);
- **Desempenho** – Mede a taxa de processamento de dados que um IDS é capaz de realizar. Os IDS de tempo real devem possuir um desempenho que atenda ao tempo de resposta a incidentes desejados;
- **Tolerância a Falhas** – Capacidade do IDS em resistir às falhas e/ou ataques (especialmente os de negação de serviços) contra si, sem perda de suas funcionalidades.

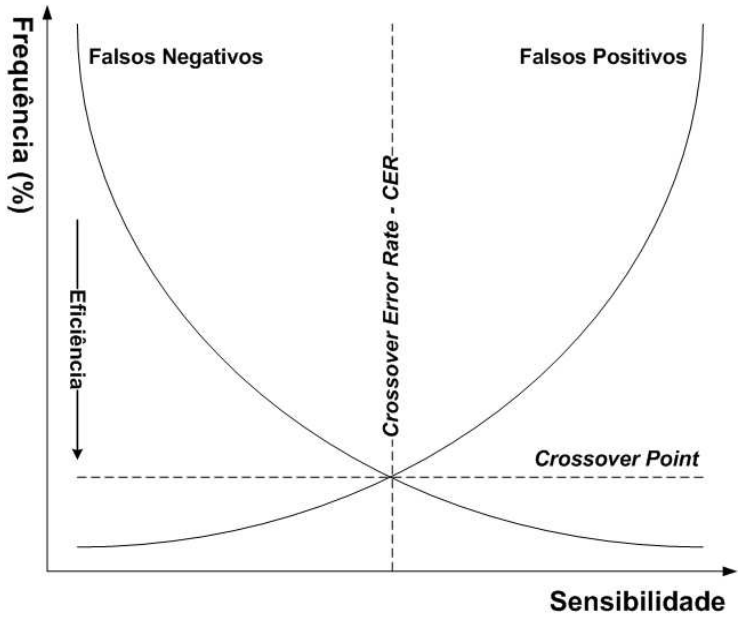


Figura 2.8. Gráfico representativo do *Crossover Error Rate – CER.*

Outro aspecto importante na avaliação da eficiência de um IDS está na relação entre os índices de Falsos Positivos e Negativos (*Crossover Error Rate – CER)*. Essa relação de equilíbrio visa balancear as taxas de erros de forma a otimizar tanto a **Completude** quanto a **Acurácia** do IDS. O gráfico da Figura 2.8 ilustra essa relação.

O eixo “y” representa a freqüência (Taxas) em que ocorrem os Falsos Positivos e/ou Negativos. O eixo “x” indica em ordem crescente os níveis de sensibilidade de detecção

configurados no IDS. O significado da sensibilidade varia com o tipo de IDS, representando, de uma forma geral, as configurações que tornam o IDS mais rigoroso em suas análises, gerando um maior número de alarmes. Observa-se que quanto mais for incrementado o nível de sensibilidade do IDS, maior será o número de intrusos detectados, reduzindo o índice de Falsos Negativos. Em contrapartida, nesse caso, o índice de Falsos Positivos também cresce progressivamente à medida que a sensibilidade aumenta, tornando inviável a utilização do IDS. No sentido oposto, quanto menor for a sensibilidade menor será o índice de Falsos Positivos, ao preço de uma redução brusca nos acertos, ou seja, um aumento exponencial de Falsos Negativos. O ponto ótimo está indicado no gráfico da Figura 2.8, e é onde há intersecção entre as curvas de Falsos Positivos e Negativos. Nesse ponto, as freqüências se igualam e quanto menor for o valor da freqüência, no ponto de intersecção (*crossover point)*, mais eficiente é o IDS.

Na busca incessante pela eficiência, várias abordagens vêm sendo propostas ao longo do tempo. Uma das linhas de pesquisa é aquela que investiga o uso de algoritmos de Inteligência Computacional nas implementações dos IDS. Dentre eles, destacam-se os inerentes a Redes Neurais e a Lógica Nebulosa. No próximo item são abordados os principais conceitos alusivos a Lógica Nebulosa, pois tal abordagem é relevante a arquitetura de IDS proposta neste trabalho.

2.5 - Lógica Nebulosa

Os dois principais aspectos da imperfeição da informação são a imprecisão e a incerteza. Essas 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 [30, 31]. Essa 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. Essa 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. Essas faixas de valores são modeladas por conjuntos nebulosos que são nomeados através de rótulos.

Para descrever 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 um ou mais conjuntos nebulosos.

Em geral, um sistema nebuloso é composto por 5 componentes, conforme ilustrado na Figura 2.9.

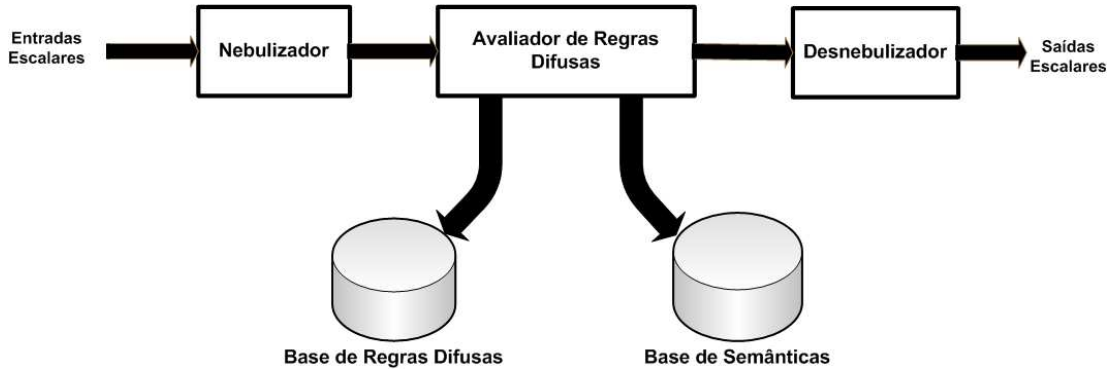


Figura 2.9. Diagrama de um sistema nebuloso.

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 esse passo, essas 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, essas saídas sofrem um processo de *desnebulização*, onde são novamente transformadas em valores escalares.

2.6 - Trabalhos Relacionados

A detecção de intrusos tem sido foco de inúmeras pesquisas ao longo dos últimos vinte anos. Diversas abordagens foram apresentadas, ao longo do tempo, dando forma a atual taxonomia dos IDSs, conforme descrito na Seção 2.3. As mais recentes contribuições nessa área são as: **(i)** que investigam novas técnicas de detecção de intrusos, dentro das classificações

consagradas; **(ii)** que integram as diversas abordagens em sistemas híbridos; **(iii)** que exploram características inerentes à tecnologia empregada na detecção de intrusos e **(iv)** que utilizam algoritmos de inteligência artificial na elaboração dos detectores.

Em [11], é proposta uma arquitetura para detecção de intrusos, por anomalia, em redes sem fio móveis, onde cada nó da rede pode participar do processo de detecção, através do uso de agentes de software. Cada nó monitora a sua vizinhança em busca de anomalias no uso dos protocolos de roteamento. Similarmente, em [32], é proposto um sistema de detecção de intrusos distribuído para redes sem fio. As diferenças estão na inclusão de um componente responsável pelas ações de contramedidas e de que o protótipo foi testado diante de ataques de *man-in-the-middle*. Em [33], é proposto um procedimento de detecção de nós não autorizados ao acesso de serviços específicos e de nós que foram comprometidos ao longo de sua conexão em uma rede sem fio *ad-hoc*. Apesar de a proposta possuir menor sobrecarga computacional em relação a soluções baseadas em criptografia, ela é baseada no uso de agentes instalados nos nós. O procedimento de detecção é dividido em duas fases, sendo a primeira o acompanhamento do processo de autenticação normal na rede. A segunda fase se inicia após, com a monitoração do nó por um agente de software instalado, que verifica desvios significativos no perfil padrão do nó (*anomaly detection*) e detecta ataques conhecidos por comparações com as suas respectivas assinaturas (*misuse detector*). Contudo, essas três propostas, ao utilizarem os recursos dos nós na execução dos agentes, aumentam o consumo das baterias e a sobrecarga computacional dos nós, o que pode degradar o desempenho das aplicações de tempo real, por exemplo. Esses fatos são agravados quando a rede é formada por dispositivos móveis de baixo poder computacional e com baterias limitadas. Em [34], é proposto um algoritmo para minimizar o problema do consumo de energia em detectores de intrusos distribuídos para redes sem fio, através de uma escolha criteriosa dos nós IDS, baseada nas cargas de baterias remanescentes em cada nó. Os nós da rede com maior reserva de baterias, dentro de determinada área de vizinhança, são usados como IDS, poupando os demais, ao custo da diminuição dos pacotes observados. Em contrapartida, essa abordagem reduz o desempenho do IDS no tocante ao seu índice de acertos, pois reduz a amostragem de pacotes analisados na rede.

Em [35], foi proposto um sistema de detecção de intrusos baseado, também, em uma infra-estrutura distribuída, com o emprego de quatro agentes de software (gerente, monitor, de decisão e de resposta). Esse IDS é do tipo HIDS e utiliza o método de detecção por anomalia.

Contudo, essa proposta também não é recomendada para a utilização em dispositivos móveis, especialmente os de baixo poder computacional, pelos mesmos motivos já citados. Em [36], é descrita e implementada uma arquitetura distribuída de um detector de intrusos baseado em agentes autônomos que executam tarefas específicas. Uma análise probabilística bayesiana é executada em função das informações de opinião dos agentes, gerando alarmes associados a uma probabilidade de sua ocorrência. Contudo, essa abordagem é mais adequada para uso em IDS sofisticados, por exigir um consumo mais alto de processamento. Em [37], é proposta uma arquitetura híbrida usando ambos os métodos de detecção (Anomalia e Abuso), integradas através de um sistema de suporte a decisão baseado em regras. Porém, a integração das abordagens é simples, ao se basear em apenas três regras. Além disso, o IDS não foi testado contra ataques do tipo homem no meio (*man-in-the-middle*), que é uma das principais preocupações no contexto das redes sem fio. Em [38], foi proposto um IDS voltado para as WLAN, que atua na camada de enlace, através do seqüenciamento dos quadros transmitidos, a fim de prover autenticação dos mesmos ao longo das transmissões, evitando o ataque de personificação. Todavia, essa proposta limita-se apenas às redes do padrão IEEE 802.11. Em [39], é proposto um IDS que busca identificar processos rodando nos dispositivos que causem a exaustão das baterias em dispositivos móveis. Através da monitoração do uso da CPU, acesso ao disco e outros parâmetros, o IDS estima o consumo de energia e identifica os processos maliciosos que buscam esgotar as baterias. Esta proposta é específica a esse tipo de ataque de negação de serviços, não se aplicando às outras categorias.

Em [40] e [41], são propostos dois mecanismos para a utilização em detecção de intrusos por anomalia, baseados nos comportamentos de mobilidade dos usuários. Essa abordagem ainda é pouco explorada, possuindo raros trabalhos a respeito. O primeiro [40] é voltado para redes celulares e cria um padrão de normalidade baseado nos itinerários que os usuários rotineiramente usam. Esses itinerários são mapeados através das células que compõem a cobertura da rede celular. Ou seja, os processos de *roaming* entre as células determinam o percurso do nó. O segundo [41] é voltado para redes sem fio móveis, e cria um padrão de normalidade baseado em um período de observação de 3 a 6 meses, definido como UMP (*user mobility profile*). Esses perfis, da mesma forma, estabelecem padrões baseados nos itinerários que normalmente os usuários utilizam no dia a dia. Nesse trabalho, os itinerários são baseados pela localização geográfica do usuário em cada data/hora da semana. O mecanismo de localização utilizado é o

APRS. Contudo, os resultados obtidos comprovam que os mecanismos propostos somente são adequados aos usuários que possuem um itinerário regular, não sendo eficientes nos demais casos ou quando os usuários mudam suas rotinas normais. Além disso, caso um atacante se enquadre no perfil da vítima por conhecimento da base de perfis, que é praticamente estática, poderá realizar os seus ataques.

Em [42], foi apresentada uma proposta de IDS nebuloso baseado em uma infra-estrutura de agentes móveis. Nessa proposta, uma máquina de inferência nebulosa é utilizada na integração das informações geradas pelos agentes. Contudo, a infra-estrutura permanece sendo a baseada em agentes de software que competem com o processamento dos nós na rede. Em [43] 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. Apesar de se comprovar a eficiência da utilização dos algoritmos de clusterização nebulosos em sistemas de detecção de intrusos, essa proposta não é aplicável a IDS de tempo real, devido ao tempo de processamento necessário para se realizar toda a clusterização da massa de *logs.*

Recentemente, a proposta de [14], 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, esse trabalho também não é eficaz na detecção de atacantes que possuam dispositivos autorizados.

2.7 - Identificador de Dispositivos por Assinatura de Transmissão

O trabalho proposto em [14] apresenta um tipo de análise que foi inicialmente utilizada pelos militares em operações Guerra Eletrônica (GE). Qualquer equipamento que utilize o espectro eletromagnético está passível de sofrer análises dos transmissores. Na sociedade civil, os primeiros a se utilizarem dessa tecnologia foram algumas companhias de celulares no intuito de diminuírem as fraudes com clonagens de telefones. Recentemente, observa-se a tendência de sua utilização em sistemas de detecção de intrusos para redes sem fio. Essa abordagem está integrada à arquitetura EWIDS, proposta neste trabalho, por intermédio de um componente chamado IDISP (Identificador de Dispositivos).

O identificador proposto em [14], atua na camada 1 (Física) para identificar de maneira unívoca os transmissores das interfaces de rádio dos dispositivos sem fio. Baseia seu funcionamento no espectro de freqüência dos sinais eletromagnéticos gerados pelos transmissores. O ponto chave da abordagem reside no fato de que a densidade espectral dos sinais transmitidos é função dos componentes de hardware específicos de cada interface física. Essas características eletromagnéticas identificam univocamente o "indivíduo", a interface física específica, diante de seus pares, desde que os parâmetros para análise sejam bem escolhidos e de acordo com alguns critérios lógicos [14]. Esse identificador funciona associando uma determinada transmissão em andamento a um perfil de transmissão correspondente. Para tal, faz-se necessário criar um banco de dados com os perfis de transmissão de cada transceptor autorizado e especificar um esquema de comparação e classificação dos transmissores em uso. O identificador de dispositivos, com seus diversos módulos, está ilustrado na Figura 2.10.

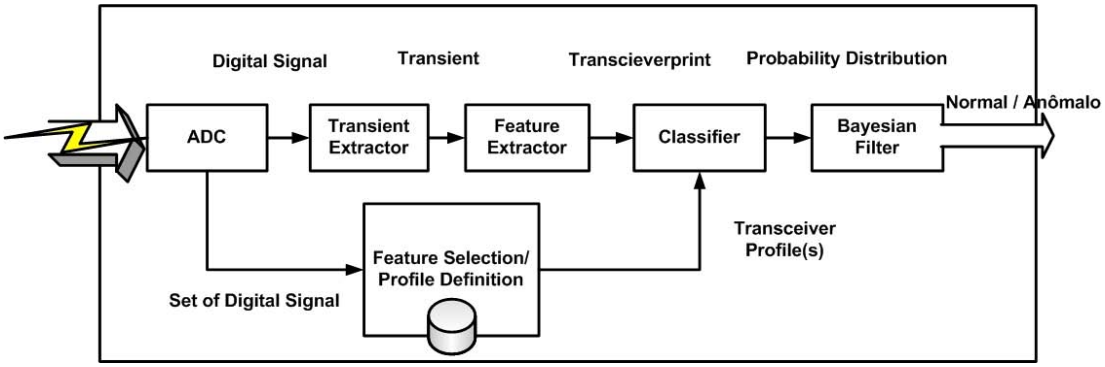


Figura 2.10. Digrama em blocos do componente IDISP.

O sentido da informação se inicia com a conversão do sinal analógico obtido da interface física da antena em um sinal digital utilizando-se um conversor analógico digital (ADC – *analog to digital converter*). Na forma digital, a porção do transiente do sinal é extraída pelo "Extrator de Transiente" (*Transient Extractor*). Após isto, os valores de amplitude, fase e freqüência do sinal são extraídos subsequentemente pelo "Extrator de Características" (*Feature Extractor*). Esses valores são tratados e combinados para compor as características específicas que irão definir a assinatura de cada um dos transmissores dos dispositivos móveis autorizados da rede sem fio. O "Classificador" (c*lassifier*) é usado depois para determinar a probabilidade de uma assinatura de transmissão obtida ser um dos perfis armazenados no identificador (*Feature Selection / Profile Definition*). Por último, o "Filtro Bayesiano" (*Bayesian Filter)* é aplicado para

produzir uma decisão final a respeito do estado final da análise: Normal ou Anômalo de uma assinatura de transmissão.

Por ser uma tendência recentemente explorada para a detecção de intrusos em rede sem fio, existem alguns poucos trabalhos na literatura que investigam especificamente essa abordagem [14]. Além de raros, tais trabalhos carecem de uma análise mais minuciosa de como esses mecanismos de identificação podem se integrar a outros módulos de um sistema de detecção de intrusos para ambientes sem fio.

2.8 - Considerações finais do Capítulo

Neste Capítulo, foram apresentados os conceitos básicos necessários à fundamentação da arquitetura EWIDS proposta. Foram descritas de forma resumida as principais tecnologias de rede sem fio, em especial as de alcance metropolitano com ênfase no padrão IEEE 802.16. Por estarem intimamente ligadas a arquitetura proposta, as técnicas utilizadas nos mecanismos de posicionamento de nós sem fio, bem como os principais sistemas atualmente utilizados e suas características foram introduzidos. Em seguida, os conceitos de segurança em redes foram abordados, destacando-se os Sistemas de Detecção de Intrusos, foco deste trabalho. Por ser parte integrante do IDS proposto, os principais conceitos sobre Lógica Nebulosa foram apresentados, seguidos da análise dos trabalhos relacionados. Por último, foi descrito um sistema de identificação de dispositivos por intermédio de assinatura de transmissão, que está integrado na arquitetura EWIDS proposta, através do componente IDISP.

Observam-se, em face dos trabalhos relacionados levantados, diversas lacunas deixadas pelas abordagens propostas para IDSs, que visem solucionar os problemas existentes nas redes sem fio, dentre as quais pode-se citar a ausência de:

(i) mecanismos que explorem as próprias características das redes sem fio (meio de transmissão e mobilidade);

(ii) sistemas que ofereçam baixa carga computacional devido ao problema da limitação de recursos dos dispositivos móveis.

(iii) trabalhos baseados em localizações dos nós (*Located Based*) que não apenas levem em consideração os perfis de itinerários dos usuários, mas também que observem as características cinemáticas dos dispositivos em tempo real.

(iv) esquemas que, ao contrário das propostas baseadas em perfis de usuários, necessitem uma menor quantidade de informações de cada dispositivo móvel de maneira que o IDS seja mais escalável, haja visto que as redes metropolitanas sem fio podem potencialmente possuir uma grande quantidade de dispositivos.

(v) propostas que visem a integração de abordagens distintas, como é o caso do sistema de identificação de dispositivos através de assinatura de transmissão proposto em [14].

Assim, é apresentada, no Capítulo 3, a descrição da Arquitetura EWIDS que visa preencher essas lacunas descritas anteriormente.

Capítulo 3 - Arquitetura proposta

Diferentemente dos sistemas de detecção de intrusos tradicionais, a arquitetura proposta para detecção de intrusos em redes metropolitanas sem fio [13] atém-se às peculiaridades das redes sem fio. Por isso, o EWIDS busca nas características específicas do meio de transmissão, da própria mobilidade e da tecnologia empregada, as soluções para o problema da detecção de intrusos. Apesar de considerar aspectos de tecnologia, a proposta não perde generalidade uma vez que, sendo modular, permite que facilmente sejam introduzidos outros componentes que atendam tecnologias diversas.

Outra peculiaridade da arquitetura proposta é a adoção do paradigma de proteção em camadas, que permite dotar, de forma flexível, esses tipos de redes com esquemas de defesa contra vulnerabilidades específicas dos padrões sem fio. A arquitetura EWIDS [13] tem o propósito de fornecer às redes sem fio um nível de segurança adicional em relação àqueles já existentes nos padrões sem fio. Em especial, os riscos de ataques dos tipos de Personificação (*MAC spoofing*), Homem no meio (*man-in-the-middle*) e Roubo de Sessão (*session hijacking*) são reduzidos.

Os IDS que venham a adotar a arquitetura proposta podem ser classificados como IDS do tipo *Anomaly Detection*, pois fazem uso de informações comportamentais da rede para detectar intrusos [10, 28].

Este capítulo está organizado em seis seções. Na Seção 3.1 é feita uma descrição geral da arquitetura EWIDS e de seus componentes. A Seção 3.2 apresenta a integração do mecanismo de identificação de dispositivos por assinatura de transmissão na arquitetura EWIDS. Os componentes ANAMOB (Analisador de Mobilidade) e JUIZ são detalhados nas seções 3.3 e 3.4, respectivamente. Na Seção 3.5, como estudo de caso, utiliza-se a topologia PMP (*Point to Multipoint*), sobre a qual duas formas de distribuir os componentes da Arquitetura EWIDS são estudadas e como esses componentes podem interfacear com dois sistemas de posicionamento (GPS e APRS). A Seção 3.6 finaliza o capítulo com as considerações finais.

3.1 - Descrição geral da arquitetura EWIDS

A arquitetura proposta possui alto grau de modularidade, cujos componentes possuem interfaces bem definidas que permitem suas inclusão, alteração e exclusão, sem afetar a disponibilidade do sistema, ou seja, os seus componentes podem operar separadamente e possuir implementações diferentes.

Três novos componentes são acrescentados à arquitetura clássica de um IDS de maneira que os requisitos de autenticação, irretratabilidade e controle de acesso [4], descritos no Capítulo 2, sejam alcançados em uma rede sem fio metropolitana. A integração desses novos componentes resulta na arquitetura estendida EWIDS, conforme ilustrado na Figura 3.1 onde esses componentes estão destacados com linhas mais escuras. A nomenclatura utilizada para identificação dos novos componentes foi criada no intuito de procurar intuir as suas funcionalidades, facilitando, assim, a compreensão de seus papéis.

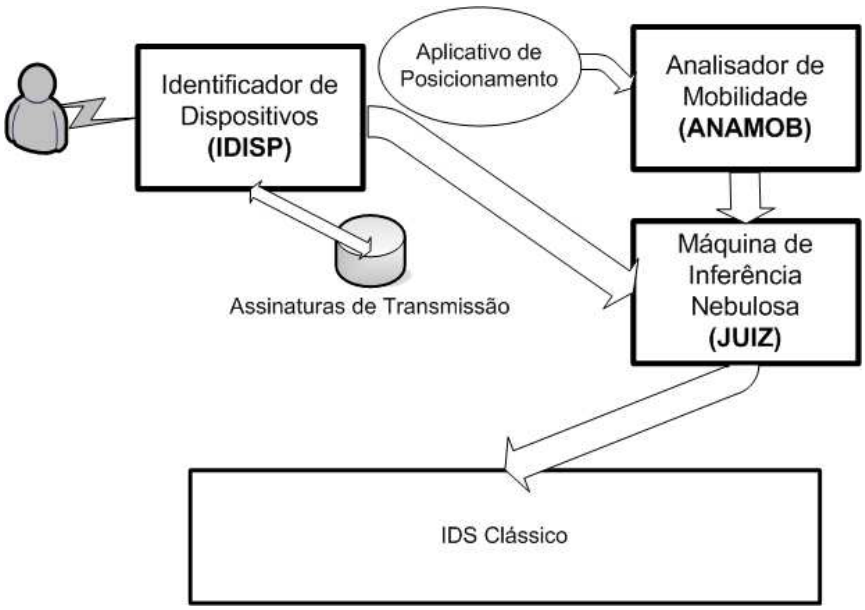


Figura 3.1. Arquitetura EWIDS proposta [13].

A EWIDS é capaz de detectar de forma ***integrada e híbrida*** as ocorrências anômalas quanto ao uso não autorizado de dispositivos (assinatura de transmissão) e quanto à localização incoerente de usuários (análise cinemática). É ***reativo***, pois, após a identificação de uma anomalia ou ataque, informa a ocorrência ao componente responsável por realizar as contramedidas na arquitetura clássica (componente IDS Clássico da Figura 3.1). É de ***monitoração contínua e em tempo real***, pois se propõe a identificar e informar o evento anômalo antes do ataque obter o

sucesso pretendido. É possível de ser usado como ***instrumento de auditoria e análise forense***, a partir do fato que os eventos podem ser armazenados em arquivos (*logs*). Os novos componentes que compõem a arquitetura EWIDS são:

- **IDISP** - Identificador de DISPositivos;
- **ANAMOB** - ANAlisador de MOBilidade; e
- **JUIZ** - uma Máquina de Inferência Nebulosa.

O primeiro componente – **IDISP** – valida o transceptor, analisando a assinatura de transmissão do dispositivo, proposto por [14]. O esquema adotado neste trabalho consiste na verificação das peculiaridades espectrais do transceptor rádio utilizado na conexão sem fio durante a fase transiente da transmissão. Assim, identifica-se 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. Essa abordagem visa se contrapor às técnicas de clonagem de equipamentos e a ataques comuns como a personificação pela falsificação do endereço MAC das interfaces de rede sem fio (MAC *spoofing*). Esse componente é um detector de intrusos que atua exclusivamente na camada física, distinguindo os dispositivos autorizados dos intrusos.

O segundo componente – **ANAMOB** – é um analisador da mobilidade para uma rede metropolitana, proposto neste trabalho, e se baseia em uma análise cinemática do movimento dos usuários. Em outras palavras, esse componente é adequado para redes onde esses usuários podem se mover dentro da cobertura de um determinado provedor de acesso sem fio metropolitano (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”, ou seja, um determinado usuário só pode estar em um único lugar no mesmo instante de tempo. Esse princípio está fundamentado nas seguintes premissas: **(i)** um usuário somente ocupa um único lugar (posição) em um mesmo instante de tempo; **(ii)** um usuário pode estar autenticado em um ou mais dispositivos móveis; **(iii)** os dispositivos móveis por “*default*”, devem estar próximos do usuário; **(iv)** as posições dos dispositivos determinam indiretamente a localização do usuário; **(v)** sendo pelo menos dois dispositivos, que possuem posições próximas entre si, são autenticados por

usuário; **(vi)** a posição de um dispositivo respeita a evolução cinemática do usuário; e **(vii)** os dispositivos devem estar dentro de uma área esperada / 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 determinação da 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 [18]. Assim, qualquer movimentação do usuário é monitorada através dos dispositivos aos quais estiver associado e, assim, esses dados de movimento (posições históricas) gerados 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 dessa 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, 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** - é responsável por correlacionar os alarmes oriundos dos outros dois componentes, sendo, portanto, o elo de integração da 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, esse componente possibilita o 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, a partir daí, ações de contramedidas defensivas, que estão fora do escopo deste trabalho, podem ser disparadas pelo componente específico da arquitetura clássica (IDS clássico da Figura 3.1). Em suma, como as informações de entrada do **JUIZ** possuem naturezas distintas na determinação de anormalidades, a análise e

integração simultânea dessas informações fornecidas por tais componentes “purificam” as decisões, aumentando a confiabilidade do sistema. Outra característica do **JUIZ** é a utilização de conceitos de inteligência computacional na implementação do componente através de uma máquina de inferência nebulosa.

Os componentes da arquitetura estendida proposta [13] devem ser inseridos fisicamente nos pontos da rede onde estão localizados os elementos de concentração, para permitir a aquisição dos dados necessários ao seu funcionamento. Isto significa dizer que não necessariamente esses componentes devem ser processados nas mesmas máquinas dos concentradores de tráfego da rede. O ideal é que estejam disponíveis máquinas dedicadas para esse fim de maneira a não deteriorar o desempenho das tarefas principais dos elementos centrais (estação base) e, ao mesmo tempo, tornar o IDS mais eficiente.

3.2 - Integração do componente IDISP na arquitetura EWIDS

Na arquitetura EWIDS, o componente IDISP possui o mecanismo de identificação da assinatura de transmissão proposto por [14], cuja descrição está no Capítulo 2, é integrado ao sistema de detecção de intrusos, através do componente JUIZ. Essa integração é, portanto, uma das contribuições do trabalho em tela e é concretizada pelo correlacionamento dos alarmes gerados por IDISP na Máquina de Inferência Nebulosa contida no componente JUIZ. Este componente exerce um papel importante na detecção de ataques de personificação, já descritos e funciona como um divisor de águas na separação de ataques de origem externa e interna. No primeiro caso, ataques externos, o IDISP contribui decisivamente na detecção dos invasores, observando-se o desempenho médio de 94% de acertos [14]. No segundo caso, ataques internos, o componente IDISP não é efetivo na detecção dos ataques, pois, nessa situação, os atacantes utilizam normalmente dispositivos autorizados, cabendo somente aos componentes ANAMOB e JUIZ as tarefas de detecção.

3.3 - Analisador de Mobilidade – ANAMOB

O funcionamento do ANAMOB fundamenta-se no controle do posicionamento dos dispositivos móveis associados a um determinado usuário e, também, nas premissas já citadas na Seção 3.1. Antes do detalhamento do funcionamento do ANAMOB, faz-se necessário introduzir os conceitos de mobilidade absoluta e relativa que nortearam a concepção desse componente.

3.3.1 - Mobilidade Absoluta e Relativa

O processo de detecção de intrusos por anomalia do movimento é conduzido sob dois focos de mobilidade: do dispositivo, o qual está sendo analisado (Mobilidade Absoluta) e do grupo de dispositivos relacionados ao um mesmo usuário (Mobilidade Relativa). Do ponto de vista de um único dispositivo, **Mobilidade Absoluta**, qualquer transmissão de dados do usuário é considerada anormal caso a sua posição geográfica seja diferente daquela **esperada** ou **provável**. As posições geográficas **esperadas** são as oriundas das variações de posição dos usuários que estão sempre conectados na rede móvel, em função das faixas de velocidades inseridas no perfil momentâneo de movimento do usuário e as suas variações de posição.

Já as **prováveis**, por sua vez, resultam do movimento imaginário, suposto ou provável do usuário, que estava desconectado ou operando em modo *idle* em algum instante anterior ao cálculo da variação do movimento. A normalidade do movimento, neste caso, é inferida de acordo com as faixas de velocidades inseridas no último perfil registrado antes de sua desconexão ou operação em modo *idle*. Para tal, é necessário registrar previamente o DATUM, última posição conhecida do dispositivo, no seu perfil de movimento que é designado de Vetor-Datum. Esse vetor contém, além do DATUM, a velocidade do dispositivo, a variação dessa velocidade, a velocidade média baseada no histórico recente do movimento, a distância total percorrida, o número de transmissões efetuadas e um registro de tempo (*timestamp)*. Vale salientar que as decisões tomadas em função do posicionamento **provável** tendem a ser menos confiáveis do que aquelas associadas ao posicionamento **esperado**, uma vez que a incerteza nos cálculos de posicionamento no último caso é menor.

Tanto no caso de posições **esperadas** quanto de posições **prováveis**, o ANAMOB cria círculos de distância dinamicamente, em torno da última posição conhecida dos dispositivos / usuário (DATUM), onde uma nova informação de posição é supostamente esperada. Em outras palavras, se o usuário estiver dentro do círculo de posição esperada ou provável (CDPE), considerando uma margem de segurança, sua transmissão ou tentativa de conexão será considerada normal. A Figura 3.2, por exemplo, ilustra a trajetória de um usuário em uma área servida por uma infra-estrutura de rede móvel e o uso do conceito do CDPE. As posições de 0 a 5 são aquelas onde o usuário realizou uma transmissão e o mecanismo de posicionamento reportou a sua localização, permitindo ao componente ANAMOB realizar a análise cinemática. Os

CDPE's criados ao redor das posições 0 a 5 são calculados em função dos perfis recentes de velocidades dos dispositivos e do tempo decorrido. Quanto maior o tempo decorrido entre duas informações consecutivas de posição ou maior a velocidade do perfil do usuário, maior será o raio do CDPE e, conseqüentemente, a sua área. Esse cálculo é feito para todas as posições (até a 5, nesse caso) recebidas pelo componente ANAMOB, durante o período de *login* do usuário. Com isto, toda posição reportada que esteja contida no interior desses círculos é julgada normal, a luz da Mobilidade Absoluta. Logo, os atacantes (indicados na Figura 3.2) posicionados fora desses círculos serão prontamente identificados em caso de ataques. Dessa forma, o conceito de Mobilidade Absoluta empregado na arquitetura EWIDS limita geograficamente a atuação dos atacantes que procuram explorar exatamente a liberdade de posicionamento oferecida pelas redes sem fio, especialmente as metropolitanas.

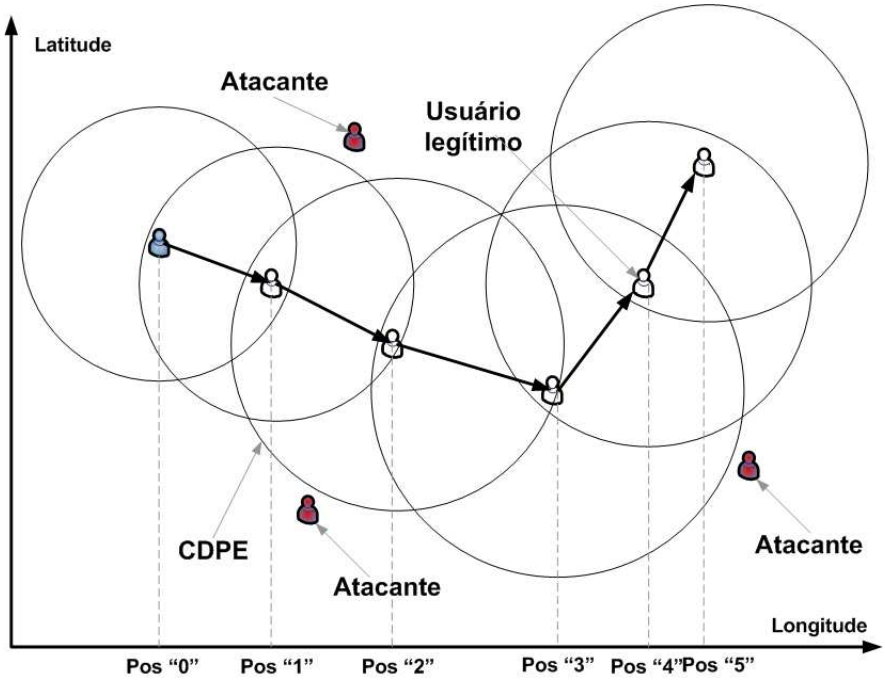


Figura 3.2. Conceito do CDPE utilizado pelo componente ANAMOB.

Do ponto de vista da **Mobilidade Relativa**, o movimento do dispositivo em análise é comparado com o movimento dos outros dispositivos associados ao mesmo usuário. Ou seja, os comportamentos cinemáticos dos dispositivos pertencentes a um mesmo grupo devem possuir um grau de compatibilidade entre si. A verificação da posição geográfica relativa do dispositivo em análise fundamenta-se no fato de que o usuário, por padrão, carrega consigo os dispositivos pertencentes a ele. Logo, é estabelecido que os dispositivos do grupo devem estar posicionados

dentro de uma distância máxima, chamada de Raio de Inclusão Aceitável (RIA), para que se tenha uma situação de normalidade. Em princípio, qualquer dispositivo afastado dos demais do seu grupo é considerado desgarrado, gerando um alarme ao componente JUIZ.

Analogamente à verificação da posição geográfica, a verificação da consistência da velocidade relativa do dispositivo em análise baseia-se na premissa de que os dispositivos do grupo estão atrelados ao usuário. Assim, as velocidades relativas recentes não podem ser muito discrepantes, sob pena de o componente ANAMOB determinar que o dispositivo em análise está em situação de anormalidade.

O emprego do conceito da Mobilidade Relativa na arquitetura EWIDS complementa a análise feita sob o foco da Mobilidade Absoluta e é especialmente interessante na ocorrência de furtos ou roubos de dispositivos e quando o usuário esquece seu dispositivo móvel em algum lugar. É ainda efetivo em situações de ataque, nos quais o posicionamento do intruso é tal que a verificação do perfil de Mobilidade Absoluta falha em detectar.

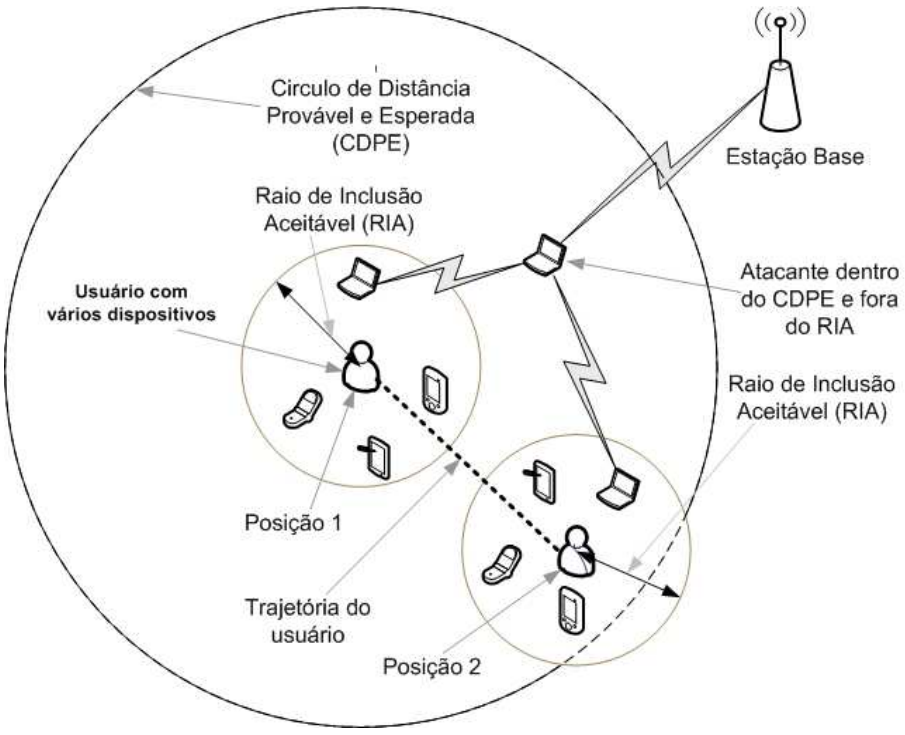


Figura 3.3. Exemplo de ataque detectável na verificação do PMR.

Neste caso, a verificação do perfil de Mobilidade Relativa, quando utilizada conjuntamente com a absoluta, torna o IDS mais eficiente, pois consegue detectar ataques em um

maior número de situações diferentes. Um exemplo desses tipos de situações é a que está detalhada na Figura 3.3. Devido à posição do atacante, esse passa despercebido na verificação do perfil de mobilidade Absoluta porque, apesar de estar parado, permanece dentro do CDPE nos dois instantes de tempo consecutivos assinalados na Figura 3.3. Contudo, esse ataque é frustrado quando da verificação do Perfil de Mobilidade Relativa, uma vez que o intruso se encontra fora do Raio de Inclusão aceitável (RIA).

Por fim, o importante na arquitetura EWIDS é se estabelecer uma relação direta entre as posições e o movimento dos dispositivos relacionados ao mesmo usuário, a fim de se constatar qualquer irregularidade em seus s de posição. Vale ressaltar que margens de segurança são consideradas nos cálculos de posicionamento a fim de se evitar excessos de alarmes falsos (Falsos Positivos).

3.3.2 - Descrição de Funcionamento

Em função dos conceitos de Mobilidade Absoluta e Relativa descritos na Seção 3.3.1, o funcionamento do componente ANAMOB pode ser visualizado através de quatro blocos funcionais, conforme detalhado na Figura 3.4. Essa organização funcional contempla os dois novos conceitos introduzidos neste trabalho: o Perfil de Mobilidade Absoluto (PMA) e o Perfil de Mobilidade Relativo (PMR), representados na Figura 3.4 através de blocos de mesmo nome.

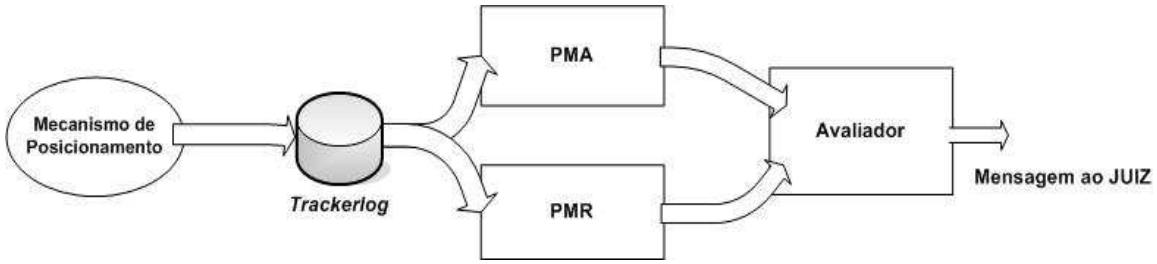


Figura 3.4. Componente ANAMOB.

O fluxo de informações e as interações entre esses componentes funcionais podem melhor ser definidos estabelecendo-se cinco fases distintas:

(1) Entrada de dados e armazenamento do aplicativo de posicionamento (*Trackerlog*);

(2) Verificação do Perfil de Mobilidade Absoluto (PMA);

(3) Verificação do Perfil de Mobilidade Relativa (PMR);

(4) Execução do Algoritmo de Decisão do ANAMOB (Avaliador)*;* e

(5) Envio de mensagem ao JUIZ (Avaliador).

Fase1 - Entrada e Armazenamento de dados do aplicativo de posicionamento

A primeira fase, **Entrada de dados do aplicativo de posicionamento**, visa introduzir no ANAMOB as informações (*input)* necessárias ao seu processamento. O tipo de aplicativo de posicionamento, que gera essas entradas, é transparente para a arquitetura e está fora do escopo deste trabalho. Portanto, para a arquitetura são importantes quatro dados oriundos da aplicação de posicionamento e que compõem o vetor de entrada: o usuário, o dispositivo, a posição geográfica e o instante referente (*timestamp*). Vale ressaltar que as informações de posição possuem erros de precisão que variam em função do tipo de mecanismo de posicionamento empregado. Esses dados são organizados cronologicamente em uma estrutura de dados (*Trackerlog*), de forma a estabelecer um histórico de posicionamento para cada usuário e dispositivo. Além disso, é possível indexar os dispositivos por usuários, com suas posições históricas (*Trackerlog).* Esses dados são armazenados para a utilização do ANAMOB ou para a realização de uma auditoria no próprio sistema.

Fase 2 - Verificação do Perfil de Mobilidade Absoluta

O bloco PMA é o responsável pelas operações da segunda fase, **Verificação do Perfil de Mobilidade Absoluta**, que consiste na verificação da normalidade da posição do usuário no foco do próprio dispositivo. É também efetuado o acompanhamento do usuário através da evolução cinemática do seu movimento. Para tal, devem-se levar em consideração três variáveis: a posição geográfica, o tempo e a velocidade. A primeira variável, no caso do sistema GPS, é dada em Latitude e Longitude. Portanto, são representadas em graus, minutos e segundos, onde 01 (um) grau possui sessenta minutos e cada minuto sessenta segundos. Sabe-se que cada minuto, sobre a superfície terrestre, representa 01 (uma) milha náutica em distância, que, por sua vez, corresponde 1852 metros. Porém, a inserção desse parâmetro (posição geográfica) carece de uma análise mais minuciosa. Por exemplo, o sistema GPS, conforme descrito no Capítulo 2, possui, devido a diversos fatores, certa imprecisão, produzindo erros nas suas medidas. No escopo do presente trabalho, esses erros têm uma influência na confecção do algoritmo que deve considerar uma margem de segurança na determinação do raio do CDPE, que é atribuído ao dispositivo. Contudo, essa margem de segurança deve ser cuidadosamente definida por causa do problema do

equilíbrio entre os índices de falsos positivos e falsos negativos. Por exemplo, a não utilização da margem de segurança implica em um grande aumento do índice de acertos ao custo de também aumentar o índice de falsos positivos. Logo, existe um ponto ótimo (*crossover error rate*) no qual se busca minimizar simultaneamente os índices de falsos positivos e falsos negativos.

A segunda variável, o tempo, é obtida no vetor de entrada (*timestamp)*. A terceira variável, a velocidade, é a razão entre a distância percorrida e a variação de tempo. A distância percorrida é calculada através da distância euclidiana entre dois pontos (diferença vetorial de posicionamento em instantes consecutivos). A variação do tempo se dá pela diferença entre os dois últimos *timestamps.*

Porém, em cenários reais as velocidades estão em constantes mudanças, com pequenas ou grandes variações, dependendo da situação. Logo, a margem de segurança empregada para o erro de posicionamento deve contemplar também as possíveis variações de velocidade, minimizando o seu impacto.

Quanto à velocidade do usuário, dois perfis são considerados neste trabalho: a pé e o automotivo. A escolha desses perfis fundamenta-se no fato de que os mesmos correspondem às formas mais comuns nas quais as pessoas normalmente se deslocam no dia a dia. Além, evidentemente, da possibilidade das pessoas poderem estar paradas em uma mesma posição.

De posse do vetor de dados de entrada (*input*), o PMA inicia os cálculos cinemáticos referentes a cada usuário / dispositivo que são executados de acordo com o *status* cronológico de posicionamento dos dispositivos no instante anterior da efetivação desses cálculos. O status é função das situações dos dispositivos em uso pelo mesmo usuário na rede e são descritos em seguida.

- Status 1 - Dispositivo novo (após a primeira autenticação) – *Trackerlog* com apenas 01 (um) registro – o que acabou de chegar;
- Status 2 - Dispositivo já autenticado e em uso normal – Registros no *Trackerlog* com seqüência contínua;
- Status 3 - Dispositivo já autenticado, mas adormecido ou desautenticado – Registros no *Trackerlog* com quebras na seqüência temporal.

Após o correto enquadramento da informação de entrada em um dos status descritos, são cumpridas as seguintes etapas no cálculo cinemático:

- recuperação do último Vetor Datum do dispositivo, salvo o Satus 1;
- determinação da distância percorrida;
- cálculo da velocidade;
- cálculo da variação de velocidade;
- cálculo do Círculo de Distância Provável / Esperado (CDPE);
- verificação - posição *versus* CDPE;
- estabelecimento do novo Vetor-Datum.

Após a obtenção dos dados do último vetor-Datum do dispositivo no *Trackerlog* durante a primeira etapa, as quatro subseqüentes são sucessivamente executadas utilizando-se as equações da Figura 3.5.

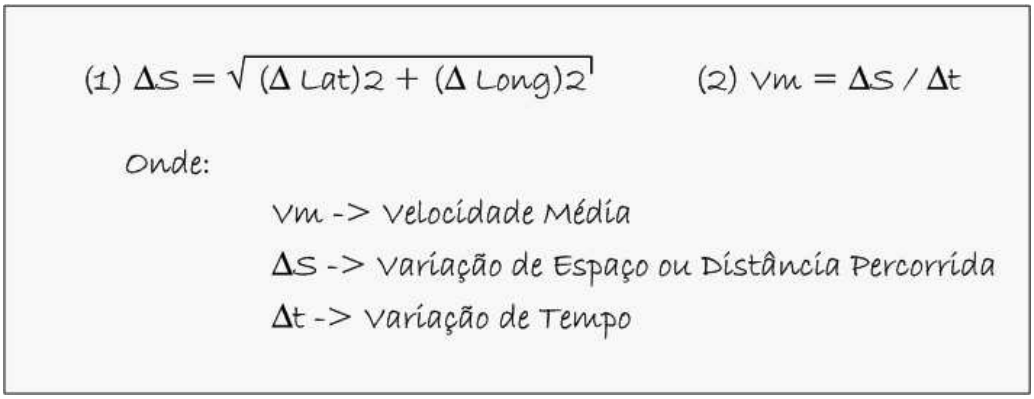


Figura 3.5. Equações do comportamento cinemático dos usuários.

Para o cálculo da distância percorrida, aplica-se a equação 1 da Figura 3.5, determinando-se a distância euclidiana entre as duas últimas posições reportadas do dispositivo. Na determinação da velocidade estimada do dispositivo aplica-se a equação 2 da Figura 3.5, sendo a variação de tempo a diferença entre os dois últimos *timestamps.* A variação de velocidade é dada pela diferença entre as duas últimas velocidades calculadas (diferença entre a atual e a histórica). Para o cálculo do raio do CDPE, efetua-se a multiplicação entre o valor da velocidade estimada para o dispositivo e a variação de tempo medida por intermédio dos dois últimos *timestamps*.

Na etapa de verificação, testa-se a validade da posição reportada, que consiste em verificar se a distância percorrida pelo dispositivo é maior ou menor do que o raio do CDPE calculado. Quanto maior for a diferença entre a distância percorrida e o raio do CDPE, mais anormal será considerada a posição reportada. Sendo essa etapa de verificação determinante no desempenho final do bloco PMA, nela é adotado um algoritmo de decisão mais elaborado que, neste trabalho, foi inspirado em uma organização similar a utilizada em um tribunal. Para a execução dessa etapa, conforme detalhado na Figura 3.6, três novos blocos, que passam a compor o PMA, são necessários: o Promotor, o Defensor e o Juiz-PMA.

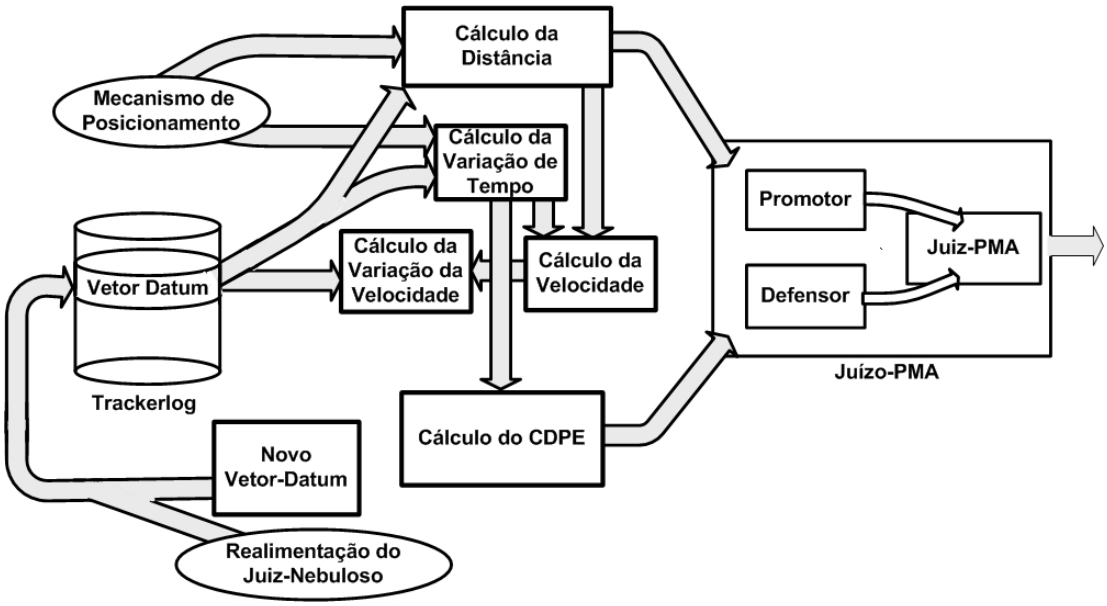


Figura 3.6. Diagrama geral do bloco PMA.

O bloco Promotor efetua a verificação da distância com o raio do CDPE de maneira direta, detectando corretamente um número maior de anormalidades (baixo índice de Falsos Negativos), porém produzindo, em contrapartida, um número maior de Falsos Positivos. O bloco Defensor acrescenta ao raio do CDPE uma margem de segurança em função da possibilidade de variações de velocidade e erros nos mecanismos de posicionamento. Esse bloco reduz o índice de falsos positivos, em detrimento do aumento do índice de falsos negativos. O bloco Juiz-PMA (Figura 3.6) integra as análises do Promotor e Defensor de modo a otimizar os resultados no tocante aos índices de falsos positivos e negativos. Além disso, o Juiz-PMA vincula sua decisão a um grau de anormalidade, cujo valor é calculado em função do número de vezes que o raio do CDPE foi ultrapassado. Quanto maior este valor mais anormal é a posição do dispositivo. Outro

aspecto importante está no fato de que existem três casos que refletem as três combinações possíveis nas análises dos resultados do Promotor e Defensor:

- Promotor e Defensor avaliam a posição como normal;
- Promotor e Defensor avaliam a posição como anormal;
- Promotor avalia a posição como anormal e Defensor como normal.

No terceiro caso, a anormalidade é atenuada pela avaliação do Defensor, ocasionando uma redução no valor calculado do Grau de Anormalidade do PMA. Essa redução influenciará a decisão final do componente JUIZ (Máquina de Inferência Nebulosa), podendo até gerar uma saída final de normalidade, conforme os outros dados de entrada.

O estabelecimento de um novo vetor-Datum para o dispositivo dependerá de uma realimentação de normalidade do componente JUIZ (saída final do EWIDS). Em caso de ser inválido, o vetor-Datum do dispositivo permanece sendo o anterior válido. A realimentação do JUIZ evita que um vetor-Datum falso seja considerado.

Fase 3 - Verificação do Perfil de Mobilidade Relativa

Na terceira fase, **Verificação do Perfil de Mobilidade Relativa**, que é executada pelo bloco PMR (Figura 3.4), comparam-se as posições de cada um dos dispositivos, relacionados ao mesmo usuário, com a posição do dispositivo em análise, em busca de possíveis anomalias entre elas. Para tal, essa fase, conforme esquematizado na Figura 3.7, é subdividida nas seguintes etapas: **(i)** Identificação dos dispositivos relacionados – Origem no *trackerlog;* **(ii)** Sincronização dos registros envolvidos e **(iii)** Comparação das posições;

Figura 3.7. Mecanismo de verificação do PMR.

A identificação dos dispositivos relacionados**, primeira etapa,** visa obter na base de dados (*Trackerlog*) os dispositivos que estão associados a um mesmo usuário. Os respectivos registros, já ordenados cronologicamente, são agrupados por usuário. A **segunda etapa**, sincronização dos registros envolvidos, tem como função ajustar as diferenças de posicionamento

dos dispositivos do grupo devido aos diferentes instantes de tempo (*timestamps*) nos quais foram realizadas as medidas de posicionamento. Assim, torna-se possível realizar as comparações (terceira etapa) de maneira mais coerente. Na **terceira etapa**, é realizado um processo de comparação (*match*) entre as posições do dispositivo em análise (referência) e as posições dos outros dispositivos do grupo, levando-se em conta as diferenças de tempo entre os registros armazenados. De posse das distâncias entre o dispositivo em análise e os outros dispositivos do grupo verificam-se quantas dessas distâncias estão contidas dentro de uma medida aceitável, chamada de Raio de Inclusão Aceitável (RIA). O critério de decisão adotado para determinar a anormalidade do dispositivo em análise foi o da maioria simples, ou seja, caso, pelo menos 50% dessas distâncias (*matches*) sejam menores do que o valor atribuído ao RIA, considera-se o dispositivo em análise em posição normal, caso contrário em posição anormal. Essa análise fornece o primeiro parâmetro que compõe o Estado do PMR.

O bloco PMR também calcula o seu próprio Grau de Anormalidade, que é o segundo parâmetro do estado do PMR. Esse parâmetro é o resultado da razão entre a média dos valores obtidos nos pares (*matches*) e a distância aceitável (RIA). Assim como ocorre na verificação do PMA, está incluído no RIA uma margem de segurança para os possíveis erros de precisão dos mecanismos de posicionamento e/ou variações de velocidades.

Por fim, os resultados gerados nessa etapa estabelecem o Estado do PMR para o dispositivo em análise (Norma/Anormal e Grau de Anormalidade do PMR) que servirá de entrada para a próxima fase (Algoritmo de Decisão).

Fase 4 - Execução do Algoritmo de Decisão do ANAMOB

Na quarta fase, **Execução do Algoritmo de Decisão do ANAMOB,** o bloco **Avaliador** (Figura 3.4) é o responsável por integrar as análises efetuadas nas verificações dos PMA (foco no dispositivo) e PMR (foco no grupo de dispositivos associado ao mesmo usuário). Submetendo-se as entradas a um conjunto de regras, obtém-se a análise final do componente ANAMOB, no tocante ao acompanhamento da mobilidade do dispositivo. Vale ressaltar que no caso de um usuário com apenas um dispositivo, apenas a verificação do PMA é realizada, sendo essa a que representará a análise do ANAMOB.

Os resultados podem indicar desde uma situação normal até uma totalmente anormal, o que sugere um gradiente nos s ao componente JUIZ. Portanto, as saídas do Avaliador são

graduais e acompanhadas de um Grau de Anormalidade do ANAMOB (GA-ANAMOB). A tabela verdade a seguir representa as possibilidades de entradas oriundas do PMA e PMR e as saídas do ANAMOB.

Tabela 1. Mecanismo de decisão do Avaliador

PMA	PMR	Saída ANAMOB	GA-ANAMOB
V	V	V	Mínimo entre GA-PMA e GA-PMR
F	V	F	Média entre GA-PMA e GA-PMR
V	F	F	Média entre GA-PMA e GA-PMR
F	F	F	Máximo entre GA-PMA e GA-PMR

A tabela 1 indica que na ocorrência de anormalidade por qualquer um dos blocos PMA ou PMR, a saída de ANAMOB, gerada pelo **Avaliador** será considerada anormal. Em contrapartida, quando há discordância entre PMA e PMR, o valor do Grau de Anormalidade do ANAMOB é atenuado, o que influenciará a análise final do EWIDS através do componente JUIZ (Máquina de Inferência Nebulosa). Portanto, as médias usadas no cálculo reduzem o valor final do GA-ANAMOB.

Fase 5 - Envio de mensagem ao JUIZ

A quinta fase, **Envio de mensagem ao JUIZ,** que, também, é executada pelo bloco **Avaliador**, constitui-se no desfecho do processo de análise do componente ANAMOB. A cada evento analisado é constituída uma mensagem que possui os seguintes campos:

- Origem
- Número de sequência
- Data/Hora - *Timestamp*
- Identificação do Usuário/Dispositivo
- Análise – Normal/Anormal; e
- Grau de anormalidade de ANAMOB (GA-ANAMOB).

A origem da mensagem é o componente ANAMOB. O número de seqüência auxilia o controle de duplicatas que possam ocorrer e ordena a seqüência de eventos. O campo Data/hora visa sincronizar o correlacionamento de eventos para o componente JUIZ. A identificação do Usuário/Dispositivo aponta a origem da anormalidade ou normalidade. O grau de anormalidade do ANAMOB além de indicar o quanto severa foi a ocorrência, revela o quão afastado ou próximo está o usuário de suas posições esperadas. Esse parâmetro pode assumir valores negativos em caso de normalidade ou positivos em uma escala crescente, no caso de anormalidade. Para cada grau de anormalidade será dado um tratamento adequado pelo componente **JUIZ**.

3.4 - Componente JUIZ

O terceiro componente (Figura 3.1) da arquitetura EWIDS, **JUIZ**, possui as tarefas de receber as informações geradas nos componentes IDISP e ANAMOB, tratá-las e correlacioná-las entre si a fim de se obter um retrato mais preciso da situação dos dispositivos autenticados na rede. Dependendo da combinação de s gerados por esses dois componentes, o **JUIZ** pode, com um maior grau de certeza, concluir entre alarmes falsos até verdadeiramente perigosos, gerando, na sua única saída, mensagens de alarmes constituídos das seguintes informações: **(i)** identidade do dispositivo, **(ii)** situação do dispositivo (normal / anormal – julgamento) e **(iii)** o grau de anormalidade (sentença). Essas mensagens podem ser utilizadas por um sistema clássico de detecção de intrusos (IDS) a fim de que esse sistema possa tomar as contramedidas necessárias de forma mais precisa e eficiente.

O componente **JUIZ** para executar corretamente suas funções se vale de dois blocos, conforme esquematizado na Figura 3.8, e também de duas entradas para receber as informações necessárias.

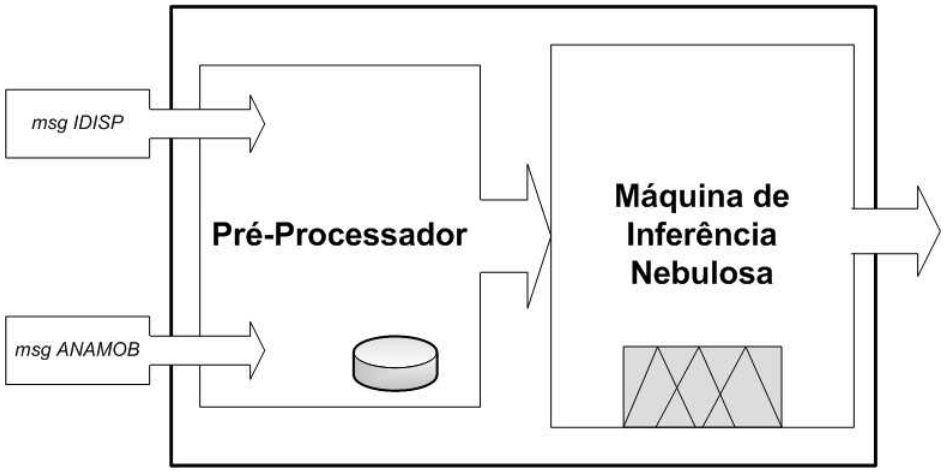


Figura 3.8. Diagrama em blocos do componente JUIZ.

A primeira entrada, aquela associada ao componente IDISP, recebe deste mensagens que são compostas por três campos, os quais se referem à autorização do dispositivo (autorizado ou não autorizado), à identidade do dispositivo (por exemplo, endereço MAC) e ao instante de chegada (*arrival time*) da mensagem proveniente do componente IDISP. Na segunda entrada, chegam as mensagens do componente ANAMOB que são compostas por seis campos, conforme já detalhado na Seção 3.3.2. A Figura 3.8 mostra que todas essas informações, tanto provenientes do IDISP quanto do ANAMOB, são primeiramente tratadas pelo bloco Pré-processador.

3.4.1 – Pré-Processador

O **Pré-Processador** é responsável por receber os s dos componentes **ANAMOB** e **IDISP** e refiná-los por intermédio de uma análise que combina informações em tempo real e informações históricas de ocorrências. O objetivo desse refinamento é o de gerar um maior número de informações que serão introduzidos na Máquina de Inferência Nebulosa. Isto permite eliminar possíveis distorções que possam ocorrer nos s isolados desses dois componentes, aumentando o grau de confiança da sua análise, na medida em que permite a constituição de um maior número de regras difusas para o bloco Máquina de Inferência Nebulosa.

A idéia de refinamento das entradas está detalhada na Figura 3.9, onde se pode constatar que as informações históricas associadas a cada dispositivo são previamente atualizadas em função das informações em tempo real advindas dos componentes IDISP e ANAMOB, antes de serem passadas à Máquina de Inferência Nebulosa. Também, está evidenciado que a Máquina de Inferência Nebulosa precisa receber as informações em tempo real.

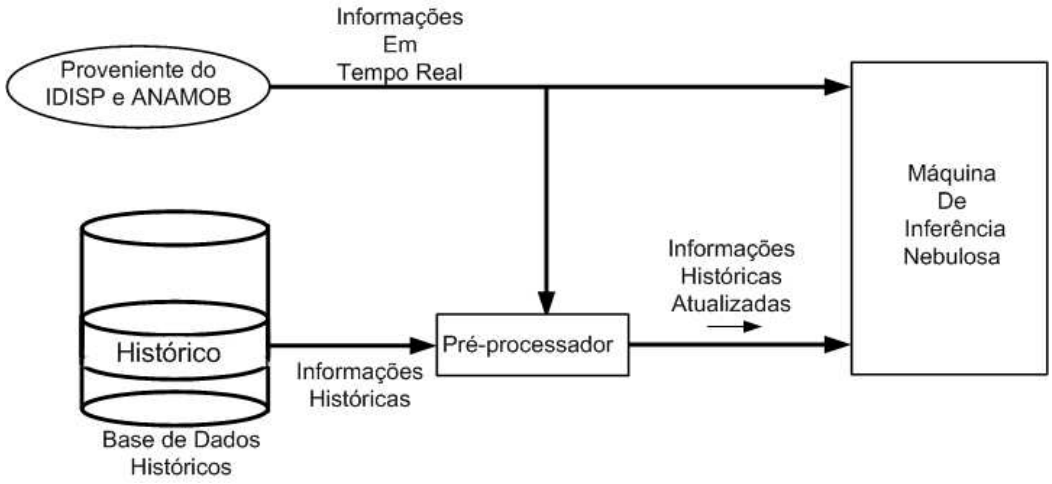


Figura 3.9. Processamento das informações.

As informações em tempo real são basicamente os dados presentes nos campos das mensagens geradas pelos componentes IDISP e ANAMOB (Seções 3.3 e 3.4). Já as informações históricas, que estão associadas a cada dispositivo e ficam armazenadas em uma base de dados, consistem em um conjunto de quatro parâmetros especialmente criados para refletir o comportamento estatístico dos resultados (decisões) dos componentes IDISP e ANAMOB. Isso propicia à Máquina de Inferência Nebulosa estabelecer critérios mais precisos para suas decisões. Os quatro parâmetros são os seguintes:

- **Índice de Alarmes gerados por IDISP** - taxa percentual de alarmes gerados por IDISP, levando-se em conta o número de alarmes sobre o total de eventos analisados;
- **Índice de Alarmes gerados por ANAMOB** - taxa percentual de alarmes gerados por ANAMOB, também se levando em conta o número de alarmes sobre o total de eventos analisados;
- **Média dos Graus de Anormalidade de ANAMOB -** média dos GA´s reportados pelo ANAMOB em um histórico recente de análises;
- **Número de Transmissões efetuadas pelo dispositivo (eventos) -** total de transmissões realizadas pelo transceptor rádio do dispositivo.

O **Índice de Alarmes gerados pelo IDISP** visa possibilitar à Máquina de Inferência Nebulosa uma análise estatística desses alarmes a fim de se inferir quanto a traços de anormalidade ou normalidade. O protótipo apresentado em [14] apresenta como resultados um

índice de acertos nas análises de 94%. Ou seja, existe um erro de análise na faixa de 6%. Portanto, por inferência, um índice de alarmes de até 6% pode ser considerado normal. Contudo, a análise conjunta de todos os parâmetros é que realmente pode determinar, com mais precisão, as conclusões.

O **Índice de Alarmes gerados pelo ANAMOB** é utilizado para se ter a medida da reincidência de alarmes do ANAMOB, que implicará em um aumento gradativo no GA (Grau de Anormalidade) final do EWIDS. Ou seja, quanto maior o índice desse alarme mais consistente fica a saída do EWIDS, reduzindo a possibilidade de ser um Falso Positivo ou Falso Negativo.

A **Média dos Graus de Anormalidade do ANAMOB** é usada com uma outra medida da tendência dos s sucessivos, podendo atenuar ou agravar os alarmes. A média deve ser a de um histórico recente a fim de representar o mais próximo possível a situação atual. A média, diferentemente dos índices de alarmes, trata com os valores atribuídos aos alarmes, possibilitando uma avaliação da severidade da anomalia. Quanto maior for o valor da média, mais “severos” são os alarmes e vice-versa.

O **Número de Transmissões efetuadas pelo dispositivo** possui o objetivo de informar a Máquina de Inferência Nebulosa se o tamanho das amostras usadas nos cálculos das métricas anteriores é pequeno ou não. Quando a amostra é pequena, as medidas ficam contidas na fase inicial do transiente estatístico, que pode interferir nas análises dos índices, gerando Falsos Positivos ou Falsos Negativos.

A Figura 3.10 detalha o bloco Pré-processador, indicando todas as entradas necessárias à Máquina de Inferência Nebulosa que constituem o seu vetor de entrada. Nas entradas, são explicitadas as origens das informações (tempo real e histórica), além de mostrar os tipos de informação utilizados nos cálculos dos quatros parâmetros das informações históricas.

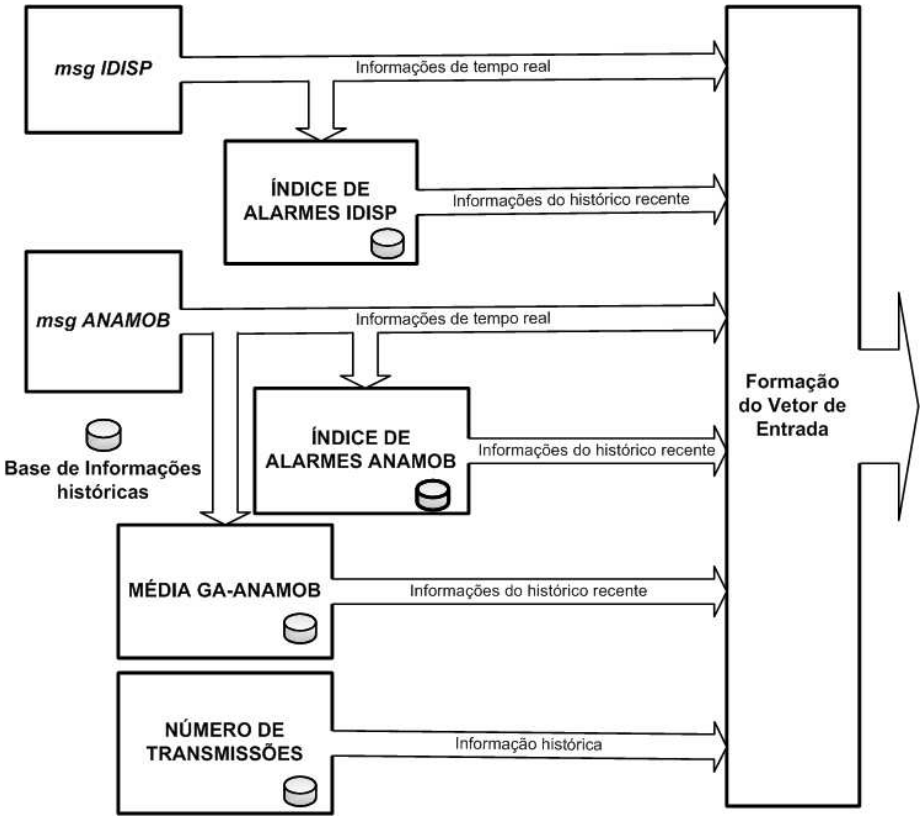


Figura 3.10. Mecanismo de Pré-Processamento de entradas.

3.4.2 - Máquina de Inferência Nebulosa

O bloco Máquina de Inferência Nebulosa é o elemento integrador da arquitetura EWIDS, recebendo as entradas já processadas pelo Pré-processador para realizar a análise final do EWIDS. Essa análise pode resultar em s de normalidade ou anormalidades (alarmes), ambos associados a um Grau de Anormalidade (GA). Esse bloco segue os princípios da Lógica Nebulosa descritos no Capítulo 2 e sua implementação está detalhada no Capítulo 4. Entretanto, o seu funcionamento, em linhas gerais, obedece aos princípios específicos descritos a seguir.

- Todas as entradas possuem duas referências comuns: um usuário e um dispositivo;
- Por ser em tempo real, as entradas são tratadas à medida que chegam;
- Por possuir uma arquitetura genérica, pode suportar diversas formas de implementações do mecanismo de decisão, inclusive outras não nebulosas.

O detalhamento das regras da máquina de Inferência Nebulosa é feito no Capítulo 4, contudo as regras genéricas, que servem de base para outros tipos de implementações, possuem as seguintes características:

- quando ambos os componentes IDISP e ANAMOB analisam o evento como normal, esse provavelmente é normal;
- quando ambos os componentes IDISP e ANAMOB analisam o evento como anormal, esse é provavelmente anormal;
- quando ambos os componentes IDISP e ANAMOB discordam em suas respectivas análises, os demais parâmetros de entrada serão decisivos na verificação final do componente.

Por fim, depois de finalizada a análise pelo EWIDS, essa é enviada ao componente de correlações e contramedidas de uma arquitetura clássica de IDS como mais um dado a ser considerado em suas análises. Essas mensagens são enviadas tão logo sejam criadas e contêm os seguintes campos de informação: Origem (EWIDS), Número de Seqüência, Alerta associado a um GA, Usuário, Dispositivo, Momento Temporal (*Timestamp*) e CRC.

3.5 - Disposição e Interfaceamento dos Componentes da Arquitetura

A disposição e o interfaceamento dos componentes da Arquitetura EWIDS foram analisados à luz da topologia PMP (*point to multipoint)*, que é normalmente adotada nos padrões de telefonia celular, de redes sem fio 802.11, 802.20 e, em especial, o padrão 802.16 que é o estudo de caso em foco.

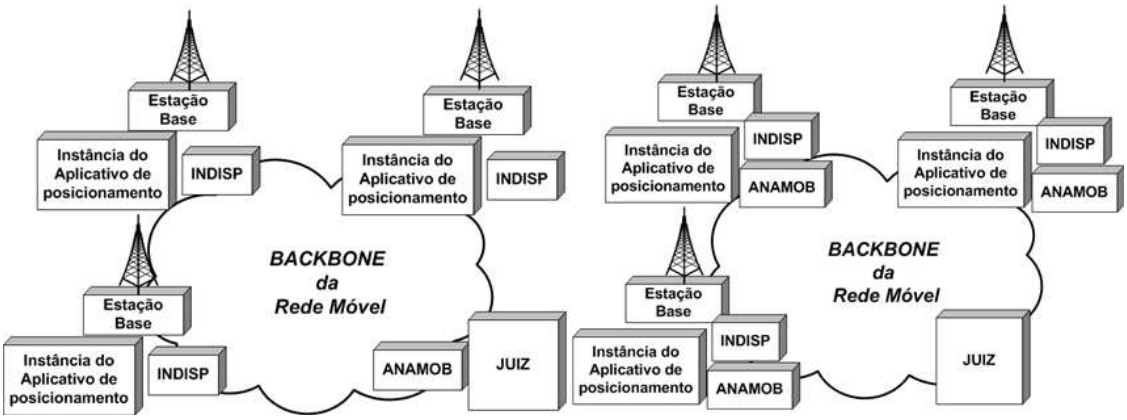
3.5.1 - Disposição dos componentes da Arquitetura

Quanto à disposição dos componentes da arquitetura proposta, tem-se, conforme esquematizado na Figura 3.11, dois cenários possíveis: (i) parcial e (ii) completamente distribuído. Nesses dois cenários, não é necessária a instalação de um sistema de comunicação especial para o envio dos dados de posicionamento oriundos dos sistemas de posicionamento e as mensagens geradas pelos componentes da arquitetura. Os *backbones* já existentes que interligam as diversas Estações Base podem ser utilizados para tal fim. Ainda nos dois cenários, é necessário que pelo menos uma instância do componente IDISP seja instalada junto as Estações Base, de

maneira que possa receber as transmissões dos dispositivos, realizar as suas análises e gerar os respectivos resultados. Entretanto, se faz necessário a sincronização das informações geradas pelos componentes da arquitetura, a fim de possibilitar o correlacionamento das mensagens que chegam ao componente JUIZ.

O cenário parcialmente distribuído, Figura 3.11.a, caracteriza-se pelo posicionamento do componente ANAMOB junto ao JUIZ em uma posição central do *backbone* da infra-estrutura da rede móvel, permitindo que as informações necessárias aos componentes sejam recebidas de todas as instâncias do aplicativo do sistema de gerenciamento localizadas em cada estação base. No cenário completamente distribuído (Figura 3.11.b), assim como ocorre com o IDISP, instâncias do ANAMOB são instaladas nas Estações Base ao invés de se ter uma única instância.

Comparando os dois cenários, o primeiro tem a vantagem de tornar o gerenciamento do sistema menos penoso devido ao menor número de instâncias distribuídas na infra-estrutura da rede móvel. Em contrapartida, devido à centralização do processamento do ANAMOB, o requisito de processamento da máquina onde é executado é maior, além de se ter um único ponto de falha, fazendo com que o sistema fique mais vulnerável. No segundo cenário, a infra-estrutura se beneficia, uma vez que os dados provenientes das diversas instâncias do ANAMOB são consolidados, propiciando uma sobrecarga de comunicação reduzida e conseqüente um menor consumo de banda. Em relação à inviolabilidade dos dados que trafegam via *backbone*, há a necessidade de se implantar independentemente do cenário utilizado esquemas de criptografia na comunicação entre os componentes da arquitetura ou entre esses e o sistema de posicionamento.



(a) Parcialmente Distribuído **(b) Completamente Distribuído**

Figura 3.11. Organização dos componentes da Arquitetura EWIDS.

3.5.2 - Interfaceamento com os Sistemas de posicionamento

O interfaceamento com os sistemas de posicionamento deve ser analisado em função da origem dos dados de posicionamento uma vez que essa origem impacta no nível de segurança do sistema. A origem desses dados pode ser o próprio dispositivo, como é o caso do GPS (*Global Position System*), ou o sistema de posicionamento como é o caso do APRS (*Automatic Position Reporting System*). Vale relembrar que os aplicativos que gerenciam os sistemas de posicionamento utilizados estão fora do escopo deste trabalho, e que a arquitetura EWIDS apenas os utiliza como entrada para o detector de intrusos.

Para o **primeiro caso** (GPS), os dados de posicionamento são gerados nos próprios dispositivos e são transmitidos juntamente com os dados das aplicações. Nesse caso, o aplicativo que gerencia o recebimento dessas informações pode possuir instâncias nas Estações Base de onde esses dados migrarão para o componente ANAMOB através de mensagens. Alguns aspectos são importantes nesse primeiro caso: **(i) Confiabilidade**, **(ii) Confidencialidade** e **(iii) Consumo de banda / processamento**. O primeiro aspecto diz respeito à garantia de que a informação de posição informada não seja falsa ou forjada. Essa preocupação está no fato de que a posição informada é feita pelo próprio dispositivo em análise, o que pode gerar dúvidas quanto a sua veracidade. Além disto, existe a preocupação de que as informações de posição possam ser alteradas, intencionalmente ou não, no percurso entre o dispositivo e o componente ANAMOB. Logo, nesse aspecto devem ser tomadas medidas que garantam que a informação passada não possa ser alterada (Integridade). O segundo aspecto diz respeito à Confidencialidade dos dados. Questões de privacidade e segurança dos usuários estão envolvidas nesse aspecto. Portanto, o tráfego dessas informações deve ser codificado com algoritmos de criptografia, a fim de prover a confidencialidade necessária. O terceiro aspecto, consumo de banda, está relacionado ao volume de mensagens de posição geradas pelo sistema de posicionamento. Porém, cabe ressaltar que neste caso o processamento é menor, pois as posições são computadas *in loco*, no próprio dispositivo.

Para o **segundo caso** (APRS), os dados de posicionamento são calculados através dos métodos descritos no Capítulo 2. Nesse caso, o aplicativo que processa e gerencia as informações de posição as envia diretamente ao componente ANAMOB através de mensagens. Realizando uma análise comparativa dos quatro aspectos tratados no primeiro caso (**Confiabilidade**,

Confidencialidade e **Consumo de banda / processamento**), o segundo caso possui algumas diferenças em relação ao primeiro. No aspecto da Confiabilidade, os mecanismos de triangulação são mais seguros, pois as informações de posição são calculadas em local onde há um maior controle sobre o processamento. Com isto, tanto as preocupações com a Confiabilidade e a Integridade dos dados ficam restritas ao trecho de rede, no *backbone* da infra-estrutura da rede móvel, onde trafegam as informações do aplicativo de posicionamento para o componente ANAMOB. Em relação ao Consumo de banda / processamento, esses são maiores do que no primeiro caso, pois são necessárias as realizações de cálculos para a determinação das posições dos dispositivos, além de que, para se realizar esses cálculos, várias informações sobre linhas de marcações devem trafegar das Estações Bases para o aplicativo de posicionamento, gerando um maior consumo de banda. Salienta-se que, nesse caso, para cada posição, espera-se pelo menos três linhas de marcação.

3.6 - Considerações finais do capítulo

Neste capítulo, foi apresentada a arquitetura EWIDS que estende as funcionalidades de sistemas de detecção de intrusos tradicionais para redes metropolitanas sem fio, baseado em uma abordagem híbrida, pois faz uso de informações de naturezas distintas para tomar decisões quanto à existência de intrusos na rede. Baseia-se, também, em componentes independentes, proporcionado, em caso de indisponibilidade de um desses componentes, que o sistema permaneça em operação, porém produzindo uma maior imprecisão nos resultados. Além disso, essa abordagem diferencia-se das tradicionais por explorar características específicas de redes metropolitanas sem fio, tais como, a **assinatura de transmissão** e **a mobilidade de dispositivos e usuários**. A arquitetura proposta, através de um esquema de detecção de anomalias sobre essas duas características, permite ao IDS estendido verificar tentativas de uso indevido na rede, identificando dispositivos não autorizados e em posições geográficas incompatíveis com o padrão cinemático dos dispositivos e usuários.

Assim, as principais contribuições do presente trabalho na detecção de intrusos são as seguintes: **(i)** utilização de informações oriundas de características específicas das redes móveis, que normalmente são fontes de vulnerabilidades, na detecção de intrusos; **(ii)** análise cinemática de dispositivos e usuários baseados em premissas intrínsecas ao uso de dispositivos móveis pelos usuários; **(iii)** estabelecimento de dois perfis para a análise cinemática - os Perfis de Mobilidade

Absoluta (PMA) e Relativa (PMR); **(iv)** o modelo utilizado no algoritmo de decisão do PMA sobre a anormalidade de posicionamento motivado nos tribunais de justiça, propiciando uma melhor análise e **(v)** integração de informações de naturezas distintas (assinatura de transmissão e mobilidade de dispositivos e usuários) empregando técnicas de lógica nebulosa com o objetivo de tornar mais eficiente o mecanismo de decisão.

A Arquitetura proposta pode ser utilizada em sistemas de detecção de intrusos militares ou oferecida como um serviço adicional de segurança para usuários interessados nos provedores de banda larga sem fio metropolitanos. Dessa forma, atende-se às questões de custo e de escalabilidade, especialmente quando tratamos de aplicações comerciais civis.

No Capítulo 4, está descrita a implementação do protótipo, onde também se detalha o ambiente e as ferramentas usados durante o desenvolvimento.

Capítulo 4 - Implementação

A fim de possibilitar a realização de testes para a validação da arquitetura EWIDS, fez-se necessária a implementação de um protótipo que pudesse ser submetido a várias simulações, com o objetivo de coletar medidas estatísticas de métricas específicas. Para possibilitar tais simulações, foi necessária também a criação de cenários apropriados que representassem algumas situações do mundo real e servissem de entrada para o protótipo. Logo, a criação desses cenários compôs, juntamente com o protótipo, a fase de implementação do trabalho em tela. Entretanto, como a composição de cenários está mais fortemente atrelada aos testes, a sua descrição foi incluída no Capítulo 5.

Excetuando a Seção 4.1, que descreve as ferramentas utilizadas, e a Seção 4.2, que detalha o esquema utilizado no desenvolvimento do protótipo, a organização das seções deste capítulo segue a mesma lógica do Capítulo 3 e, também, do fluxo natural das operações de simulação descrito na Seção 4.2. Ou seja, possui um seqüenciamento em função dos componentes da arquitetura, de seus módulos e também do esquema de controle que foi definido para executar as simulações. Então, a Seção 4.3 descreve os *Scripts* MatLab desenvolvidos que foram necessários ao controle geral das simulações. Na Seção 4.4, o Injetor de Erros de Posicionamento é apresentado. A Seção 4.5 atém-se à implementação dos componentes da Arquitetura EWIDS: IDISP, ANAMOB e JUIZ. A última Seção resume os pontos mais importantes deste capítulo com as considerações finais.

4.1- O ambiente MATLAB e as ferramentas *Simulink* e *FIS-Editor*

O ambiente *MatLab* e as ferramentas *Simulink* e *Fuzzy Inference System Editor* (*FIS-Editor*) foram escolhidos para a implementação e simulação do protótipo. A escolha do *MatLab* permitiu a integração, em um só ambiente, de todos os módulos implementados, inclusive a utilização do *FIS-Editor* para a implementação do módulo Máquina de Inferência Nebulosa do componente JUIZ. Adicionalmente, o *MatLab* possibilitou a otimização da implementação e das simulações devido aos procedimentos pré-existentes para automatização de cálculos matriciais e vetoriais, bastante úteis para o tipo de processamento necessário ao protótipo. Permitiu, ainda, a validação gradual dos diversos módulos e sub-módulos à medida que iam sendo codificados.

O *Simulink* é um pacote de *software* para modelagem, simulação e análises de sistemas dinâmicos. Para a modelagem, o *simulink* oferece uma interface gráfica com o usuário (GUI) para

a criação de modelos em forma de diagrama de blocos. Cada bloco representa uma função ou um conjunto de funções associadas que recebe o nome de subsistema. Ou seja, a modelagem é representada graficamente em diagramas de blocos em vários níveis, pois um bloco ou subsistema pode constituir-se de vários outros blocos ou subsistemas. Esses podem ser interligados diretamente ou, quando não adjacentes, através do compartilhamento de uma área de memória específica para o *Simulink*.

O *FIS-Editor* é uma ferramenta associada ao *MatLab* que possibilita a criação de sistemas nebulosos através de uma interface gráfica com o usuário. O editor possibilita a configuração dos diversos métodos utilizados nos sistemas nebulosos, a criação de variáveis nebulosas e seus respectivos conjuntos, seus formatos e semânticas, bem como a base de regras difusas a ser utilizada. A integração com o ambiente *MatLab* permite instanciar o sistema nebuloso escolhido durante a execução dos *scripts* e/ou chamadas nos modelos *Simulink.* Desta forma, o *FIS-Editor* facilita a implementação, garantindo a validação dos componentes implementados.

Além da utilização das ferramentas *Simulink* e *FIS-Editor*, foi também usado o editor de códigos do *MatLab* na confecção dos *scripts* necessários aos testes e às simulações. A linguagem utilizada nos *scripts* foi a do próprio ambiente *MatLab.* Foram implementados três *scripts*, sendo dois relacionados à geração de cenários e, o outro, ao controle geral de simulação. Sendo, este último, o responsável por iniciar as simulações e o cenário de teste, por instanciar o modelo *simulink* e a Máquina de Inferência Nebulosa, assim como por calcular as métricas para, por fim, gerar os relatórios estatísticos.

Em suma, a fase de desenvolvimento do protótipo foi dividida nas seguintes etapas:

- Concepção do esquema geral de controle das simulações;
- Confecção de três *scripts MatLab*;
- Implementação do Injetor de Erros de Posicionamento;
- Emulação do componente IDISP;
- Implementação do componente ANAMOB;
- Implementação do componente JUIZ.

4.2 - Esquema geral de controle das simulações

A razão da criação de um esquema geral para o controle das simulações advém da complexidade e quantidade de cenários de simulação e, para cada um deles, um razoável número de parâmetros a serem ajustados. Assim, a automação introduzida pelo esquema proposto na Figura 4.1 permitiu uma maior flexibilidade, confiabilidade e rapidez na execução dos testes.

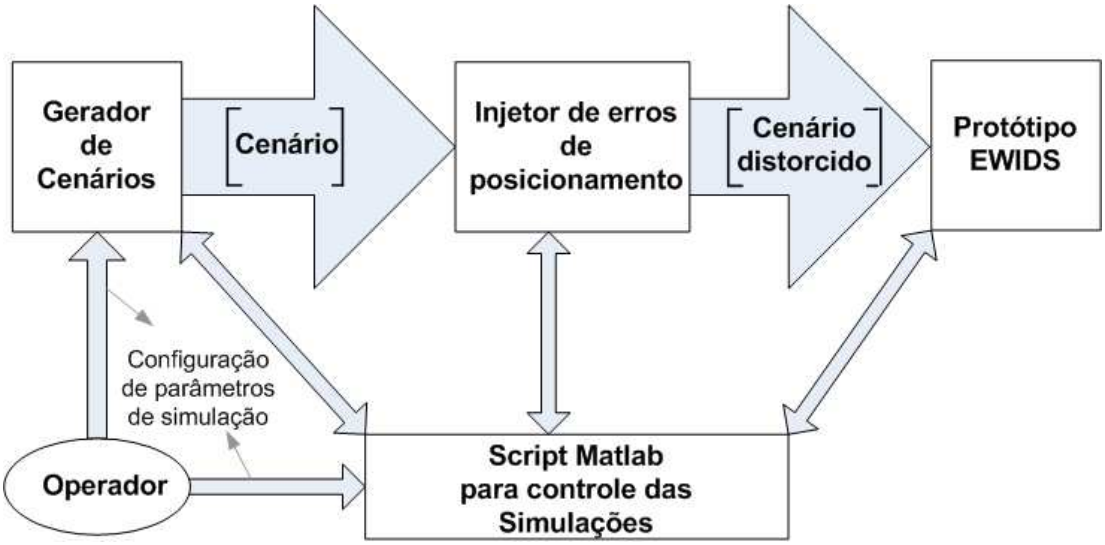


Figura 4.1. Esquema geral de controle das simulações.

A Figura 4.1 apresenta os quatro elementos mais gerais que materializam as simulações no ambiente MATLAB. O primeiro, Gerador de Cenários, cria os cenários mediante configuração dos parâmetros executada pelo operador através de uma interface gráfica, agilizando, assim, essa operação. O produto final desse módulo é o cenário, conforme esquematizado no interior da seta horizontal à esquerda do desenho que interliga esse módulo ao Injetor de Erros de Posicionamento. O cenário nada mais é do que uma estrutura de dados, mais especificamente, no ambiente MATLAB, uma matriz. Conforme mencionado no início deste capítulo, o detalhamento do Gerador de cenários foi incluído no Capítulo 5, Simulações e Análise de Resultados.

O segundo elemento, Injetor de Erros de Posicionamento, tem como funções a geração e a incorporação de erros às informações de posicionamento, que são produzidas de forma precisa pelo Gerador de Cenários. Assim, é possível, durante as simulações, verificar o desempenho da Arquitetura EWIDS diante das imprecisões (variações) de posicionamento comumente encontradas nos sistemas de posicionamento disponíveis no mercado. A razão de se ter colocado o Injetor de Erros de Posicionamento fora do Gerador de Cenário reside no fato de que esse

Gerador foi implementado por dois *Scripts MatLab* enquanto que para o Injetor foi utilizado o Simulink, pois os erros devem ser gerados em tempo de simulação.

O terceiro elemento, *Script MatLab* de Controle, coordena todo o processo de simulação, sincronizando as operações dos três outros elementos. Ele, inclusive, permite que um conjunto de cenários diferentes seja gerado em seqüência e, assim, executado pelo protótipo EWIDS.

O último elemento, Protótipo EWIDS, contempla todas as operações dos componentes da Arquitetura EWIDS, ANAMOB e JUIZ, assim como, a integração da funcionalidade do Componente IDISP à própria Arquitetura.

4.3 - Os *scripts* MatLab

Os *scripts* implementados utilizam a linguagem própria do ambiente *MatLab* e são: **(i)** um *script* para controle das simulações – *EWIDS.m;* **(ii)** um Gerador de Cenário, composto por dois códigos – *geracenario.m* e *atac_moveis.m*.

As funções do *script* para controle das simulações (*EWIDS.m)* são: **(i)** carregar o cenário a ser simulado; **(ii)** instanciar o modelo *Simulink* e a Máquina de Inferência Nebulosa e **(iii)** gerar os relatórios estatísticos da simulação em função do número de rodadas estabelecidas. O *script* de controle realiza também a inicialização de todas as variáveis necessárias ao modelo *Simulink*, recalculando-as a cada rodada de simulação. A criação de relatórios (matrizes) contendo os valores obtidos pelos principais módulos do modelo *simulink* foi de suma importância nas fases de validação e testes de desempenho do protótipo. A terceira função, geração dos relatórios estatísticos, inclui o cálculo das médias dos valores das métricas escolhidas na simulação, o cálculo dos seus respectivos desvios padrões, variâncias e intervalos de confiança.

Para o armazenamento das variáveis e arquivos, o ambiente MatLab possui basicamente três áreas de memória. A primeira delas é o **diretório *work*** onde são armazenados em disco todos os arquivos oriundos das implementações e a serem utilizados nas simulações (*scripts*, modelo *Simulink,* Máquina de Inferência Nebulosa e arquivos *.mat).* Um arquivo "*.mat"* armazena o estado de determinada variável ou grupo de variáveis após a execução de um *script,* para utilização posterior. Um exemplo de um arquivo *".mat"* são os cenários a serem rodados nas simulações (*cenario_xpto.mat*). A segunda área de memória é o ***workspace*** onde são armazenadas as variáveis inicializadas e/ou geradas nos *scripts*, em tempo de execução. Essas

variáveis contidas no *workspace* também podem ser usadas pelo modelo *Simulink*, durante as simulações, através do seu carregamento para a **área de memória do *Simulink*** e/ou escritas dessa área para o *workspace*, após o término da execução do modelo. A área de memória do *Simulink* é a terceira, e é de uso exclusivo do modelo *Simulink*. Nesse local, ficam armazenadas as variáveis carregadas (lidas) do *workspace* e as criadas em tempo de simulação. Após o término da execução do modelo *Simulink*, essas variáveis são apagadas ou podem ser salvas no *workspace*, conforme já descrito.

Durante a execução do ***script*** para controle da simulação, diversas variáveis são inicializadas. Um grupo dessas é de utilidade do próprio *script*, outras são para a utilização do modelo *Simulink* e outras são para o cálculo dos resultados estatísticos das simulações. A Tabela 1 do apêndice "I" exibe as principais variáveis e suas descrições, a fim de facilitar o entendimento das seções seguintes, onde essas variáveis são citadas.

O gerador de cenários será descrito no próximo capítulo, conforme já mencionado, juntamente com o processo de simulação e análises de resultados, por possuir uma relação direta com o tópico.

4.4 - Injetor de Erros de Posicionamento

A saída gerada por esse elemento é o cenário distorcido, conforme indicado no interior da seta à direita da Figura 4.1 que liga o Injetor de Erros de Posicionamento ao protótipo EWIDS. A natureza das informações contidas na matriz Cenário Distorcido é a mesma daquelas contidas na matriz Cenário, só que com a inclusão dos erros de posicionamento dos dispositivos. O Injetor de Erros de Posicionamento, do ponto de vista de implementação, é um módulo *Simulink* que contém um subsistema responsável por ler as entradas advindas da "matriz_cenário", criada pelo *script* Gerador de Cenários, tratá-las de forma a introduzir nas mesmas um erro oriundo da imprecisão do mecanismo de posicionamento e, desta forma, introduzir os dados para a análise do EWIDS. A Figura 4.2 mostra a implementação em *Simulink* do protótipo EWIDS e do Injetor de Erros como o produtor do cenário distorcido e suas respectivas entradas e saídas.

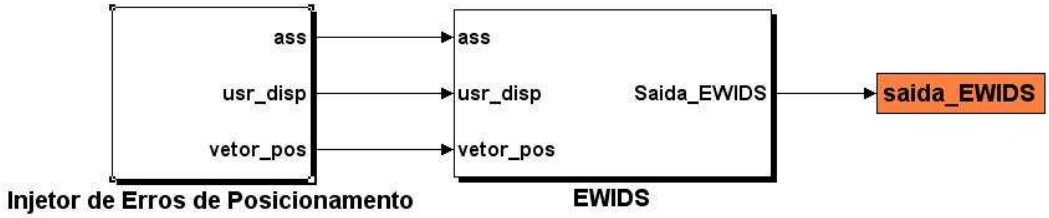


Figura 4.2 Módulos *Simulink* do protótipo EWIDS e do Injetor de Erros.

A entrada oriunda da "matriz_cenário" é carregada dentro do módulo Injetor de Erros de Posicionamento através de uma chamada da variável *"evt"* (vide apêndice "A") do *workspace* para o *Simulink,* razão pela qual a respectiva entrada não está representada na Figura 4.2. Na dinâmica da simulação, o *script* de controle realiza uma leitura linha por linha dessa matriz, sendo cada linha considerada como um evento da simulação. Essas linhas, na prática, são armazenadas na variável "*evt*", vetores compostos pelos seguintes parâmetros de uso no *Simulink:* Assinatura de Transmissão (0–Falso e 1–Verdadeiro), *timestamp*, número do usuário/dispositivo e coordenadas cartesianas do dispositivo na rede (x,y). Os parâmetros *timestamp e* coordenadas cartesianas (x, y), após serem distorcidas com a introdução do erro de posicionamento, formam a saída "*vetor_pos*" mostrada na Figura 4.2. As saídas "*ass" e "usr_disp"* são variáveis locais do *Simulink,* criadas em tempo de simulação, que armazenam os valores contidos nos parâmetros Assinatura de Transmissão e número do usuário/dispositivo, respectivamente. O protótipo EWIDS recebe essas três entradas e, após o seu processamento, retorna a variável "*saída_EWIDS"* (Figura 4.2) que corresponde a resposta do protótipo ao evento em análise.

O erro do mecanismo de posicionamento, introduzido pelo Injetor de Erros, é calculado da forma descrita a seguir.

1. obtém-se um número aleatório entre zero e o erro máximo. (Ex. 15 metros). Esse número é obtido através de uma função randômica;
2. escolhe-se um valor aleatório entre 0 e 2π (Radianos), a fim de se definir a direção da nova posição já com o erro atribuído no item 1;
3. insere-se a posição verdadeira do dispositivo (Ex. Posição cartesiana "x" e "y"); e
4. calcula-se a nova posição em função dos itens 1 e 2.

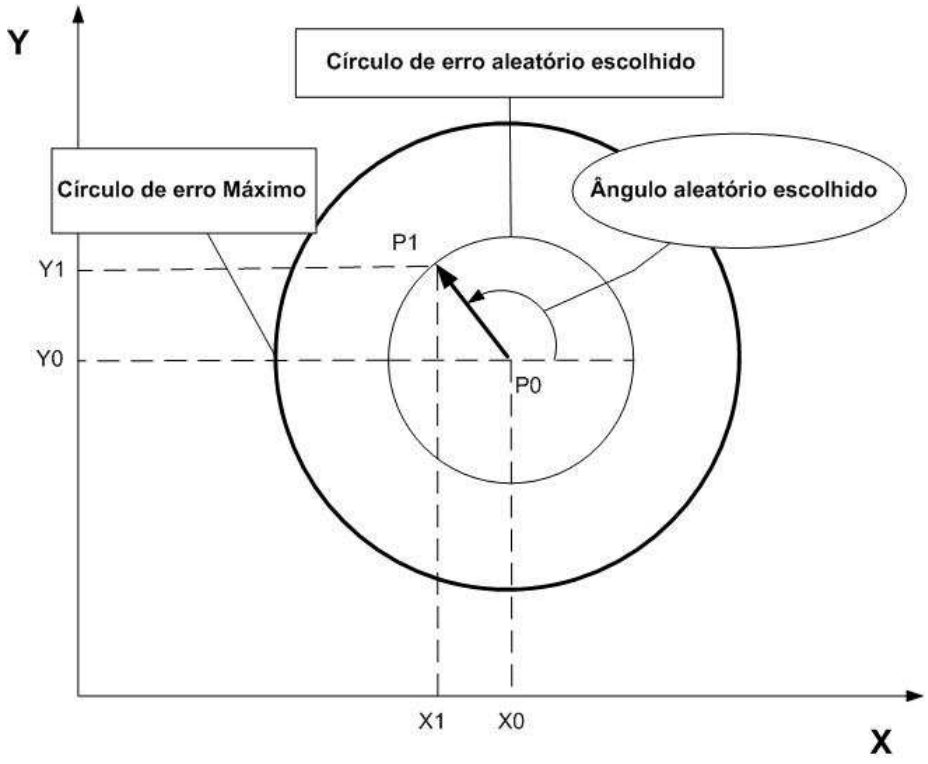


Figura 4.3. Mecanismo de atribuição de erro.

A Figura 4.3 mostra P_0 como a posição, constante na matriz cenário, inicial e verdadeira do dispositivo. A posição P_1, que é um elemento da matriz distorcida, indica a posição a ser introduzida para a avaliação de EWIDS, considerando-se o erro do mecanismo de posicionamento. Essa posição foi calculada a partir de um valor aleatoriamente escolhido entre zero e o erro máximo e o ângulo entre 0 e 2π radianos, conforme já mencionado.

Adicionalmente, o apêndice "A" contém o detalhamento do esquema utilizado na confecção do Injetor de Erros de Posicionamento.

4.5 - Protótipo EWIDS

O Protótipo **EWIDS** [13] possui todos os três novos componentes que deram origem a arquitetura estendida proposta, que são: **IDISP, ANAMOB e JUIZ**. Os dois primeiros verificam a anormalidade dos dispositivos considerando, respectivamente, a **assinatura de transmissão** do transceptor e o **comportamento cinemático** do dispositivo. O terceiro – JUIZ - **integra** as informações (*msg*_JUIZ) geradas pelos dois módulos anteriores (IDISP e ANAMOB), determinando a avaliação final do **EWIDS**, conforme descrito no Capítulo 3. A implementação desse módulo seguiu os requisitos estabelecidos na arquitetura proposta, garantindo a integridade

do protótipo. A Figura 4.4 mostra o diagrama em blocos *Simulink* do Protótipo **EWIDS**, onde estão contidos os módulos correspondentes aos componentes da arquitetura.

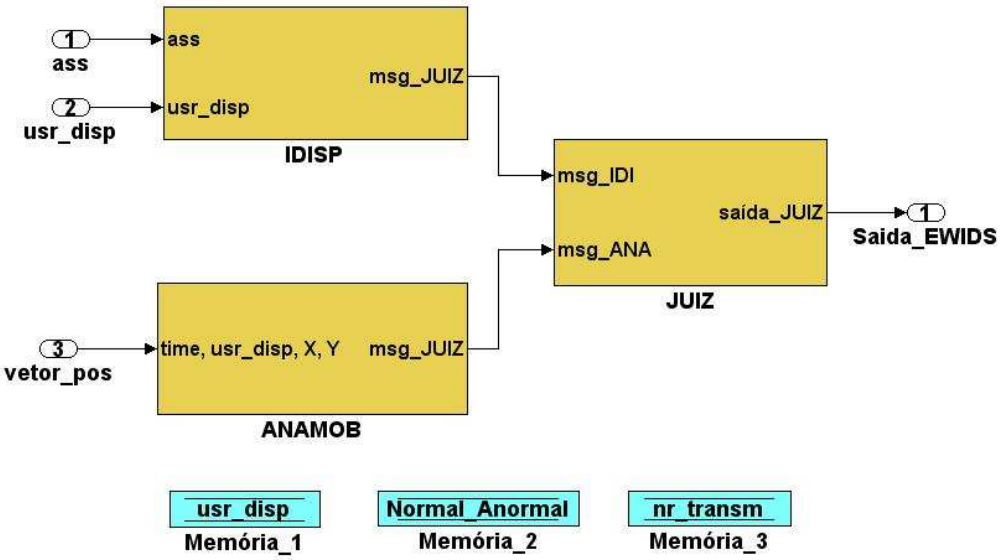


Figura 4.4. Módulos do Protótipo EWIDS.

Os blocos *Memória_1, Memória_2 e Memória_3* representam três áreas de memória reservadas pelo *Simulink* para armazenamento das variáveis nelas mostradas, para uso em tempo de simulação por outros Módulos.

Vale ressaltar que a implementação dos componentes da arquitetura EWIDS, através da ferramenta *Simulink*, se dá em vários níveis de abstração, dependendo do módulo. Por essa razão e a fim de se buscar uma maior concisão e a completude desejada, a descrição realizada neste capítulo ater-se-á aos níveis contidos nas Figuras, ou seja, até o terceiro nível de abstração. Os demais níveis, que contêm um maior grau de detalhes da implementação feita no *Simulink* estão contidos nos apêndices, citados ao longo do texto.

4.5.1 - Emulação do Componente IDISP

O primeiro componente, **IDISP,** conforme citado no Capítulo 3 é baseado no trabalho proposto em [14]. O módulo *Simulink* correspondente a esse componente emula o comportamento estatístico do mecanismo de análise de assinatura de transmissão publicado em [14], significando que a funcionalidade em si desse mecanismo não foi implementada, mas sim um módulo que gera estatisticamente os mesmo resultados que aquele. Então, esse módulo foi

confeccionado de forma que 6% das avaliações são realizadas com erros. Em outras palavras, o módulo **IDISP** possui uma precisão de 94%.

A implementação do módulo **IDISP** segue as seguintes etapas, descritas a seguir.

- Gera-se um número aleatório entre 0 e 100;
- Compara-se esse número gerado com o valor 94;
- Se o número gerado for maior, ocorre um erro, senão ocorre um acerto.

Quando ocorre um erro, o valor boleano (V ou F) da assinatura de transmissão é invertido. Ou seja, uma assinatura verdadeira passa a ser considerada falsa e vice-versa. Desta forma, simula-se estatisticamente o desempenho do componente **IDISP**, introduzindo-se os dados relativos a esse componente de maneira mais real no Módulo **JUIZ**. O apêndice "B" detalha o módulo **IDISP** no *Simulink.*

4.5.2 - Implementação do Componente ANAMOB

O segundo componente, **ANAMOB,** foi todo implementado no *Simulink* e está detalhado por intermédio do diagrama em blocos da Figura 4.5, que é um detalhamento do módulo **ANAMOB** da Figura 4.4. Esse diagrama contém, entre outros, três módulos principais especificados na arquitetura: **PMA** (Perfil de Mobilidade Absoluto), **PMR** (Perfil de Mobilidade Relativo) e **Avaliador.** Os demais módulos (*Trackerlog*, Verificador de Dispositivos Relacionados e msg_JUIZ) são auxiliares.

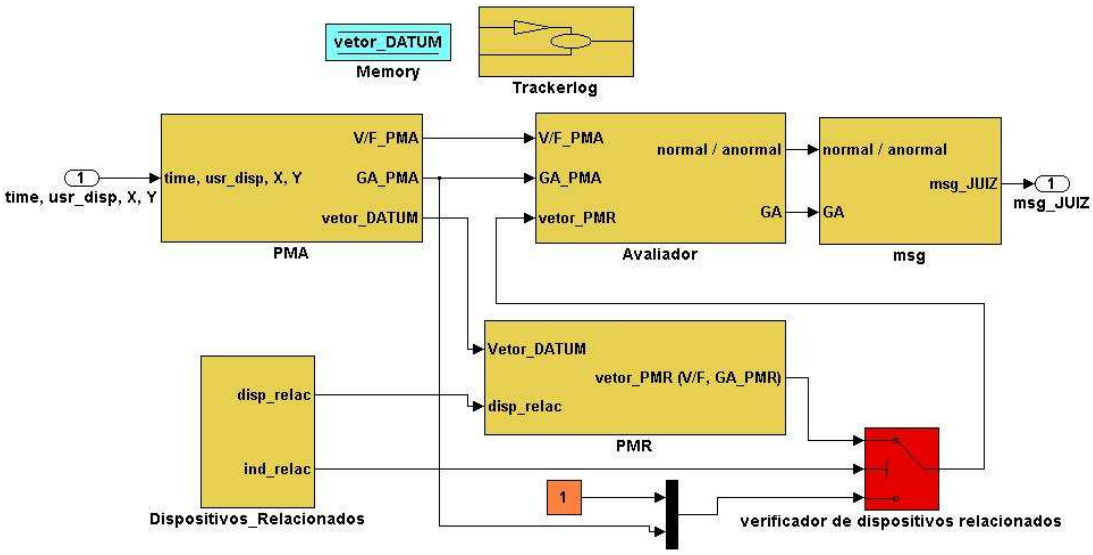


Figura 4.5. Diagrama em blocos *Simulink* do módulo ANAMOB.

Além desses módulos, foi criada uma área de memória (*Memory)*, para armazenamento do novo "vetor-Datum" calculado, a ser utilizada em tempo de simulação.

A seguir, são descritas as implementações dos três módulos principais, com suas entradas e saídas, e suas inter-relações com os módulos auxiliares.

Módulo PMA

O módulo **PMA** calcula a última posição do dispositivo, dentro do histórico de movimento do mesmo, analisando a sua coerência. Esse histórico é definido pelos parâmetros da evolução cinemática do dispositivo que vem sendo acompanhado ao longo de sua conexão. Relembrando, as posições podem ser consideradas como anormais (discrepantes) ou normais e para tais é atribuído um valor GA_PMA (Grau de Anormalidade do PMA). A especificação desse cálculo está contida no apêndice "C". 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.

O módulo **PMA** recebe como entrada um vetor com quatro parâmetros, conforme ilustra a Figura 4.5:

- *Timestamp (*"time"*);*
- Usuário e o Dispositivo a avaliar ("usr_disp");
- Coordenada cartesiana "X"; e
- Coordenada cartesiana "Y".

Além desses parâmetros, o módulo PMA carrega do *workspace* para a área de memória do *Simulink* o último vetor-Datum gravado do dispositivo contido na variável *matriz-Datum.* A localização do vetor-Datum é feita através da indexação da linha "usr_disp" da matriz. De posse desses dados, é possível a construção dos sub-módulos que representam, no protótipo, as funcionalidades especificadas na arquitetura. Desta forma, é calculada a distância entre o de posição atual com o armazenado no vetor-Datum, com a implementação do cálculo da distância euclidiana. É calculada a diferença de tempo entre os *timestamps*, a velocidade do dispositivo e a variação dessa velocidade. O raio de CDPE (Círculo de Distância Provável ou Esperado) é determinado pela informação de velocidade armazenada no último vetor-Datum e a diferença de

tempo calculada. O juízo-PMA (Promotor, Defensor e Juiz) e suas funcionalidades especificadas na arquitetura são também implementados no módulo PMA, gerando as duas primeiras saídas observadas na Figura 4.5 (V/F_PMA e GA_PMA). Ou seja, Julgamento_PMA e Sentença_PMA. Além dessas, um novo vetor-Datum é calculado para o dispositivo que será utilizado no módulo PMR, compondo, assim, a terceira saída vista na Figura 4.5. Relembra-se que esse novo vetor-Datum somente será sobrescrito na variável *ma*triz_Datum, após ser considerado normal o evento analisado. Essa nova gravação é controlada pelo módulo auxiliar *Trackerlog*, após receber uma realimentação do Juiz Nebuloso.

O detalhamento da implementação do módulo **PMA,** através de seus diversos sub-módulos, estão detalhados no apêndice "C".

Módulo PMR

O módulo **PMR** (Figura 4.5), como especificado na arquitetura, é usado quando há mais de um dispositivo relacionado ao mesmo usuário. Ele é o responsável por verificar a compatibilidade da evolução cinemática do dispositivo em análise com as do grupo de dispositivos pertencentes ao mesmo usuário. Nessa implementação, para a realização das comparações (*matches*) definidas na arquitetura, foi feita a opção pela abordagem do posicionamento geográfico e não por velocidades ou ambas. Desta forma, as distâncias relativas entre eles são então 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 (Raio de Inclusão Aceitável – RIA). Desta forma, quando há mais de 50% de dispositivos relacionados ao mesmo usuário contidos dentro desse raio, ou seja, a maioria desses dispositivos relacionados, o dispositivo em análise é aprovado no teste do **PMR**. Ou seja, a implementação do módulo visa contribuir com o propósito especificado na arquitetura, qual seja: não basta para o dispositivo possuir coerência no movimento, mas deve-se, também, respeitar a proximidade relativa entre os dispositivos do mesmo usuário. Esse módulo agrega confiabilidade ao mecanismo de decisão do componente ANAMOB (o Avaliador), pois inclui mais um parâmetro para a sua análise, como veremos mais adiante.

O módulo **PMR** recebe duas entradas (Figura 4.5): **(i)** "vetor_Datum" e **(ii)** "Disp_relac". A primeira oriunda do módulo **PMA** e a segunda do módulo auxiliar

"Dispositivos Relacionados" (vide apêndice "F"). Esse Módulo é responsável por ler duas variáveis no *workspace* (apêndice "I"). A primeira é a variável "ind_relac" que representa o número de dispositivos relacionados ao usuário portador do dispositivo em análise. Ou seja, se um certo usuário possuir três dispositivos autenticados na rede, o valor de "ind_relac" será dois. A segunda variável é uma matriz ("ind_relac" X 4), chamada de "disp_relac", que contém diversos parâmetros relacionados ao movimento dos dispositivos relacionados. Cada linha dessa matriz possui as informações de um dispositivo relacionado. As colunas contêm os seguintes parâmetros relativos a cada dispositivo: **(i)** *time;* **(ii)** "X"; **(iii)** "Y" e **(iv)** "veloc". Esses quatro parâmetros indicam em quais coordenadas cartesianas cada dispositivo relacionado estava em determinado momento (valor de *time*) e sua última velocidade calculada. O valor de *time* representa o último momento que houve um de posição considerada válida para o dado dispositivo. Vale ressaltar que os s de posição de cada um deles ocorrem em momentos distintos, e essas diferenças são tratadas no módulo **PMR.** As saídas do módulo auxiliar "Dispositivos Relacionados" são portanto as variáveis "disp_relac" e "ind_relac", conforme ilustra a Figura 4.5.

Outra característica da implementação está no fato de que o módulo **PMR** somente é executado quando existem dispositivos relacionados. Ou seja, quando o valor de "ind_relac" (tipo inteiro) é diferente de zero. Para tal, foi incluído uma função *switch* (Módulo Verificador de Dispositivos Relacionados da Figura 4.5) que desconsidera (*bypass)* o módulo quando não é necessária a sua execução. Nesse caso, o valor do "vetor_PMR" que serve de entrada no módulo **Avaliador** é o vetor **[1; GA_PMA]**, conforme mostra a Figura 4.5. Esse valor funciona como uma *flag* para o **Avaliador** que dará um tratamento adequado a esse caso. Quando há dispositivos relacionados, o módulo **PMR** será executado e retornará a sua avaliação ("V/F_PMR") e o seu Grau de Anormalidade correspondente ("GA_PMR"), formando o "vetor_PMR".

A descrição detalhada do módulo **PMR**, contendo as implementações de todos os seus sub-módulos *Simulink* está contida no apêndice "D".

- **Módulo Avaliador**

O módulo **Avaliador** (Figura 4.5) correlaciona as duas análises, **PMA** e **PMR**, gerando uma decisão final de **ANAMOB**. Para tal, o módulo recebe três entradas: **(i)** "V/F_PMA"; **(ii)** "GA_PMA" e **(iii)** "vetor_PMR", que é composto por "V/F_PMR" e "GA_PMR". Através das

combinações desses parâmetros o módulo **Avaliador** gera duas saídas: **(i)** Decisão (Normal/Anormal) e **(ii)** GA_ANAMOB. Na implementação escolhida para o protótipo uma saída do tipo Decisão será considerada como Anormal quando pelo menos um dos módulos PMA e PMR a considerar Anormal. O Grau de Anormalidade do ANAMOB (GA_ANAMOB) será função das combinações de entrada no avaliador, sendo como via de regra que quando houver uma discordância entre PMA e PMR, o GA_ANAMOB será atenuado. A descrição detalhada do módulo **Avaliador** e seus sub-módulos está contida no apêndice "E".

Módulos auxiliares *msg_JUIZ* e *Trackerlog*

Após o processamento do módulo **Avaliador,** as duas saídas resultantes (Figura 4.5) são, então, introduzidas no módulo **msg_JUIZ** para o seu posterior envio ao componente **JUIZ.** O módulo **msg_JUIZ** forma um vetor de três elementos, formados pelas duas variáveis de entrada, acrescidas da identificação do dispositivo e usuário (apêndice "F"). O módulo auxiliar ***Trackerlog*** (apêndice "F") possui a finalidade de atualizar a variável "matriz_datum", que funciona como uma base de dados contendo todos os "vetores_Datum" dos dispositivos. Essa atualização é feita sobrescrevendo a linha correspondente ao dispositivo em análise com os novos valores do "vetor_Datum" que foram calculados. Porém, essa atualização somente é concretizada após a validação do componente **JUIZ**, quando esse confirma que a transmissão do dispositivo foi considerada legítima.

Finalmente, a saída do componente **ANAMOB,** nessa implementação, é um vetor com os seguintes elementos:

- Identificação do Usuário/Dispositivo;
- Avaliação ANAMOB (Normal/Anormal); e
- Grau de Anormalidade (GA_ANAMOB).

4.5.3 - Implementação do Componente JUIZ

O componente **JUIZ** correlaciona às entradas de **IDISP** e **ANAMOB**, através de um módulo "Pré-processador" que prepara as entradas para a Máquina de Inferência Nebulosa, que é o coração do protótipo. A Figura 4.6 mostra os módulos que compõem o componente **JUIZ**.

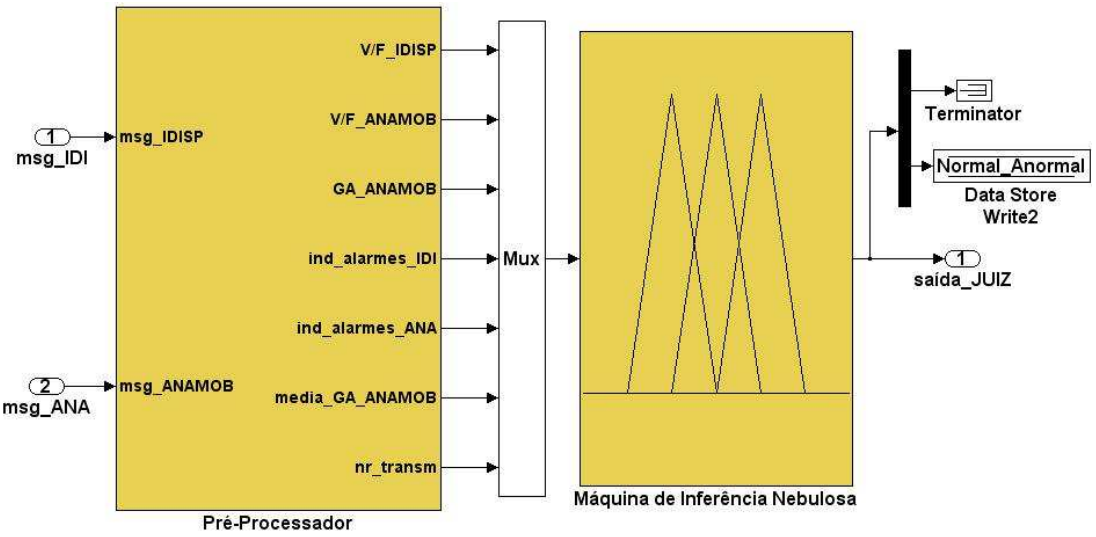


Figura 4.6. O componente "JUIZ".

Módulo Pré-processador

O módulo Pré-processador faz uso das mensagens de **IDISP** e **ANAMOB,** resultando nas seguintes variáveis: **(i)** usr_disp (Identificação do usuário e dispositivo); **(ii) V/F_IDISP; (iii) V/F_ANAMOB e (iv) GA_ANAMOB**. Além dessas, o módulo utiliza-se da variável matricial **Log** (Tabela 1 do apêndice "I") que armazena informações dos dispositivos na rede, no tocante aos seguintes parâmetros históricos: **(i) ind_alarmes_IDI** (total de eventos alarmados para o dispositivo em análise no componente IDISP); **(ii) ind_alarmes_ANA** (total de eventos alarmados para o dispositivo em análise no componente ANAMOB) e **(iii) media_GA_ANAMOB** (média dos Graus de Anormalidade reportados por ANAMOB, para o dispositivo em análise, quando o evento foi considerado anormal, isto é, **V/F_ANAMOB** igual a zero). A variável **Log** é atualizada a cada evento pelo *script* de controle, após a execução do modelo *simulink* instanciado. O último parâmetro usado pelo módulo é a variável **nr_transm** (número total de eventos – transmissões ou s de posições – produzidos pelo dispositivo em análise), armazenada na memória local do *simulink.*

O parâmetro "**usr_disp"** é utilizado apenas para identificar o dispositivo em análise, não sendo utilizado na Máquina de Inferência Nebulosa. Os outros sete parâmetros contribuem na formação do vetor de entrada da Máquina de Inferência Nebulosa chamada, a partir deste ponto, de **Juiz Nebuloso.** O apêndice "G" contém a ilustração da implementação do Pré-Processador.

Máquina de Inferência Nebulosa – Juiz Nebuloso

O Juiz Nebuloso foi implementado no ambiente *MatLab*, utilizando-se a ferramenta *FIS-Editor* que gera o arquivo *juiz.fis* (vide Tabela 1 do apêndice "I"). Conforme ilustra a Figura 4.6, parte da saída do tipo vetor do bloco correspondente ao Juiz Nebuloso é salva na memória local do *Simulink* e serve de realimentação para o módulo *Trackerlog* do componente ANAMOB.

A primeira etapa da construção do Juiz Nebuloso compreende a definição das variáveis nebulosas como também dos seus respectivos conjuntos 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. Esses testes visaram um aperfeiçoamento das saídas quanto a sua correção (Falsos Negativos) e quantidades de Falsos positivos. Na fase de testes foram implementadas várias versões da Máquina de Inferência, onde foram investigadas diversas possibilidades de implementação. Foram observados os desempenhos dos protótipos com combinações diversas de variáveis nebulosas, assim como as formas de representá-las através de vários formatos de conjuntos nebulosos. Também foram testadas várias bases de regras difusas, com diferentes combinações e quantidades de regras. Outro ponto importante foi a avaliação dos diversos métodos de "*Desnebulização"* possíveis de serem usados. Desta forma, foi obtida a Máquina de Inferência Nebulosa [13] mais adequada para o sistema. Portanto, a máquina de inferência resultante do processo de refinamento veio a possuir um total de sete variáveis de entrada e duas de saída, que são 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_ANA***, 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_ANAMOB***, sendo a média dos GA´s reportados por ANAMOB (Normal, Baixo, Média e Alta), considerada como uma outra medida da tendência dos s 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. Esses 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.
- **Sentença,** indicando o Grau de Anormalidade (GA) (Normal, Baixa, Média e Alta) associado ao julgamento.

A Figura 4.7 ilustra a interface do editor *MatLab*, contendo a representação das variáveis de entrada, da base de regras difusas e das saídas do sistema.

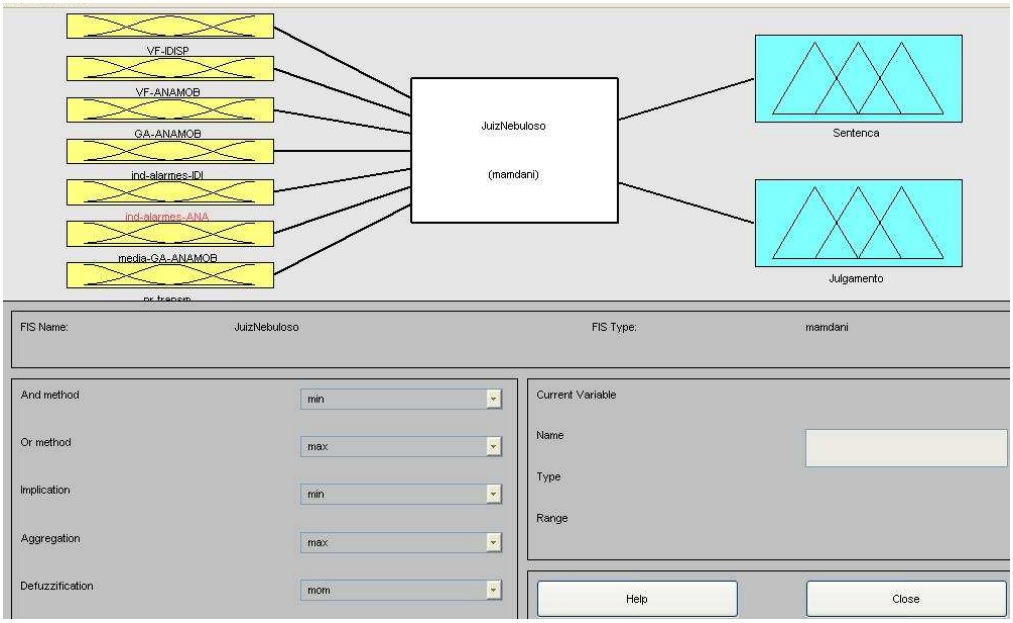


Figura 4.7. Interface do *FIS Editor* do ambiente MatLab.

A forma gráfica escolhida para os conjuntos nebulosos (trapezoidal, triangular, etc.) representa a função de pertinência do conjunto, sendo o seu rótulo o indicativo da semântica a ele associada. 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.

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 dos conjuntos nebulosos.

Desta forma, foram definidas todas as variáveis nebulosas, com seus conjuntos e semânticas. Em seguida, foram construídas as regras de inferência, que complementam 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). Disto resultam as saídas que determinam um alarme ou não, 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 podem agrupar vários rótulos adjacentes em uma mesma situação. Desta forma, o número de regras foi reduzido para um total de 110. A Figura 4.8 exemplifica duas das variáveis nebulosas contidas no sistema.

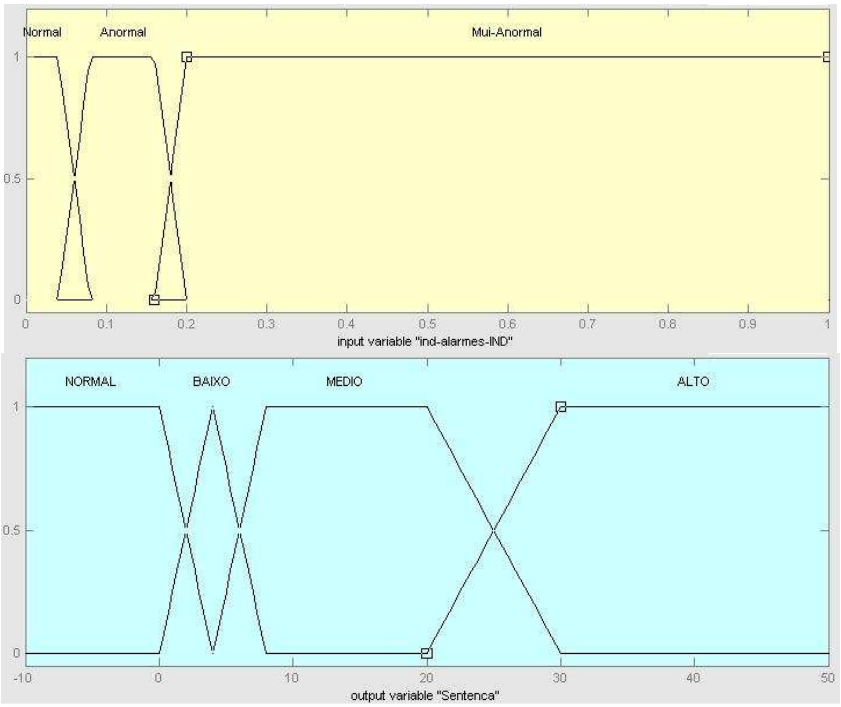


Figura 4.8. Variáveis Nebulosas "ind_alarmes_IDI" e "Sentença".

O apêndice "H" contém todas as variáveis nebulosas implementadas nesse sistema.

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. [30]

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

Por fim, 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 de regras difusas:

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

Em resumo, o processo de "*Desnebulização*" determina 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. O apêndice “H” possui a base de regras difusas e suas 110 regras.

Concluindo, 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 é atribuído um Grau de Anormalidade que pode ser Normal, Baixo, Médio ou Alto.

4.6 - Considerações finais

O Capítulo 4 apresentou uma descrição detalhada do processo de implementação do protótipo da arquitetura **EWIDS** e a infra-estrutura do ambiente necessário a execução das simulações, mostrando todas as etapas que as compuseram. A cada módulo implementado, o mesmo era submetido a testes de validações, a fim de se verificar a correção do mesmo. Várias versões foram testadas, onde eram observados os seus desempenhos, principalmente quanto aos acertos e falsos positivos. Ao final, obteve-se o protótipo a ser submetido às simulações completas.

O próximo capítulo descreve todo o processo de simulação que foi submetido o protótipo e os cenários utilizados. Apresenta, também, para cada um dos cenários, os resultados obtidos e suas respectivas análises.

Capítulo 5 - Simulações e Análises dos Resultados

Com o intuito de validar o protótipo implementado, fez-se necessário a criação de diversos cenários onde se pudesse testar, através de simulações, os componentes da arquitetura EWIDS. Esses cenários buscam representar situações o mais próximo possível do mundo real, onde estivessem contidos os principais atores, atacantes e usuários legítimos, com seus dispositivos móveis, em uma dada área de cobertura metropolitana. Por essa razão, todos os cenários gerados visam espelhar nas simulações as condições operacionais de uso das redes móveis metropolitanas, em especial, as de banda larga sem fio, similares ao padrão IEEE 802.16e (*full mobility*) [1]. Adicionalmente, foram introduzidas, nesses cenários, as informações de posição dos dispositivos, com imprecisão que normalmente é encontrada nos sistemas de posicionamento comerciais e as informações sobre as assinaturas de transmissão rádio dos dispositivos.

O objetivo das simulações é o de verificar a viabilidade da Arquitetura Estendida de IDS para redes sem fio (EWIDS) [13]. Tal objetivo é alcançado através da medição de diversas métricas e suas respectivas análises, buscando validar: **(i)** a integração do componente IDISP e o seu desempenho na presença de atacantes; **(ii)** a utilização do componente ANAMOB como um detector de intrusos eficaz, mediante a verificação da validade das premissas de mobilidade adotadas na sua concepção, em face da imprecisão de posicionamento normalmente presente nos sistemas de posicionamento encontrados atualmente no mercado e **(iii)** a eficácia do protótipo EWIDS, em particular, a correção das saídas geradas pelo componente JUIZ, elemento integrador da EWIDS.

Para tal, este capítulo está organizado em cinco seções. A Seção 5.1 define a metodologia utilizada nos testes e o tratamento estatístico adotado. O módulo Gerador de Cenários que foi previamente introduzido no Capítulo 4 e os cenários selecionados para os testes estão detalhados na Seção 5.2. A Seção 5.3 descreve os testes efetuados no protótipo assim como apresenta os respectivos resultados e suas análises. A Seção 5.5 finaliza o capítulo apresentando as considerações finais.

5.1 Metodologia

A metodologia empregada nos testes buscou verificar quantitativamente o desempenho da arquitetura de IDS proposta. Para tal, foram criadas as seguintes métricas [10, 28, 29] descritas a seguir.

(i) Percentual de atacantes descobertos (% AD) – 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. Essa métrica refere-se somente as saídas do componente JUIZ;

(ii) Percentual de Alarmes Corretos (% AC) – número de alarmes corretos sobre o total de transmissões atacantes;

(iii) Índice de Falsos Negativos (% FN) – total de transmissões atacantes não identificadas sobre o total de transmissões atacantes. Essa métrica é o complemento da anterior (% AC);

(iv) Índice de Falsos Positivos (% FP) – total de alarmes falsos sobre o total de alarmes;

(v) Índice de acertos com Graus de Anormalidade Alto (% GA-Alto) – total de alarmes com grau de anormalidade alto sobre o total de alarmes**;**

(vi) Índice de acertos com Graus de Anormalidade Médio (% GA-Médio) - total de alarmes com grau de anormalidade médio sobre o total de alarmes**;**

(vii) Índice de acertos com Graus de Anormalidade Baixo (% GA-Baixo) - total de alarmes com grau de anormalidade baixo sobre o total de alarmes**;**

(viii) Percentual de Alarmes Corretos em ANAMOB (% ANAMOB) - número de alarmes corretos gerados por ANAMOB sobre o total de transmissões atacantes;

(ix) Percentual de Falsos Positivos em ANAMOB - total de alarmes falsos gerados por ANAMOB sobre o total de alarmes**;**

(x) Percentual de Alarmes Corretos em IDISP (% acertos IDISP) - número de alarmes corretos gerados por IDISP sobre o total de transmissões atacantes;

(xi) Percentual de Falsos Positivos em IDISP - total de alarmes falsos gerados por IDISP sobre o total de alarmes**.**

Para que os valores obtidos para cada métrica pudessem ter uma relevância estatística, foram calculados as médias, os desvios padrão e os intervalos de confiança, observando um limite de confiança de 95%. Esses parâmetros estatísticos foram obtidos em 50 rodadas de simulações para cada cenário, com o intuito de obter intervalos de confiança aceitáveis. Esse número de rodadas foi também escolhido a fim de seguir a mesma metodologia adotada em [14].

5.2 - Cenários de testes

Devido ao número relativamente elevado de cenários e, para cada cenário, um número grande de eventos, foi necessário implementar o Módulo Gerador de Cenários, pois a sua execução manual tornar-se-ia impraticável. A interação desse módulo com os outros elementos e ferramentas que compõem o ambiente de simulação está descrita no Capítulo 4.

Assim, a Seção 5.2.1 detalha o Módulo Gerador de Cenários. Já na seção 5.2.2 são apresentados os cenários escolhidos para as simulações, juntamente com as respectivas justificativas.

5.2.1 – Módulo Gerador de Cenários

Inicialmente, para a criação de cada cenário, 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 necessários, como, por exemplo, a presença de atacantes e perfis de mobilidade e **(ii)** gera *waypoints* (pontos intermediários no percurso) muito distantes quando em cenários metropolitanos, não simulando as características de um mecanismo de posicionamento real. O uso do *setdest* se mostra eficaz quando simulamos redes locais sem fio (WLAN) ou redes de sensores sem fio (RSSF). Logo, se fez mister a criação de um gerador de cenários adequado para esse trabalho e que foi implementado através de dois *Scripts MatLab*. O primeiro executa os procedimentos para a criação de todos os tipos de cenários enquanto o segundo só é executado quando se deseja dotar os atacantes com mobilidade.

O **Gerador de Cenários** 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 desses parâmetros, o algoritmo escolhe aleatoriamente as posições iniciais dos usuários e dos atacantes e gera o movimento dos mesmos dentro da área criada. Os

atacantes podem ser estáticos ou dinâmicos, os quais estão representados na Figura 5.1 que mostra um cenário ilustrativo produzido pelo Gerador de Cenários.

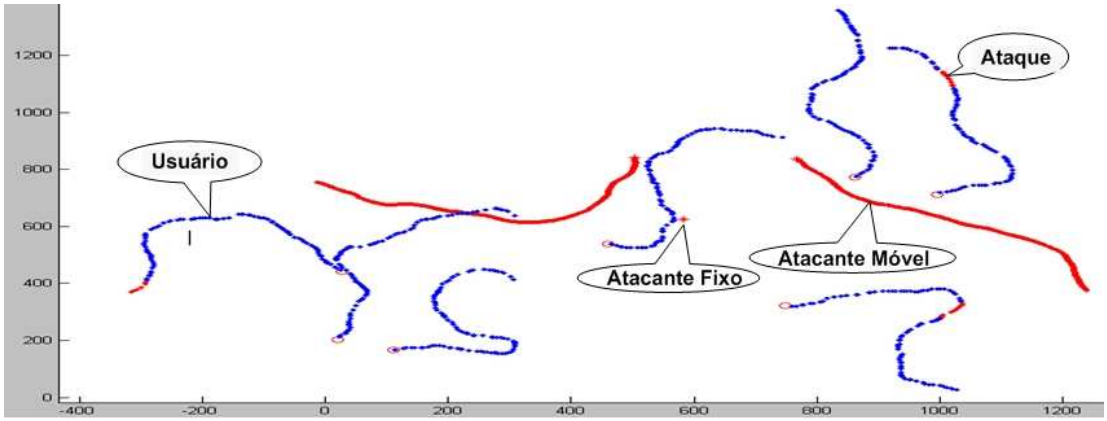


Figura 5.1 - Cenário ilustrativo gerado com sete usuários e três atacantes.

A saída do gerador é de fato o cenário a ser introduzido na simulação (módulo injetor de Erros). Na prática, a saída é uma variável *cenário.mat*, do tipo matriz Nx6, sendo "N" o número de eventos (linhas da matriz) do cenário. Cada evento está associado a um dispositivo e representa uma de suas transmissões com um de posição do mecanismo de posicionamento. As colunas desta matriz contém as seguintes informações: 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). A Tabela 2 representa parte de uma matriz-cenário exemplo, que está relacionado ao cenário da Figura 5.1.

O número do usuário/dispositivo, mostrado na coluna 3 da Tabela 2, possui a identificação do usuário e do dispositivo a ele relacionado. A casa das unidades representa o número do dispositivo, indicando que o Gerador de Cenários pode criar cenários com até 9 dispositivos por usuário. As demais casas (dezenas, centenas, etc.) representam o número do usuário.

Tabela 2 - Matriz cenário.

Ass.	*Time stamp*	Usr/ Disp	X	Y	Gab.	Ass.	*Time stamp*	Usr/ Disp	X	Y	Gab.
1	0	10	26,335	442,57	0	...	...	...	...	...	...
1	0	20	749,3	320,97	0	0	153,79	20	336,68	614,33	1
1	0	30	111,2	167,52	0	1	154,71	70	787,73	1026,2	0
...	...	...	...	...	...	1	155	50	17,769	485,01	0
1	0,65722	70	862,82	775,44	0	1	155,21	70	787,76	1027,3	0
1	1,566	60	464,84	537,54	0	1	156,09	50	17,624	487,33	0
1	2,4601	30	114,18	167,73	0	0	156,11	20	332	614,11	1
1	2,776	40	1000,7	718,33	0	1	156,31	10	157,39	631,04	0
1	3,186	10	23,959	447,53	0	1	156,63	60	532,83	760,01	0
1	3,7603	20	760,35	320,01	0	1	157,58	40	1043,2	915,39	0

5.2.2 – Cenários de simulação

A fim de possibilitar a execução das simulações, fez-se necessária a criação de cenários que buscassem aproximar os testes a situações específicas do mundo real.

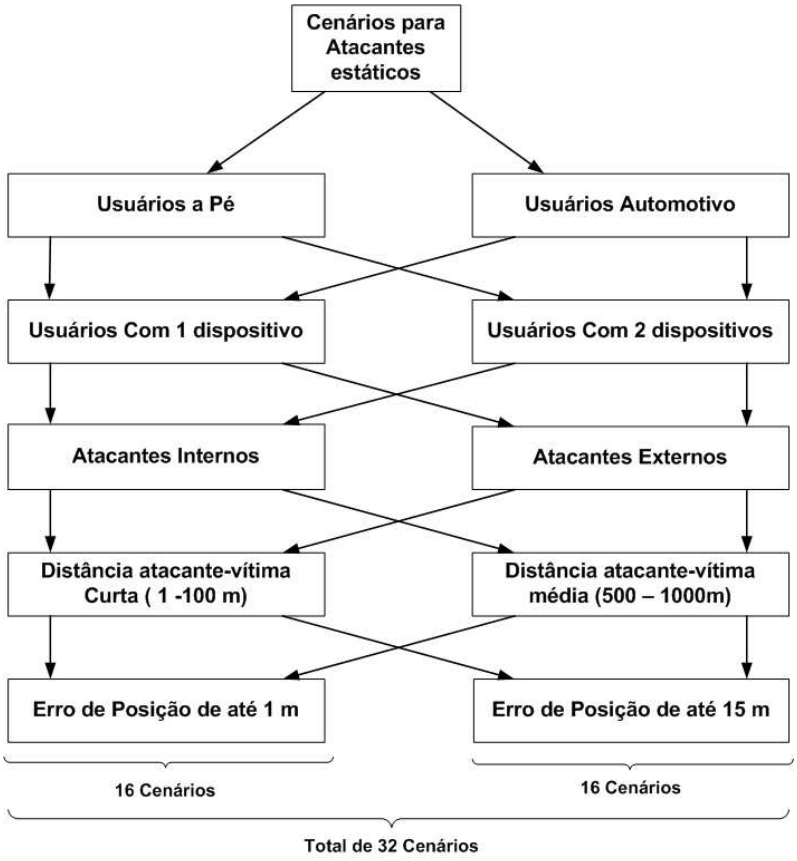


Figura 5.2 – Diagrama de formação de Cenários de Simulação.

Para tal, os 32 cenários (Figura 5.2) gerados representam a combinação das seguintes classificações criadas: **(i) Perfil de Mobilidade do usuário** – A pé ou Automotivo Urbano; **(ii)**

Número de dispositivos por usuário – 1 ou 2 dispositivos; **(iii) Origem do Ataque –** Externa ou Interna; **(iv) Distância Atacante-Vítima** – Curta ou Média e **(v) Precisão do Sistema de Posicionamento** – até 1 ou até 15 metros.

Cada cenário foi configurado com a presença de 150 usuários legítimos e 30 atacantes. Como cada atacante escolhe uma vítima, dos 150 usuários, 30 são atacados em algum momento durante a geração do cenário. O número escolhido de atacantes visa tornar os resultados estatísticos da métrica de Atacantes Descobertos (AD) mais confiáveis e estáveis, pois quanto maior o tamanho da amostra mais representativa ela é do universo amostrado. Ressalta-se que o número total de dispositivos pode ser de 150 ou 300, dependendo da relação de dispositivos por usuário (1 ou 2, respectivamente). Esses totais influenciam diretamente o tamanho do cenário criado (tamanho da matriz-cenário), na medida em que incorre em um maior número de transmissões totais (Linhas da matriz-cenário).

A Figura 5.3. mostra um cenário, que foi utilizado nas simulações, com 300 dispositivos, 30 atacantes e com distâncias curtas entre atacante e vítima.

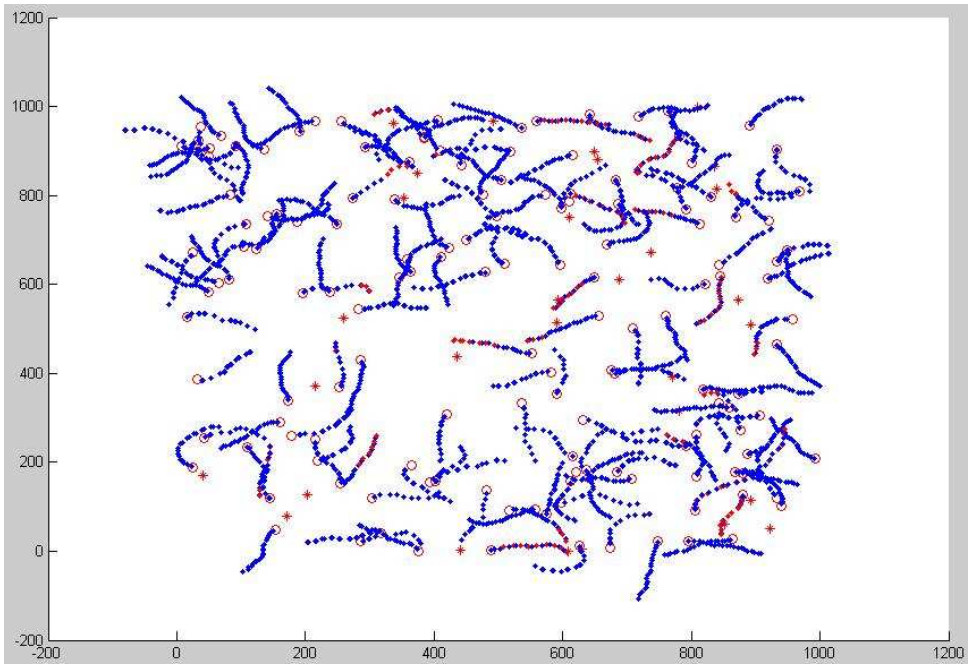


Figura 5.3. Cenário com 300 dispositivos e 30 atacantes – Distâncias Curtas.

Para as simulações, foi estabelecido um limite de onze transmissões por dispositivo, sendo a primeira aquela que contém a posição inicial de cada um deles. A razão do

estabelecimento, nesta versão, de 11 transmissões por dispositivo se deveu a limitação da capacidade da estação utilizada para as simulações e ao tempo de simulação. Assim, considerando as 11 transmissões por dispositivos, os cenários com 150 dispositivos (um dispositivo por usuário) possuem matrizes-cenário com tamanho de 1650 linhas e os que contêm 300 dispositivos (dois dispositivos por usuário) matrizes-cenário de 3300 linhas. Isso significa que, durante o processo de simulação de um cenário, com 50 rodadas e matriz-cenário com 3300 linhas, por exemplo, o EWIDS analisa 165000 eventos, discernindo entre a legitimidade ou não de cada uma das transmissões representadas pelas linhas da matriz-cenário.

A diferença do número de eventos entre os diversos cenários (1650 e 3300 eventos) influencia nos índices de Falsos Positivos (FP). Essa diferença foi propositalmente estabelecida, sendo de suma importância na análise das variações de FP do componente JUIZ (Saída do EWIDS), diante de amostras de tamanhos diferentes, no intuito de comparar a sua estabilidade (FP) com as dos demais componentes (ANAMOB e IDISP) que não empregam os conceitos inerentes à lógica nebulosa. Esse fenômeno no comportamento do índice de Falsos Positivos está detalhado na Seção 5.3, onde é apresentada a análise dos resultados.

Justificativas das escolhas das classes

Os **perfis de mobilidade do usuário** visam investigar o desempenho do EWIDS diante de dois perfis mais comuns de locomoção dos usuários. Os valores das velocidades escolhidas para os cenários a pé (1 a 3m/s) e automotivo (7 a 17m/s) representam as faixas normais de valores nesses perfis, observando que, no caso automotivo, essa velocidade representa valores para uma situação urbana. No caso a pé, os valores de velocidade foram determinados por observações feitas em situações reais. Para o perfil automotivo urbano, as médias de velocidades consideradas estão contidas na faixa permitida para veículos, no interior de um perímetro urbano, pelos órgãos competentes (25 a 60 Km/h aproximadamente).

O **número de dispositivos por usuário** tem uma forte influência no desempenho da EWIDS devido à abordagem de análise cinemática considerando o movimento relativo dos dispositivos pertencentes a um mesmo usuário. Assim, com o intuito de analisar o desempenho da EWIDS e do ANAMOB, quando ativa o módulo PMR (Perfil de Mobilidade Relativa), foram estabelecidos usuários possuindo 1 ou 2 dispositivos. A razão dessa escolha é por essa ser a

situação mais crítica, pois quanto maior o número de dispositivos associados a um mesmo usuário, maior é a eficiência na detecção de intrusos.

A **origem do ataque** estabelece dois tipos de atacantes: os externos e os internos. Os atacantes externos possuem dispositivos com assinaturas de transmissão não cadastradas. Já os internos, ao contrário, utilizam dispositivos com assinaturas cadastradas. Tal diferenciação é feita durante o processo de geração dos cenários, atribuindo-se um *bit* correspondente a cada tipo, nas transmissões dos atacantes. Relembra-se que para os atacantes externos o componente IDISP contribui no aumento da taxa de detecção, pois identifica como verdadeiras as assinaturas dos dispositivos atacantes em 94% das vezes. Porém, vale ressaltar que o desempenho de 94% do IDISP relaciona-se à identificação dos dispositivos, de acordo com [14], e não de atacantes. Ou seja, os 6% de erro nessas identificações possuem, como está descrito nos resultados, um significado diferente quando as estatísticas de Falsos Positivos do módulo IDISP são analisadas separadamente. Esse percentual de erros implica em uma quantidade de alarmes falsos que faz aumentar significativamente o índice de Falsos Positivos do IDISP. Exemplificando, para atacantes externos, em um universo de 3000 transmissões analisadas, sendo 200 de atacantes, o IDISP identificará em média 188 transmissões atacantes, por serem dispositivos não cadastrados. Os Falsos Negativos são representados pelas 12 transmissões não detectadas. Todavia, os 6% de erros representam, também, que das 2800 transmissões legítimas, 168 serão consideradas falsas (Alarmes Falsos), significando 47,2% de Falsos Positivos ([168/[168+188]]*100). Esse problema é tratado na integração do módulo ao EWIDS, através de sua máquina de inferência nebulosa (JUIZ), o que pode ser constatado nos resultados.

Outro fato importante, é que 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. Porém, nesses cenários, o componente IDISP não contribui de forma decisiva na detecção dos atacantes, pois esses se utilizam de dispositivos cadastrados. Este é, portanto, o pior caso, cabendo ao componente JUIZ avaliar as anomalias pelos s de ANAMOB.

A **distância entre o atacante e a vítima** tem, também, forte impacto no desempenho da Arquitetura EWIDS, uma vez que, como essa baseia o seu funcionamento no posicionamento dos

dispositivos, é intuitivo concluir que quanto mais perto está um atacante de sua vítima mais facilmente esse atacante pode ser confundido com um usuário legítimo. Foram, então, definidos dois ***padrões de distâncias***: Curta (1 a 100m) e Média (500 a 1000m). Observa-se que não foram necessárias simulações com cenários de longa distância (acima de 1000m), pois os cenários com distâncias médias são conclusivos para distâncias maiores, como veremos mais adiante. O momento do início do ataque é escolhido aleatoriamente, aumentando a dificuldade da detecção. Além disso, em geral, o comportamento de um atacante real é o de não revelar a sua identidade quando executa um ataque. Portanto, um atacante procura se passar por outros usuários através da interceptação do sinal de transmissão do dispositivo legítimo e sua respectiva substituição pelo sinal do atacante. Em suma, durante um ataque as posições do usuário legítimo são substituídas pelas posições dos atacantes no cenário. As intenções finais dos atacantes são indiferentes ao sistema. Com isto, o cenário a ser usado no processo de simulação contém a informação de **assinatura de transmissão** e de **posição de cada dispositivo** ao longo de determinado período de tempo, simulando o movimento de todos os atores (usuários e atacantes) dentro de uma cobertura metropolitana.

A **precisão do sistema de posicionamento** pode também levar a EWIDS a decisões errôneas sobre eventos suspeitos na rede móvel, tornando-se um parâmetro vital na verificação da eficácia da Arquitetura EWIDS quanto à detecção de intrusos. As imprecisões de posições introduzidas nos cenários (Tabela 2) são feitas em tempo de simulação pelo módulo Injetor de Erros, descrito no Capítulo 4. Isto significa que as coordenadas de posições expressas nos cenários gerados representam à localização exata que o dispositivo está em determinado instante. Como mencionado, neste trabalho, foram inseridos os erro de precisão de um sistema GPS comercial comum que varia de 0 a 15 metros [18]. Porém, alguns equipamentos oferecem uma precisão maior (DGPS), o que, para aplicações militares, por exemplo, significa uma precisão de até 1 metro. Dessa forma, é possível verificar o desempenho da EWIDS diante dessas duas imprecisões de posição.

O **perfil de mobilidade dos atacantes**, que define atacantes do tipo estático e dinâmico, também poderia ter sido considerado como a sexta classe de cenário, o que elevaria para 64 o número de cenários (6 classes: $2^6 = 64$). Entretanto, normalmente, o atacante se movimenta na fase passiva do ataque (monitoração – Ex. *warchalking e wardriving*) e fica estático na fase ativa (Ex. *Hijacking e man-in-the-middle*), para não se distanciar da vítima e evitar procedimentos de

handoff entre células o que poderia dificultar o seu ataque. Então, foi definido que os cenários de simulações contemplariam somente as situações referentes a atacantes estáticos.

5.3 Resultados Obtidos e Análises

Conforme descrito anteriormente, cada cenário foi submetido a 50 rodadas de simulações, de onde foram extraídas os valores das médias, desvios padrões e intervalos de confiança de cada métrica escolhida. Esses valores podem ser consultados nas tabelas contidas no apêndice "J". Porém, para facilitar a análise dos resultados, as Figuras 5.4, 5.5, 5.6 e 5.7 apresentam de forma gráfica os resultados obtidos nas simulações, com os seus respectivos intervalos de confiança. Os gráficos foram organizados de forma a facilitar a comparação dos desempenhos dos componentes da arquitetura (JUIZ, ANAMOB e IDISP), de acordo com cada tipo de cenário criado.

Assim, cada figura contém quatro gráficos que são identificados pelo tipo de cenário (Atacantes Externos ou Internos e Precisões de até 1 ou 15m no mecanismo de posicionamento). Os eixos "y" dos gráficos indicam, em porcentagem, o valor de cada métrica: **AD-AC** – Atacantes Descobertos e Alarmes Corretos (Figura 5.4); **FN** – Falsos Negativos (Figura 5.5); **FP –** Falsos Positivos (Figura 5.6) e **GA-AC** – Graus de Anormalidades dos Acertos (Figura 5.7). Os eixos "x" indicam as especificações de cada tipo de cenário (distâncias Atacantes-Vítima Curta ou Média e um ou dois dispositivos por usuário). A seqüência de cenários plotada nos eixos "x" buscou apresentar a tendência (crescente ou decrescente) das métricas obtidas para o componente JUIZ, saída final do EWIDS, assim como dos componentes ANAMOB e JUIZ, a fim de facilitar as análises comparativas entre os três componentes da arquitetura EWIDS.

5.3.1 Resultados para Atacantes Descobertos e Alarmes Corretos

A Figura 5.4 contém os resultados obtidos para as métricas AD-AC (Atacantes Descobertos e Alarmes Corretos, respectivamente). Observa-se nos gráficos da Figura 5.4 que, em **distâncias médias** (entre 500 e 1000 m) entre o atacante e a vítima, os índices de AD (JUIZ) e AC para os componentes JUIZ e ANAMOB são de 100%. O índice de AC para o IDISP está em torno de 94% para atacantes externos e de 6% para internos, tanto para distâncias curtas ou médias.

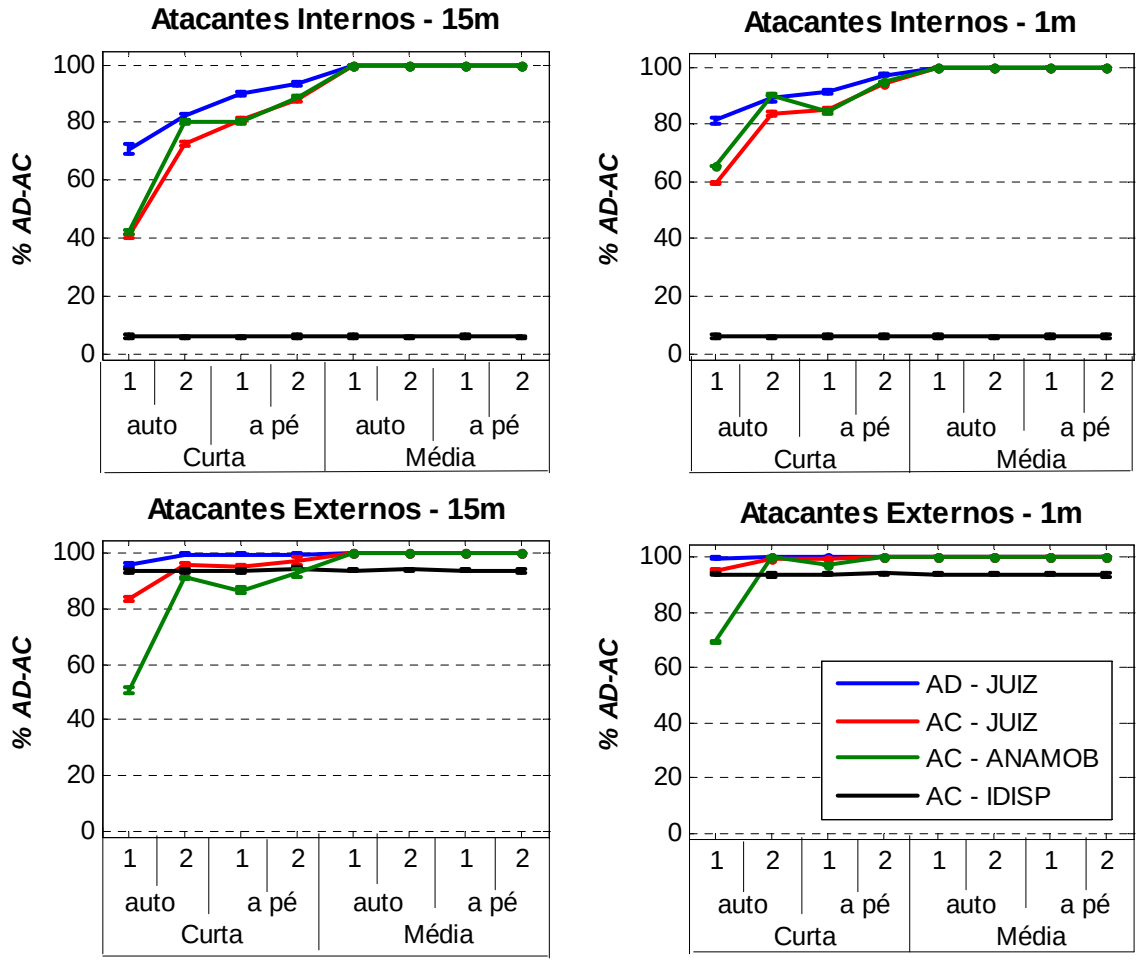


Figura 5.4. Resultados obtidos para Atacantes Descobertos (AD) e Alarmes Corretos (AC).

Em **distâncias curtas** (entre 1 e 100 m), os índices de AD são de 100% para o cenário com atacantes externos e precisão de até 1m no mecanismo de posicionamento. No cenário com atacantes externos e precisão de 15m, o índice de AD somente não é de 100% no caso curta distância atacante-vítima, perfil automotivo e usuário com 1 dispositivo. Este índice é de 96,3%. No cenário com atacantes internos, os menores índices de AD estão nos cenários com precisão de até 15m nos mecanismos de posicionamento, variando desde 70,9%, no perfil automotivo e usuário com 1 dispositivo, até 93,6%, no perfil a pé e usuário com 2 dispositivos. Nos cenários com precisão de até 1m no mecanismo de posicionamento, os índices de AD variam de 81,3% até 97,3%. Para os índices de AC, os menores valores são encontrados nos cenários com atacantes internos e precisões de até 15m, sendo de 40,7% para o JUIZ e 42,1% para ANAMOB. Os maiores, ainda em distâncias curtas, são de 88,2% e 89%, para o JUIZ e ANAMOB,

respectivamente. Os melhores valores são encontrados nos cenários com atacantes externos e precisão de até 1m. Os acertos são de 100%, exceto para os casos automotivos com 1 dispositivo com 69,4% para o ANAMOB e 95,4% para o JUIZ.

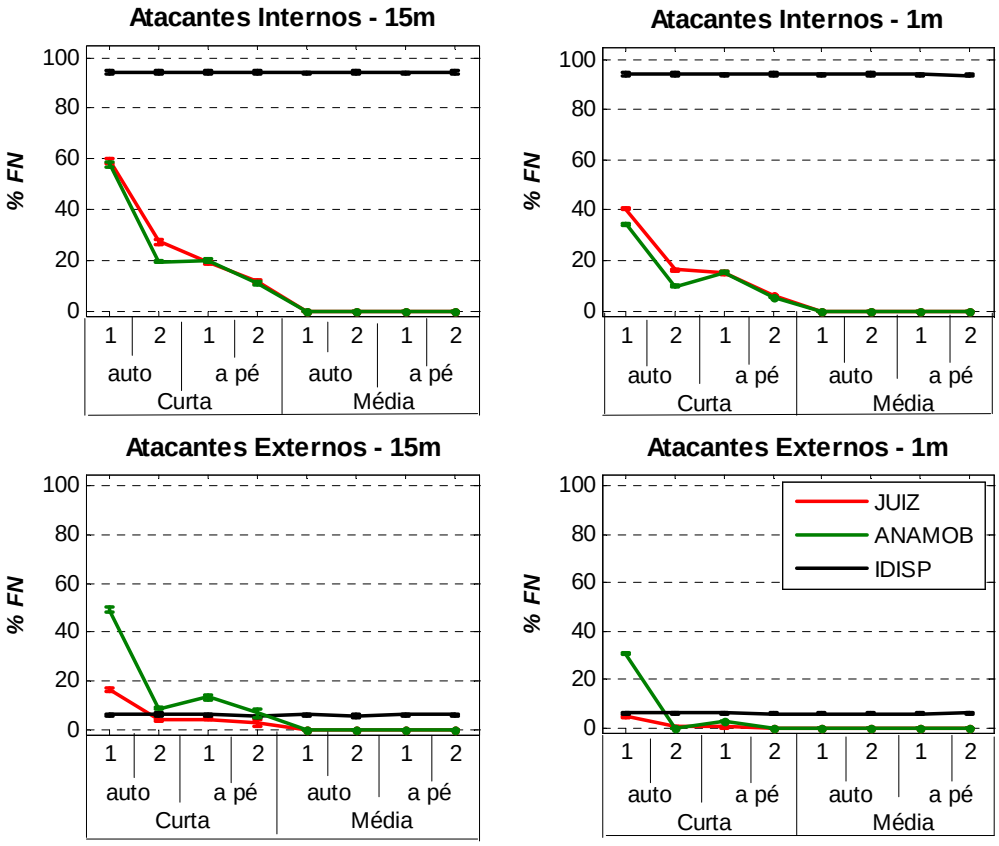


Figura 5.5. Resultados obtidos para Falsos Negativos (FN).

A Figura 5.5 apresenta quatro gráficos referentes à métrica Falsos Negativos (FN), que na verdade é o complemento para 100% dos índices de Acertos (AC) já descritos acima.

Análises dos Resultados para Atacantes Descobertos e Alarmes Corretos

Observa-se um desempenho superior (100%) em todos os casos em que a distância atacante-vítima é média ou superior. Isso demonstra que esse parâmetro é um fator decisivo no desempenho do IDS proposto. Outro aspecto está no desempenho do IDISP, mostrando um comportamento já esperado. Os 6% de acertos, no IDISP, para os atacantes externos está no fato de que os “erros” de identificação, nesse caso, podem ser acertos quanto ao fato de coincidir em ser um atacante. Nota-se que o desempenho no perfil a pé é superior ao automotivo, pois o

automotivo possui maiores velocidades, o que aumenta as áreas onde um usuário pode estar, podendo mascarar a presença de um atacante. Os acertos também aumentam com usuários com 2 dispositivos, por causa da ativação do módulo PMR do ANAMOB. É relevante observar que a imprecisão de até 15m no mecanismo de posicionamento ocasiona mais erros de avaliação do que a imprecisão de 1m. Observa-se, também, que para atacantes internos, o IDISP praticamente não ajuda na detecção, o que causa uma ligeira queda no desempenho do JUIZ em relação ao ANAMOB nos perfis automotivos apenas. No entanto, esta queda é bem pequena em relação a que o próprio IDISP sofre.

5.3.2 Resultados para Falsos Positivos

A Figura 5.6 apresenta os resultados obtidos para a métrica Falsos Positivos (FP).

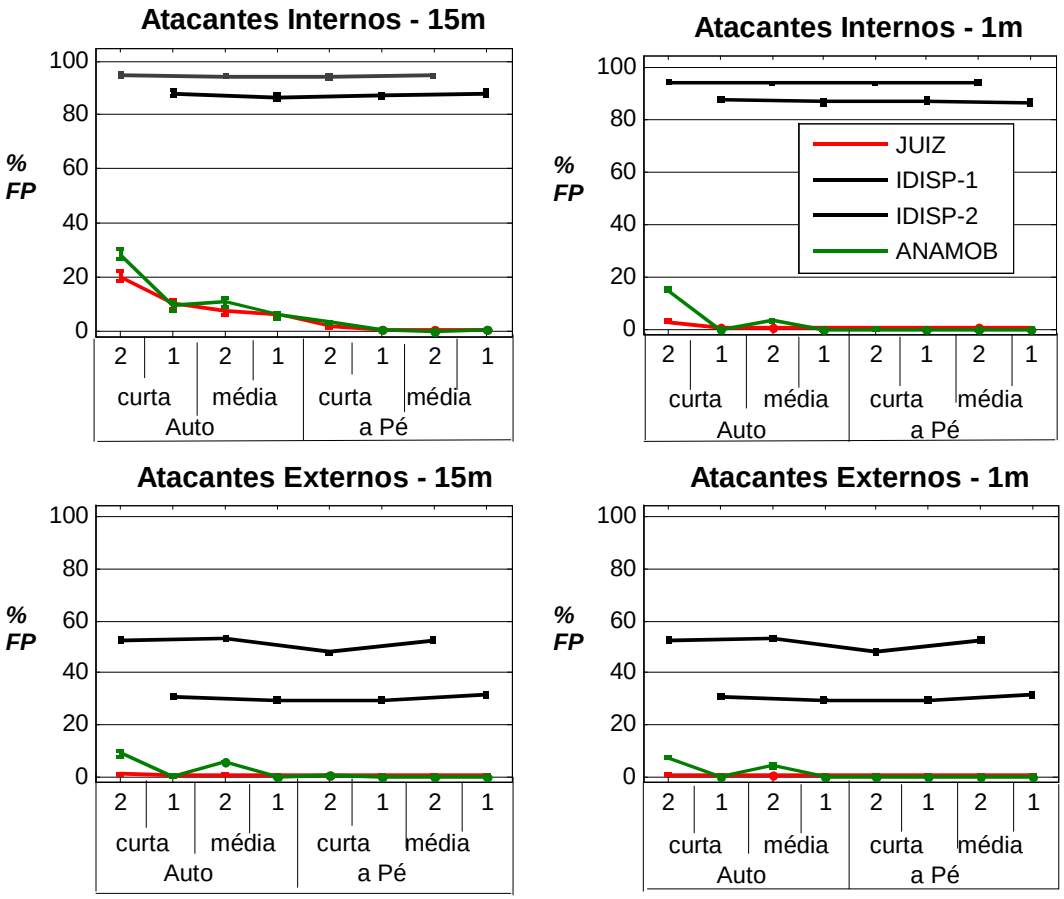


Figura 5.6. Resultados obtidos para Falsos Positivos (FP).

Para **cenários a pé,** os índices de FP são de 0%, exceto para o cenário com atacantes internos, precisão de 15m, distância atacante-vítima curta com 2 dispositivos por usuário. Nesse

caso, o índice é de 10%. Para o componente IDISP, como já esperado, os índices variam de 87% a 94% para atacantes internos, com 1 ou 2 dispositivos por usuário, respectivamente e de 30% a 50% para atacantes externos, com 1 ou 2 dispositivos por usuário, respectivamente.

Nos **cenários automotivos,** os FP do JUIZ estão sempre próximos de 0%, exceto no cenário com atacantes internos com precisão de até 15m e 1m. Nesses casos o índice de FP-JUIZ é de 20,2% para precisão de 15m e de 3% para precisão de 1m, enquanto os índices de FP-ANAMOB são de 28,4% e 15,1%, respectivamente. Observa-se também um pequeno aumento nos índices de FP-ANAMOB quando em cenários com 2 dispositivos. Um outro fato observado é que, no cenário com atacantes externos, com precisão de até 15m no mecanismo de posicionamento, os índices de FP de ANAMOB e JUIZ são menores do que para atacantes internos. Tal fato ocorre, pois, para atacantes externos, o componente IDISP possui um índice menor de FP, refinando a saída do JUIZ, o que promove uma realimentação mais correta (Vetor-Datum) ao *trackerlog* (ANAMOB), tornando-o também mais preciso.

Análises dos Resultados obtidos para Falsos Positivos

Constata-se um melhor desempenho relativo a essa métrica nos perfis a pé do que nos automotivos. Isto se dá, pois no perfil a pé existem poucas variações de velocidades em uma faixa de valores menores, fazendo com que o ANAMOB seja mais preciso. Além disso, a imprecisão de até 15m no mecanismo de posicionamento ocasiona mais erros de avaliação do que a imprecisão de 1m. Nota-se também que quando há 2 dispositivos esse índice é maior para o ANAMOB, por dois motivos descritos a seguir: O primeiro é o tamanho da amostra, já citado anteriormente. O segundo está no fato de que quando há 2 dispositivos o módulo PMR do ANAMOB é acionado, gerando mais uma entrada no módulo Avaliador do mesmo. Como descrito no Capítulo 4, o módulo avaliador possui um componente de decisão baseado em lógica clássica (tabela verdade), bastando apenas um de anormalidade de PMA ou PMR para gerar uma saída anormal. Isto aumenta os acertos, mas aumenta também os FP. Porém, esse fenômeno não ocorre com o JUIZ, pois, ele, por intermédio de sua Máquina de Inferência Nebulosa, computa, **por dispositivo**, os índices de erros dos componentes IDISP e ANAMOB antes de decidir sobre a legitimidade de uma transmissão. Assim, seu comportamento torna-se mais estável e preciso, uma vez que os erros dos componentes são considerados de forma pulverizada entre os dispositivos e não concentrada nos próprios componentes da Arquitetura proposta. Esse fato

demonstra que a implementação do JUIZ quando da adoção de abordagem nebulosa implica em uma maior estabilidade quanto aos Falsos Positivos. Outra conclusão observada nos resultados é que essa estabilidade é maior quando ANAMOB e IDISP erram menos (FP menores), ou seja a estabilidade não é ilimitada, pois a partir de 15,1% de FP em ANAMOB e 94% de FP em IDISP, o FP do JUIZ sobe para 3% e com 28,4% de FP em ANAMOB e 94% de FP em IDISP, o FP do JUIZ vai para 20,2%, revelando uma estabilidade bem menor.

5.3.2 Resultados para Alarmes Corretos com Graus de Anormalidades

A Figura 5.7 apresenta quatro gráficos com os resultados obtidos para os Graus de Anormalidades referentes aos alarmes Corretos do JUIZ (AC-GA).

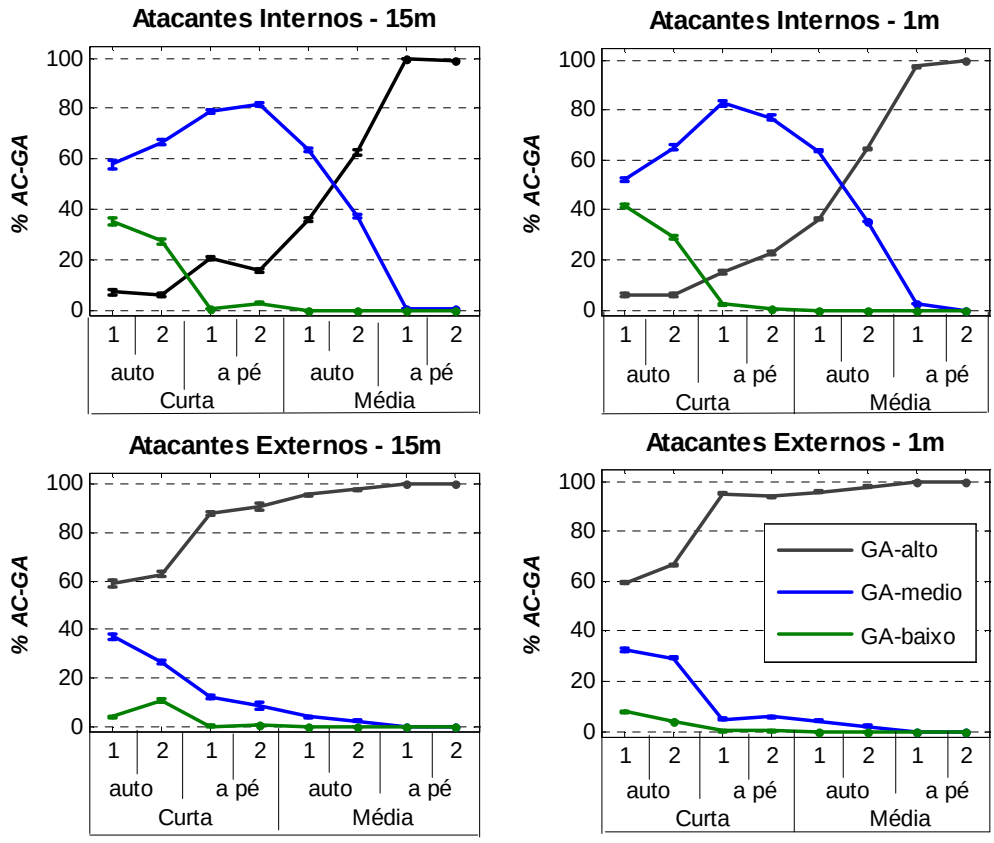


Figura 5.7. Resultados obtidos para os Graus de Anormalidades (GA).

Observa-se através dos gráficos da Figura 5.7 que, nas **distâncias médias** e com **perfil a pé,** existe a predominância de alarmes com GA-alto atingindo patamares de 100%. Em **distâncias médias,** com **perfil automotivo** e atacantes externos, ocorre GA-Alto acima de 90% com até 10% de GA-médios. Porém, nos cenários com atacantes internos, os índices são de

aproximadamente 50% para GA-alto e GA-médio. Em **distâncias curtas e atacantes externos,** os GA-alto ainda predominam com índices de 60%, seguido dos GA-médios na faixa de 30% a 39% e 1% a 10% para GA-Baixo, todos no pior caso (Distância Curta entre atacante e vítima, perfil automotivo e um dispositivo). Todavia para **atacantes internos,** os índices de GA-Alto caem para o patamar de 10% e o índice de GA-baixo sobe para a faixa de 38% a 40%, também no pior caso. Os índices de GA-Médio sobem para o patamar de 60%.

Análises dos Resultados obtidos para Graus de Anormalidade

Pode-se observar nos resultados obtidos que onde há maior índice de AD (Atacante Descoberto) e AC (Alarmes Corretos), há, também, um maior índice de GA-alto's. O contrário também é verdade. Isto significa que, quem recebe um alarme, seja um administrador do sistema e/ou outro componente, associado a um grau de anormalidade alto (GA-alto), possui uma confiança maior sobre a veracidade do alarme do que quando recebe um outro alarme com um GA-baixo. Ou seja, o EWIDS ao gerar um alarme com um GA-baixo deve ainda sofrer uma análise qualitativa a fim de refinar ainda mais o processo, aumentando os índices de acertos e reduzindo os de Falsos Positivos. Observa-se também que os maiores índices de GA-baixo, ocorrem exatamente nos mesmos cenários onde o desempenho do EWIDS referente aos Alarmes Corretos é menor, mostrando, dessa forma, a importância em se diferenciar os alarmes em graus de anormalidade diferentes, conforme constatado nos resultados obtidos.

5.4 Considerações Finais do Capítulo

Os resultados obtidos nos testes comprovam a eficácia na detecção de intrusos da arquitetura EWIDS em cenários metropolitanos de redes sem fio. Analisando os resultados, independentemente do perfil do atacante (interno ou externo), verifica-se um melhor desempenho do protótipo em distâncias médias entre o atacante e a vítima, 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 são confundidas com possíveis localizações de usuários legítimos devido as suas proximidades e pela imprecisão dos sistemas de posicionamento. Logo, os acertos tendem a cair em distâncias menores entre o atacante e vítima.

Quanto ao perfil do atacante, observa-se, como já esperado, que há um melhor desempenho nas métricas medidas nos cenários onde o atacante é externo. Nestes cenários, o componente **IDISP** contribui com a identificação dos atacantes, aumentando o desempenho do

protótipo. Nos cenários com atacantes internos, a análise final do **EWIDS** depende exclusivamente das análises do **ANAMOB**, já que o componente **IDISP** atribui como legítimas as transmissões dos atacantes em 94% dos casos.

Quanto aos Falsos Negativos ou Alarmes Corretos, observa-se nos cenários com distâncias curtas, ainda independentemente de ser um atacante interno ou externo, que o perfil a pé possui um desempenho superior ao perfil automotivo, 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, dentro do princípio da modalidade absoluta.

No tocante aos Falsos Positivos, 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. Outro aspecto relacionado ao aumento de FP para 2 dispositivos por usuário, além do tamanho da amostra já citado, é a adição da avaliação do módulo PMR (Perfil de Mobilidade Relativo), onde os acertos e erros deste componente passam a integrar a estatística, dentro de uma abordagem de lógica clássica no interior do módulo ANAMOB. Mostra-se também a estabilidade do componente JUIZ, diante das variações de Falsos Positivos de ANAMOB e IDISP, em virtude do uso da abordagem nebulosa na implementação da sua máquina de decisão.

Os resultados também demonstram a importância em se diferenciar os tipos de alarmes em Graus de Anormalidade. Demonstrou-se que onde há um maior índice de Alarmes Corretos existe também um maior índice de GA-Altos e onde há menores índices de AC, esses GA-altos caem, dando lugar a maiores índices de GA-médios e GA-baixos, dando condições de um refinamento ainda maior dos alarmes por parte de um administrador da rede ou outro sistema que possa correlacionar com outros tipos de eventos. Os resultados ainda demonstram a eficácia da integração propiciada pelo módulo Juiz de informações distintas de IDS, em especial, aquelas geradas pelo componente IDISP que, sendo utilizado isoladamente, torna-se praticamente inócuo dependendo do cenário considerado.

Capítulo 6 - Conclusões e Trabalhos futuros

Este trabalho apresentou uma proposta de extensão de uma arquitetura para Sistemas de Detecção de Intrusos (EWIDS) [13] cujo objetivo principal foi o de incrementar os níveis de segurança em uma rede sem fio metropolitana, com o aumento da taxa de detecção de invasores, através da incorporação de duas abordagens distintas e que exploram características específicas da tecnologia sem fio: a **assinatura de transmissão rádio** do dispositivo [14] e a **análise cinemática da mobilidade** [13]. A utilização dessas duas abordagens foi possível devido à integração realizada por uma **Máquina de Inferência Nebulosa** [13] desenvolvida neste trabalho**.** A arquitetura proposta viabilizou a utilização de dois fatores (Difusão Rádio e Mobilidade) considerados como fontes das mais contundentes vulnerabilidades do meio sem fio, em soluções para o problema da detecção de intrusos nessas redes.

A arquitetura EWIDS detecta anomalias nas assinaturas de transmissão e na cinemática da mobilidade do dispositivo, portanto sendo classificado como um detector de anomalias (*Anomaly Detector)* de sistemas do tipo WIDS (*Wireless Intrusion Detection System*). Ainda por utilizar informações de posição em seu processamento, o EWIDS também foi classificado como um IDS baseado em localização (*Located Based*) e de tempo real, pois monitora continuamente a rede buscando encontrar, em tempo hábil, anomalias a fim de gerar alarmes que possam impedir uma invasão durante o seu curso.

A abordagem de **assinatura de transmissão rádio**, proposta em [14] e com desempenho de 94% na identificação de transceptores rádio, foi emulada através do componente IDISP da arquitetura e integrada ao IDS proposto por intermédio do componente JUIZ. Ressalta-se que o IDISP funciona como um "divisor de águas" entre dispositivos autorizados ou não, e não como um detector de atacantes. O componente ANAMOB, proposto neste trabalho, utilizou-se da mobilidade característica das redes sem fio metropolitanas para incorporar uma abordagem baseada na **análise cinemática da mobilidade** dos dispositivos, em tempo real**.** O ANAMOB, para tal, fez uso de informações oriundas de um mecanismo de posicionamento geográfico, fora do escopo deste trabalho, que forneceu os dados de entrada necessários ao processamento do mesmo. O ANAMOB realizou a sua análise através de dois novos conceitos introduzidos neste trabalho: o Perfil de Mobilidade Absoluto (PMA) e o Perfil de Mobilidade Relativo (PMR), sendo ambos unificados pelo módulo AVALIADOR do próprio ANAMOB, concebido para

operar fundamentado nos conceitos da lógica clássica. A **Máquina de Inferência Nebulosa,** inserida no componente JUIZ, efetuou a integração das análises produzidas independentemente pelos componentes ANAMOB e IDISP, gerando uma saída única para a EWIDS, composta de um alarme (Normal ou Anormal) e um valor associado ao alarme denominado Grau de Anormalidade - GA (Alto, Médio ou Baixo).

Com o propósito de otimizar os processo de implementação e de simulação, foi escolhido o ambiente *MatLab* com suas ferramentas associadas *Simulink* e *FIS Editor* para a confecção de um protótipo representativo da arquitetura EWIDS. O protótipo é composto por uma Máquina de Inferência Nebulosa, um Gerador de Cenários e um *script* de controle das simulações, de onde puderam ser instanciados os cenários gerados, o protótipo EWIDS e realizadas as medições das métricas de forma a se obter resultados estatísticos consistentes . O processo de implementação foi progressivo e feito por etapas, à medida que iam sendo validados os módulos implementados. A Máquina de Inferência Nebulosa resultante foi alcançada após extensiva fase de testes, de onde se obteve na versão final um refinamento desejado.

Para validar o protótipo implementado, vários testes de simulações foram realizados. Para tal, foram selecionados 32 cenários representativos de uma rede sem fio móvel metropolitana como, por exemplo, as do padrão IEEE 802.16e. Além disso, os cenários foram classificados quanto ao ***Perfil de Mobilidade*** do usuário – A pé ou Automotivo Urbano; ***Número de dispositivos*** por usuário – 1 ou 2 dispositivos; a ***Origem do Ataque*** – Externa ou Interna; a ***Distância Atacante-Vítima*** – Curta ou Média e a ***Precisão do Sistema de Posicionamento*** – até 1 ou até 15 metros. Cada cenário foi submetido a um processo de simulação de 50 rodadas, onde em cada uma delas o cenário era distorcido, em tempo de simulação, pela introdução dos erros oriundos do mecanismo de posicionamento selecionado. As médias, desvios padrões e intervalos de confiança foram medidos para cada métrica selecionada.

Os resultados obtidos demonstram a eficácia e a eficiência da arquitetura EWIDS para cenários metropolitanos. Desses resultados foi possível concluir que em distâncias médias (de 500 a 1000m) ou superiores o EWIDS alcança o seu máximo desempenho em termos de Atacantes Descobertos e Alarmes Corretos ou Falsos Negativos, independentemente das demais características dos cenários. Essa constatação é de suma importância, pois em uma escala de cenário metropolitano, uma distância de 500 a 1000m pode ser considerada pequena, quando

tratamos de alcances de Estações Base de até 50Km [16]. Em distâncias curtas, os resultados obtidos variaram em função das demais classificações do cenário, sendo o pior caso o cenário com atacantes internos, precisão de até 15m no mecanismo de posicionamento, perfil de mobilidade automotivo e usuário com um dispositivo. Conclui-se, como já esperado, que para atacantes internos o IDISP não contribuiu eficientemente na análise do JUIZ e que quanto maiores forem as imprecisões nos mecanismos de posicionamento, maiores serão os erros de avaliação. Além disso, em distâncias curtas, quanto mais próximo o atacante estiver da vítima, maior a sua possibilidade de ser confundido com ela. Conclui-se, também, que quanto maiores forem as velocidades, maiores serão as áreas onde um usuário legítimo pode estar, implicando em Falsos Negativos. E, por último, quanto mais dispositivos um usuário possuir melhores são as possibilidades de acertos para o ANAMOB.

Quanto aos Falsos Positivos (FP), observou-se que os melhores resultados foram obtidos no perfil a pé e o pior caso no cenário com atacantes internos, precisão de até 15m no mecanismo de posicionamento, perfil de mobilidade automotivo e usuário com dois dispositivos. Conclui-se que para atacantes internos o IDISP não contribuiu eficientemente na análise do JUIZ e que quanto maiores forem as imprecisões nos mecanismos de posicionamento, maiores serão os erros de avaliação. Notou-se também que os resultados de FP para o componente IDISP é excessivamente alto quando inserido em cenários com atacantes, concluindo-se pela necessidade da adição de um módulo que trate os seus s de identificação de dispositivos, que neste trabalho foi feito pelo componente JUIZ. Conclui-se também que nos perfis com maiores variações de velocidades, como o Automotivo que possui uma variação de 10m/s (faixa de 7 a 17ms), aumentaram-se os índices de FP, pois as mudanças de velocidades do usuário nessas faixas podem iludir o sistema, fazendo com que, em alguns casos, o usuário legítimo seja considerado um atacante. Observou-se, também, que os resultados obtidos para Falsos Positivos do componente JUIZ, que utiliza uma abordagem de lógica nebulosa, são mais estáveis do que os resultados do componente ANAMOB que possui uma abordagem de lógica clássica em seu módulo de decisão (Avaliador), demonstrando a eficiência da abordagem nebulosa na arquitetura EWIDS. Porém, ressalva-se que essa estabilidade não é ilimitada, pois quanto maiores forem os erros do ANAMOB e IDISP, menor ela será.

No tocante aos Graus de Anormalidades reportados em conjunto com os alarmes, esses se mostraram coerentes demonstrando que esse tipo de informação pode ainda dar mais

confiabilidade aos alarmes e contribuir com um melhor refinamento das decisões de um administrador de sistemas ou outro módulo de contramedidas a que esteja conectado o EWIDS.

A análise dos resultados demonstra que a proposta de extensão EWIDS impõe uma limitação de distância ao atacante, obrigando-o a estar o mais próximo possível da vítima, caso pretenda minimizar o risco de ser detectado. Isto, quando se trata de uma escala metropolitana de vários Km^2, significa retirar toda a liberdade que um atacante teria para se posicionar. 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.

Em suma, a arquitetura EWIDS contribui com a detecção de intrusos em redes sem fio metropolitanas, minimizando os problemas da(s): **(i)** vulnerabilidades do meio sem fio; **(ii)** vulnerabilidades dos padrões e protocolos para redes sem fio; **(iii)** vulnerabilidades oriundas das políticas de suporte ao uso de equipamentos legados, pois independe das plataformas usadas; **(iv)** Robustez criptográfica *versus* desempenho dos dispositivos móveis de baixo poder computacional, pois não impacta o processamento dos nós por não utilizá-los e **(v)** detecta os atacantes de origem interna.

Além disso, a arquitetura EWIS traz as seguintes contribuições como um sistema de detecção de intrusos: **(i)** a possibilidade de detecção de intrusos independentemente de atualizações em bases de assinaturas de ataques e/ou anomalias, tornando a abordagem mais escalável, característica importante em um ambiente que potencialmente pode possuir um grande número de usuários; **(ii)** a possibilidade de detecção de ataques do “dia zero” (ataques sem assinatura conhecida); **(iii)** a não interferência nos requisitos de QoS, Mobilidade e Consumo de Energia, fundamentais nos cenários alvo, pois a arquitetura não utiliza o processamento dos nós monitorados; **(iv)** redução de falsos positivos e negativos, através da integração de informações de naturezas distintas (assinatura de transmissão e mobilidade de dispositivos e usuários) empregando técnicas de lógica nebulosa com o objetivo de tornar mais eficiente o mecanismo de decisão; **(v)** minimização do tamanho da informação armazenada em tempo real por usuário, no controle de sua mobilidade, permitindo também uma melhor escalabilidade e dinamismo em seu perfil de mobilidade e **(vi)** imposição de uma limitação na liberdade de posicionamento dos

atacantes, normalmente oferecida pelas redes sem fio, restituindo ao universo sem fio uma característica das redes cabeadas.

6.1 Trabalhos Futuros

Quanto aos trabalhos futuros, podem ser 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. Uma possibilidade está na implementação de uma Máquina de Inferência Nebulosa para o módulo Avaliador do ANAMOB, ao invés de uma abordagem clássica. Outros trabalhos futuros que visem aprofundar a investigação do desempenho do EWIDS estão relacionados à criação de novos cenários, com variações do número de atacantes e usuários, números de dispositivos por usuário, inclusão de atacantes móveis e atacantes que seguem a vítima, inclusão de cenários mistos onde os atores permutam entre os perfis automotivos e a pé e a inclusão de um percentual de dispositivos que opere em modo ocioso (*idle*), sem reportar a sua posição. Outro trabalho futuro relaciona-se a implementação do componente JUIZ, com uma abordagem de lógica clássica, a fim de comparar o seu desempenho com o protótipo testado neste trabalho, baseado em lógica nebulosa.

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. E finalmente, também como trabalho futuro vislumbra-se a possibilidade de agregar uma arquitetura que seja baseada em perfis de comportamento dos usuários, que poderia ser integrada ao EWIDS. Essa linha de pesquisa já vem sendo investigada dentro do grupo de pesquisas do mestrado.

Referências Bibliográficas

1. Padrão, Institute of Electrical and Electronics Engineers, IEEE Draft 802.16e (D9) - *Air Interface for Fixed and Mobile Broadband Wireless Access Systems*. 2005.

2. Padrão, Institute of Electrical and Electronics Engineers, IEEE 802.16 - *Air Interface for Fixed Broadband Wireless Access Systems*. 2004.

3. BOOM, D.D., *Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks*. 2004, Naval Postgraduate School: California.

4. STALLINGS, W., *Network Security Essentials*. 2002: Ed. Prentice Hall.

5. JOHNSTON, D.a.J.W., *Overview of IEEE 802.16 security*. IEEE Security & Privacy, 2004.

6. Padrão, Institute of Electrical and Electronics Engineers, IEEE Standard 802.16 - *Air Interface for Fixed Broadband Wireless Access Systems*. 2001.

7. Padrão, Institute of Electrical and Electronics Engineers, IEEE 802.11 - *Wireless Local Area Networks*. 1999.

8. HERNANDES, M.P.e.a., *PEARL Tools: um Conjunto de Ferramentas para Avaliação da Eficiência de Algoritmos de Criptografia em Dispositivos Móveis*. Salão de Ferramentas. SBRC, 2005.

9. Site, *GSM security papers*. Disponível em abril de 2006 em http://www.gsm-security.net/gsm-security-papers.shtml.

10. CROTHERS, T., *Implementing Intrusion Detection Systems: A Hands-On Guide for Securing the Network*. 2002: Ed. Wiley.

11. ZHANG, Y., WENKE LEE and YI-AN HUANG, *Intrusion Detection Techniques for Mobile Wireless Networks*, in Wireless Networks. 2003. p. 545-556.

12. SCHMOYER, T.R., *Wireless Intrusion Detection and Response. A case study using the classic man-in-the-middle attack*, in WCNC. 2004.

13. VIANNA, Nilson Rocha, Reinaldo de B. Correia, Luci Pirmez, *EWIDS: Uma Extensão para Arquiteturas de Sistemas de Detecção de Intrusos para Redes Sem Fio Metropolitanas*, Simpósio Brasileiro de Redes de Computadores (SBRC), Curitiba, 2006.

14. HALL, J., Michel Barbeau and Evangelos Kranakis. *Enhancing Intrusion Detection In Wireless Networks Using Radio Frequency Fingerprinting*. 2004: Proceeding (433) Communications, Internet, and Information Technology.

15. Padrão, Institute of Electrical and Electronics Engineers, IEEE 802.15 - *Wireless Personal Area Networks*. 2002.

16. AGIS, E., Intel. Global, *Interolerable Broadband Wireless Networks: Extending WiMAX Technology to Mobility*. Intel Technology Journal, Volume 8, Issue 3, 2004.

17. TANENBAUM, A.S., *Computer Networks*. 4ª edição americana, 2004.

18. HIGHTOWER, J., Gaetano Borriello, *Location Systems for Ubiquitous Computing*, IEEE Computer, 57-66, 2001.

19. GWON, Y., Ravi Jain, and Toshiro Kawahara, *Robust Indoor Location Estimation of Stationary and Mobile Users*. IEEE INFOCOM, 2004.

20. NAJAR, Montse, J.M.H., Josep Vidal, Antonio Castro, *Mobile Location with Bias Tracking in Non-Line-of-Sight*, ICASSP Conference, Montreal, Quebec, Canada, 2004.

21. Site, *GPS Overview*. Disponível em http://users.erols.com/dlwilson/gpswaas.htm e http://users.erols.com/dlwilson/gps.htm]. Acessado em fevereiro de 2006.

22. BAHL, Paramvir and Venkata N. Padmanabhan. *RADAR: An In-Building RF-based User Location and Tracking System*, INFOCOM, volume 2, pages 775-784, March, 2000.

23. *APRS Protocol Reference*. Protocol Version 1.0. The APRS Working Group, August, 2000.

24. Internet Engineering Task Force (IETF), RFC 3748 - *Extensible Authentication Protocol*.

25. Internet Engineering Task Force (IETF), RFC 3280 - *certificação digital X.509*.

26. MARKS, R.B., *Security review of IEEE 802.16e D8*. Disponível em http://www.drizzle.com/~aboba/EAP/review.txt]. Acessado em fevereiro de 2005.

27. MANDIN, J.e.a., *IEEE 802.16e Security Review*. Disponível em http://www.drizzle.com/~aboba/EAP/802.16eNotes.pdf. Acessado em fevereiro de 2005.

28. DEBAR, H., Marc Dacier e Andreas Wespi. *Towards a taxonomy of intrusion-detection systems*. Computer Networks, 1999(31): p. 805-822.

29. OLSON, R.H., *On the use of Bayes Theorem in estimating False Alarm Rates*. Monthly Weather Review 93: 557-558, 1965.

30. KLIR. G.J., U.S.C., and B.Yuan, *Fuzzy Set Theory: Foundations and Applications*. 1997: Prentice Hall.

31. ZADEH, L., *Fuzzy Sets*, Information and Control. 1965. p. 338-353.

32. POTTER, B., *Wireless Intrusion Detection*. Wireless Security, 2004: p. 4-5.

33. KOMNINOS, Nikos, D.V.a.C.D., *Detecting unauthorized and compromised nodes in mobile ad hoc networks and I.P. Ad Hoc Networks*, Corrected Proof, Available online 27 December, 2005.

34. KIM, Hyunwoo, D.K. and S.K., *Lifetime-enhancing selection of monitoring nodes for intrusion detection in mobile ad hoc networks.* AEU - International Journal of Electronics and Communications, Volume 60, Issue 3, Pages 248-250, 2006.

35. DASGUPTA, D., F.G., K. Yallapu, J. Gomez and R. Yarramsettii, *CIDS: An agent-based intrusion detection system*. Computers & Security, Volume 24, Issue 5, Pages 387-398, august, 2005.

36. GOWADIA, Vaibhav, C.F., Marco Valtorta, *PAID: A Probabilistic agent-Based Intrusion Detection system*. Computers & Security, Volume 24, Issue 7, Pages 529-545, October, 2005.

37. DEPREN, Ozgur, M.T., Emin Anarim, M. Kemal Ciliz. *An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks*. Expert Systems with Applications, Volume 29, Issue 4, Pages 713-722, November, 2005.

38. GUO, F.C., Tzi-cker. *Sequence Number-Based MAC Address Spoof Detection*. Recente Advances in Intrusion Detection, RAID, 2005.

39. NASH, Daniel C., T.L.M., Dong S. Ha, Michael S. Hsiao, *Towards an Intrusion Detection System for Battery Exhaustion Attacks on Mobile Computing Devices*, percomw, pp. 141-145, Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05), 2005.

40. SUN, B. and F Yu. *Mobility-based anomaly detection in cellular mobile networks*. International Conference on WiSe 04, P., Pennsylvania, USA, pp.61-69., 2004.

41. HALL, J., M.B. and E. Kranakis. *Using mobility profiles for anomaly-based intrusion detection in mobile networks*. In Proceedings of the Wireless and Mobile Computing, Networking and Communications, pages 22. August, 2005.

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

43. GOMEZ, J.a.D.D., *Evolving fuzzy Classifiers for Intrusion Detection*, Proceedings of the IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, 2002.