Universidade Estadual de Londrina

MATHEUS PEREIRA DE NOVAES

FRAMEWORK TEORIA DOS JOGOS APLICADO NA GERÊNCIA DE REDES

LONDRINA–PR

2016

MATHEUS PEREIRA DE NOVAES

FRAMEWORK TEORIA DOS JOGOS APLICADO NA GERÊNCIA DE REDES

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Mario Lemes Proença Jr.

LONDRINA–PR

2016

Matheus Pereira de Novaes
Framework Teoria dos Jogos aplicado na Gerência de Redes/ Matheus Pereira de Novaes. – Londrina–PR, 2016-
57 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. Mario Lemes Proença Jr.

– Universidade Estadual de Londrina, 2016.

1. Teoria do Jogos. 2. Gerência de Redes. 3. Detecção de Intrusão. I. Prof. Dr. Mario Lemes Proença Jr.. II. Universidade Estadual de Londrina. III. Faculdade de Ciência da Computação. IV. Framework Teoria dos Jogos aplicados na Gerência de Redes

CDU 02:141:005.7

MATHEUS PEREIRA DE NOVAES

FRAMEWORK TEORIA DOS JOGOS APLICADO NA GERÊNCIA DE REDES

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA

Prof. Dr. Mario Lemes Proença Jr.
Universidade Estadual de Londrina
Orientador

Prof. Dr. Elieser Botelho Manhas Jr.
Universidade Estadual de Londrina

Prof. Ms. Luiz Fernando Carvalho
Universidade Estadual de Londrina

Londrina–PR, 21 de dezembro de 2016

Dedico este trabalho a todos que
acreditam que a ciência pode transformar o mundo.

AGRADECIMENTOS

Gostaria de agradecer em primeiro lugar à Deus, por ter me dado discernimento e sabedoria ao longo desta jornada e sem ele acredito que não teria alcaçando meus objetivos.

Gostaria de agradecer a minha família por ter me dado todo suporte necessário e que sempre estiveram ao meu lado. Meu pai, Ademir Pereira de Novaes, a minha mãe Dirce Aparecida de Novaes, e minha irmã Mayara Fernanda Pereira de Novaes.

Gostaria de agradecer ao meu orientador Mario Lemes Proença Jr. pela oportunidade e confiança, me aceitando como orientando desde a iniciação científica até a orientação do trabalho de conclusão de curso. Também gostaria de agradecer ao professor Luiz Fernando Carvalho e ao Anderson Hiroshi Hamamoto, membros do grupo de pesquisa de redes pelo apoio na condução deste trabalho.

Agradeço também a todas as amizades que a UEL me proporcionou, que de certa forma estes amigos estiveram ao meu lado tanto em momentos de distração quanto de dificuldades.

Gostaria também de agradecer a todos os professores e técnicos da UEL que de alguma forma contribuíram para a minha formação acadêmica.

"But seek first the kingdom of God and his righteousness, and all these things will be added to you."(Matthew 6:33)

NOVAES, M. P.. **Framework Teoria dos Jogos aplicado na Gerência de Redes**. 57 p. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Estadual de Londrina, Londrina–PR, 2016.

RESUMO

Devido a grande quantidade de serviços disponíveis que utilizam de redes de computadores, faz-se necessário gerenciar e manter seguras todas as informações geradas pelos mesmos. Inúmeras técnicas vem sendo aplicadas em conjunto com *framework* de Teoria dos Jogos para auxiliar em problemas relacionadas à gerência de rede. Portanto, o objetivo do presente trabalho busca realizar um estudo do *framework* de Teoria dos Jogos para auxiliar no processo da gerência de redes de computadores.

Palavras-chave: Teoria dos Jogos. Gerência de Redes. Detecção de Intrusão.

NOVAES, M. P.. **Game Theory Framework applied to the Networks Management**. 57 p. Final Project (Bachelor of Science in Computer Science) – State University of Londrina, Londrina–PR, 2016.

ABSTRACT

Due to the huge amount of available services that use computers networks, it is necessary to hold and to manage all the generated information. Many different techniques have been applied along with Game Theory framework to support problems associated with networks manage. Therefore, the purpose of this study is to present a research about Game Theory framework to support the computers networks management process.

Keywords: Game Theory. Networks Management. Intrusion Detection.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACO	Ant Colony Optimization
AIOS	Attacker Intent, Objectives and Strategies
CIDS	Collaborative Intrusion Detection Systems
CIM	Coeficiente de Informação Máxima
CP	Collecting Processes
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSNSF	Digital Signature of Network Segment using Flow Analysis
EP	Exporting Process
GA	Genetic Algorithms
IDS	Intrusion Detection Systems
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPFIX	IP Flow Information Export protocol
IPS	Instrusion Prevention Systems
ISO	International Organization for Standardization
MP	Measurement Process
MSPCA	Multilinear Sparse Principal Component Analysis
NE	Nash Equilibrium
PCA	Principal Component Analysis
RFC	Request for Comments
ROC	Receiver Operation Characteristic
SNMP	Simple Network Management Protocol
TCP	Transport Control Protocol

ToS	Type of Services
UDP	User Datagram Protocol

SUMÁRIO

1 INTRODUÇÃO

As redes de computadores tornaram-se uns dos principais meios para a transmissão de dados. A demanda tanto da disponibilização quanto na utilização de serviços que utilizam redes de computadores como meio de comunicação vem crescendo. Em consequência desse fato, a quantidade de dados que trafegam pela rede também aumentou rapidamente. É de suma importância manter a disponibilidade, confiabilidade e integridade desses serviços aos usuários. A gerência da estrutura e da segurança das informações da rede tornou-se uma atividade com alto grau de complexidade. Logo, faz-se necessário o estudo de técnicas eficientes para auxiliar o gerenciamento da rede.

A principal tarefa da gerência de redes é garantir que os recursos da rede possam sempre estar disponíveis aos usuários da mesma. Dessa forma, a *ISO* (*International Organization for Standardization*) propôs um modelo baseado em áreas funcionais para o gerenciamento de redes, sendo elas: **Gerência de Configuração**, visa à praticidade em alterações das configurações dos dispositivos; **Gerência de Falhas**, busca identificar e solucionar de maneira rápida uma falha; **Gerência de Desempenho**, trata-se de acompanhar e realizar análises das atividades da rede para prevenção de congestionamento de tráfego; **Gerência de Contabilização**, estabelecer parâmetros quanto a utilização para uma melhor distribuição do recursos da rede e **Gerência de Segurança**, tem como principal função garantir a segurança dos equipamentos e dos dados contra ataques maliciosos.

Anomalias em redes são tipicamente relacionadas a determinados eventos que ocorrem nas atividades da rede fazendo com que o seu comportamento considerado como normal venha a desviar dos padrões. As anomalias em redes podem ocorrer por diversas causas, por exemplo, mau funcionamento de dispositivos, ataques de negação de serviço, invasão do sistema, entre outras causas. Estes tipos de anomalias podem gerar prejuízos ao funcionamento da rede, por essa razão é de grande importância o estudo e aplicação de soluções para detecção de anomalias no tráfego da rede.

Usualmente, soluções de segurança de rede são empregadas utilizando dispositivos preventivos, por exemplo, *firewall*, e/ou reativos, como anti-vírus. Entretanto, esses tipos de soluções não são suficientes para a prevenção de segurança da rede. *Intrusion Detection Systems* (*IDSs*), são dispositivos reativos, que buscam detectar e/ou impedir à ocorrência de ataques.

Os algoritmos implementados em um *IDS* são baseados em padrões de assinatura de ataque e na detecção de comportamentos anômalos da rede[5]. Uma vez que um ataque é detectado, um alarme é disparado ao administrador da rede, que tomará a ação

de mitigar ou parar o ataque. Alguns tipos de *IDSs* possuem mecanismos que tomam decisões em tempo real perante a detecção de um ataque sem a necessidade de notificar o administrador da rede. Esses dispositivos são chamados de *Instrusion Prevention Systems* (*IPSs*)[6].

A abordagem de Teoria dos Jogos vem sendo aplicada por diversos pesquisadores para auxiliar na gerência de redes[7]. A Teoria dos Jogos trata de problemáticas em que vários jogadores possuem objetivos e competem entre si. Em decorrência desse fato, a Teoria dos Jogos fornece um *framework* para análise e modelagem que pode ser aplicado em problemas de segurança de rede. Por exemplo[8], um administrador de rede e um atacante podem ser vistos como dois jogadores competindo em um jogo, no qual o *framework* pode ser usado para predizer as ações do atacante e então, determinar as decisões que devem ser tomadas pelo defensor. Além disso, a Teoria dos Jogos tem capacidade de analisar centenas de possíveis cenários antes de tomar a melhor decisão, assim refinando o processo de decisão do administrador de rede em larga escala[9].

Nesse contexto, este trabalho tem como objetivo realizar um estudo do *framework* Teoria dos Jogos aplicado à gerência de redes, buscando portanto, apresentar conceitos e definições de como o *framework* vem sendo aplicado em conjunto com heurísticas, servindo de base para soluções de problemas relacionados às atividades de gerenciamento de redes de computadores e apresentar um modelo de jogo teórico para encontrar limiares de aceitação para assinatura do tráfego de rede.

O presente trabalho encontra-se estruturado da seguinte forma: No Capítulo 2 é apresentada uma discussão de alguns trabalhos relacionados à Teoria dos Jogos e detecção de anomalias em redes. O Capítulo 3 descreve conceitos de gerência de redes e detecção de anomalias. O Capítulo 4 apresenta os conceitos e definições de Teoria dos Jogos. No Capítulo 5 é realizada uma análise de trabalhos presentes na literatura em que é aplicada a Teoria dos Jogos na detecção de intrusão. No Capítulo 6 é apresentado um modelo de jogo teórico para encontrar limiares de aceitação do tráfego normal da rede. As considerações e conclusões obtidas por meio do presente estudo encontra-se no Capítulo 7. E por fim, são apresentadas as referências bibliográficas utilizadas como base para o desenvolvimento deste trabalho.

2 TRABALHOS RELACIONADOS

Neste capítulo será feita uma breve discussão de trabalhos presentes na literatura que abordam Teoria dos Jogos e também trabalhos relacionados à detecção de anomalias em redes de computadores. Os trabalhos foram selecionados pela sua relevância e sua contribuição para comunidade científica perante a temática aqui discutida.

Ghorbani et al. [10] modelaram um jogo baseado em Sistemas de Detecção de Intrusão Colaborativo (*Collaborative Intrusion Detection Systems* - CIDSs). Os *IDSs* organizados desta forma podem consultar uns aos outros, aumentado o número de bibliotecas para consulta de detecção de intrusão. Entretanto, com o aumento do número de bibliotecas ocorre a diminuição do rendimento e ao mesmo tempo sobrecarrega o sistema devido a comunicação entre os *IDSs*. A fim de melhorar o desempenho do sistema foi utilizado a Teoria dos Jogos para políticas de configuração do sistema. Foi utilizado um jogo estocástico de soma não-nula para modelar o problema da configuração dos *IDSs* colaborativos com objetivo de buscar a configuração ideal. O conceito da solução de equilíbrio de Nash foi aplicado para descrever a estratégia ótima de cada jogador. E as políticas de configurações alteram dinamicamente conforme o estado da rede.

Liu et al. [11] apresentam uma metodologia para modelar a interação entre um atacante de *DDoS* e um administrador de rede. Esta metodologia observou que a capacidade de modelar e inferir a intenção do atacante, objetivos e estratégias (*Attacker Intent, Objectives and Strategies* - *AIOS*) pode resultar em uma eficaz avaliação de risco e previsão do dano perante um ataque. Foi apresentado neste trabalho um modelo de Teoria dos Jogos baseado em um jogo de incentivos para inferir o *AIOS*. Alguns parâmetros de largura de banda foram utilizados como métrica para medir o impacto do ataque e as medidas de incentivo tanto do atacante quanto do defensor. Também foi discutido que o melhor modelo de jogo a ser escolhido depende do grau de precisão dos *IDSs* e o grau de correlação entre os passos de um ataque.

No trabalho de Spyridopoulos et al. [12] é modelado um jogo que fornece um mecanismo de defesa contra ataques *DoS*/*DDoS*. É modelado um jogo de soma de zero não-cooperativo composto por dois jogadores em que estes jogadores tomam decisões simultaneamente em apenas uma jogada. O objetivo do atacante é encontrar uma ótima configuração dos parâmetros de ataque buscando alcançar o máximo de dano ao alvo com o mínimo de custo. Já o objetivo do defensor é garantir ótimos parâmetros para a configuração de um *firewall* para evitar um ataque e maximizar a sua função de ganho. A validação do modelo é feita através de métodos analíticos em busca da estratégia ideal.

Fernandes et al. [13] realizaram um estudo comparativo entre duas técnicas para

detecção anomalias em redes *IP* baseado em dados estatísticos. A primeira é fundamentada utilizando Análise de Componentes Principais (PCA) e a outra é baseada na metaheurística para Otimização de Colônia de Formigas (*ACO*). Com base no histórico do tráfego da rede ambos os métodos geram o perfil normal da rede chamado Assinatura Digital de Segmento de Rede utilizando Análise de Fluxo (*DSNSF*). Após a geração dessa assinatura foi realizada a comparação com o tráfego real, no entanto com o objetivo de detectar eventos anômalos, foram injetados ao tráfego real anomalias do tipo de ataque distribuído de negação de serviço e *flash crowd*. Para a caracterização foram analisadas as seguinte dimensões: bits/s, pacotes/s, fluxos/s, porta de origem e destino e *IP* de origem e destino. Os dados utilizados para teste foram coletados do tráfego da Universidade Estadual de Londrina.

Hamamoto et al. [14] propuseram um método para geração de Assinatura Digital de Rede utilizando Análise de Fluxo que utiliza como base o comportamento normal do tráfego da rede das semanas anteriores para prever um determinado dia de tráfego. A construção desta assinatura foi baseada no modelo bio-inspirado de Algoritmos Genéticos (*GA*) utilizando a organização dos dados em *clusters*. No trabalho a função a qual se buscou otimizar foi a distância Euclidiana entre o centroide e as amostras. A população inicial foi gerada aleatoriamente entre os limites dos dados de entrada. Diferente da codificação clássica que os dados são codificados em valores binários, no trabalho utilizou-se a codificação numérica. O método de seleção utilizado foi a Roleta. Já a mutação utilizou-se de maneira aleatória 3% da população subtraindo ou adicionando 5% no valor do cromossomo. Para comparar o resultado da assinatura com o tráfego real foi utilizado o Coeficiente de Correlação e o Erro Quadrático Médio Normalizado.

Chen et al. [15] propuseram um sistema de detecção de anomalias utilizando Coeficiente de Informação Máxima (CIM) para seleção de atributos e Análise de Componentes Principais Multilinear Esparso (MSPCA) para a detecção de informações anômalas. O CIM foi utilizado para maximizar a relevância entre os atributos e classes e miniminizar a redundância dos atributos selecionados. Após realizada a seleção de atributos é aplicada a *MSPCA* para separar os dados considerados anômalos dos normais. Para a validação do sistema foi utilizado o *dataset* DARPA 1999, um dos *dataset* de detecção de intrusão rotulados mais utilizado. As métricas de validação utilizadas foram a taxa de verdadeiro positivo, taxa de falso positivo e curva *ROC*(*Receiver Operation Characteristic*). A taxa de falso positivo foi de 12.8% e a taxa de verdadeiro positivo foi de 89.4%, considerado portanto um resultado satisfatório.

X. Zhao et al. [16] apresentaram uma nova abordagem não-supervisionada para detecção de anomalias baseada em ponderação de anormalidade e utilizaram uma técnica de clusterização de subespaço sem o tráfego previamente rotulado. O sistema proposto toma como entrada os fluxos de tráfegos não-rotulados e os agrupam em *clusters* com

características semelhantes. A clusterização foi utilizada para rotular como *outliers* os fluxos que não pertence a nenhum *cluster*. O *dataset* utilizado para validar o sistema proposto foi o KDD99. Este *dataset* possui uma alta porcentagem de ataques que estão subdivididos em quatro grupos: Ataque de negação de serviço (*DoS - Denial of Service*), acesso remoto não autorizado (*R2L*), acesso a raiz não autorizado (*U2R*) e Sondas (*Probe*). As acurácias obtidas para tráfego normal foram 96.07%, *DoS* 95.94%, *Probe* 96.39% *R2L* 57.98% e *U2R* 47.09%.

3 GERÊNCIA DE REDES E DETECÇÃO DE ANOMALIAS

Neste capítulo serão apresentados os conceitos e definições de Gerência e Anomalias em redes de computadores.

3.1 Gerência de Redes de Computadores

Os serviços que utilizam redes de computadores aumentaram significativamente e em diversas atividades críticas, tornando o seu uso indispensável. Uma estrutura de rede não pode ser gerenciada apenas com o esforço humano, é necessário técnicas e ferramentas para gerenciá-las[17].

A atividade de gerência de rede consiste em monitorar e controlar todos os dispositivos pertencentes à rede, sendo eles físicos ou lógicos. No entanto, é de suma importância garantir a qualidade dos serviços disponibilizados. Dessa forma, a *International Organization for Standardization* (*ISO*), propôs um modelo chamado Áreas Funcionais de Gerecimento de Rede. As quais são apresentadas a seguir:

- Gerência de Falha: para que uma rede com alto grau de complexidade se mantenha em bom funcionamento é necessário a gerência como um todo, mas também é necessário o controle de cada um dos seus componentes individualmente. Caso uma falha venha a ocorrer é importante que o gerente de rede determine o quanto antes onde essa falha ocorreu. Após a sua identificação, o passo seguinte é isolar a falha para que a rede possa continuar em funcionamento. Tendo realizado o passo anterior, reconfigurar ou modificar a rede para minimizar o impacto sem o componente que ocorreu a falha. E por fim, reparar ou substituir e restaurar a rede a seu estado inicial[17].

- Gerência de Contabilização: o gerente de rede dever ser capaz de controlar a utilização dos recursos da rede pelos usuários, garantindo que um usuário ou um grupo não abuse dos privilégios de acesso dos recursos vindo a sobrecarregar o tráfego da rede. Também tendo essa contabilização é possível que o gerente da rede acompanhe o crescimento da mesma para que planos de melhorias possam ser realizados, assim garantindo o seu bom funcionamento[17].

- Gerência de Configuração: a gerência de configuração consiste em inicializar ou desligar a rede em sua totalidade ou parte dela, garantindo a adição ou atualização entre o relacionamento dos componentes de rede e acompanhar o seu estado enquanto a rede estiver em operação. O gerente de rede deve ser capaz de alterar a conectividade dos componentes de rede quando ela precisa se adequar às mudanças

dos usuários. Realizando uma boa configuração dos componentes, um procedimento que exige uma reconfiguração, por exemplo, a recuperação de uma falha, torna-se fácil[17].

- Gerência de Performance: conforme Stallings[17] descreve, a gerência de performance é compreendida em duas categorias funcionais: monitoramento e controle. A primeira é monitorar todas as atividades que ocorrem na rede, já a segunda permite realizar ajustes para melhorar o desempenho da rede. A gerência de performance garante ao menos níveis mínimos de desempenho para assegurar todo o tráfego que passa pela rede.

- Gerência de Segurança: a prática de gerenciamento de segurança está concentrada em garantir proteção aos recursos disponíveis da rede e também as informações dos usuários. Esta prática deve incluir geração, distribuição e armazenamento de chaves de criptografia. Também deve-se monitorar e controlar o acesso à rede, realizando coleta e armazenamento de registro para auditoria e de *logs* de segurança. Logo, políticas de controle e acesso devem ser adotadas para que o sistema de rede como um todo esteja protegido[17].

O monitoramento da rede fornece ao gerente informações importantes que auxiliam no reconhecimento de atividades anormais no tráfego. Desse modo, é comum à aplicação de dados resultantes de protocolos de gerenciamento de rede. Esses protocolos fornecem dados estatísticos relacionados ao tráfego.

3.1.1 Gerência utilizando SNMP

O nome *SNMP* é um acrônimo para *Simple Network Management Protocol*, é o protoloco padrão de rede *TCP/IP* que foi desenvolvido pelo *IETF* no ano de 1990 pela *RFC* 1157[18]. O *SNMP* foi desenvolvido com o intuito de promover um protocolo que permita facilitar à gerência e monitoramento dos diversos equipamentos de rede e que também fosse acessível de se implementar. O *SNMP* é um protocolo da camada de aplicação que utiliza do protocolo *UDP* para realizar a comunicação entre agente e gerente.

Uma rede que implementa o protocolo *SNMP* é constituída por três componentes básicos:

- **Gerente**: um gerente é responsável por monitorar, controlar e solicitar dos agentes informações dos dispositivos gerenciados.

- **Agente**: o agente basicamente é um *software* instalado nos dispositivos que se comunicam com o gerente passando informações sobre as operações dos dispositivos.

- **Dispositivos gerenciados**: os dispositivos gerenciados são nós da rede que implementam o *SNMP*, por exemplo, *switches*, roteadores e *hubs*.

3.1.2 Gerência baseada em fluxos

Devido a ampliação do grau de complexidade dos sistemas de redes, foi necessário um maior detalhamento no controle dos dados do tráfego. Foi então que surgiu a abordagem de gerência baseado em fluxos de rede. Um fluxo de rede é definido como sendo uma sequência de troca de pacotes entre dois pontos, podendo ser unidirecional ou bidirecional[19]. A capacidade de caracterizar o tráfego *IP* e compreender como e onde ele flui é fundamental para a disponibilidade da rede, desempenho e solução de problemas. O monitoramento de fluxos de tráfego de *IP* facilita a capacidade de um planejamento mais preciso e garante que os recursos sejam utilizados de forma adequada em apoio às metas organizacionais[20].

3.1.2.1 Netflow

O *Netflow* foi desenvolvido por Darren e Barry Bruin em 1996 na Cisco[19]. Ele é a tecnologia precursora no monitoramento e exportação de fluxo de rede. Um fluxo é armazenado em uma estrutura chamada *cache* NetFlow que é definido por um conjunto de pacotes sendo eles compostos pelas seguintes informações: endereço de *IP* de origem, endereço de *IP* de destino, porta de origem, porta de destino, protocolo da camada de transporte, *Byte ToS* e Interface de entrada, conforme é ilustrado na Figura 1. Estas informações de fluxos são extremamente úteis para a compreensão do comportamento da rede.

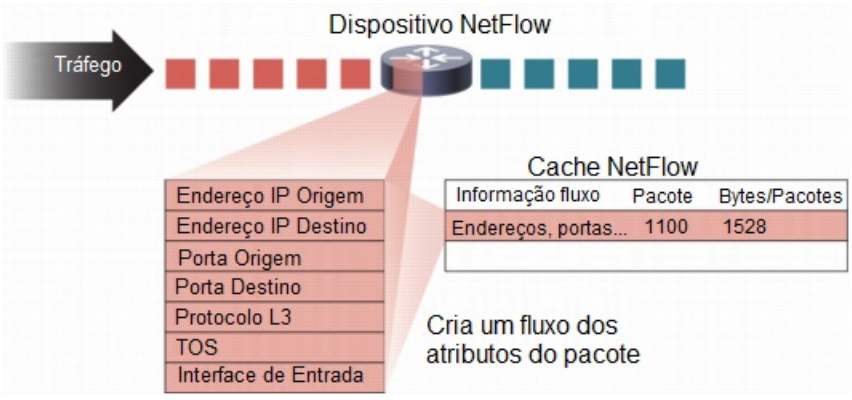

Figura 1 – Criação de fluxos em cache NetFlow. (Adaptada de [1])

3.1.2.2 sFlow

O *sFlow* é uma outra tecnologia de exportação de fluxos que foi desenvolvida pela *InMon Inc* e tornou-se um padrão definido pela *RFC* 3176[21][19]. Umas das principais diferenças desta tecnologia é a exportação de fluxos realizadas através de amostragem.

A concepção do sFlow tem como principal objetivo prover um protocolo elementar de exportação, capaz de monitorar redes que operam em altas taxas de 10Gbps a 100Gbps.

O sFlow é constituído por sensores e coletores, conforme pode ser observado na Figura 2. Nesta aplicação os sensores são denominados agentes. O agente sFlow é um processo de *software* que é executado como parte do *software* de gerenciamento de rede dentro de um dispositivo, que irá monitorar a rede e gerar os dados que serão recebidos pelos coletores. Já o coletor, a partir dos dados recebidos dos agentes, geram métricas para o gerenciamento da rede.

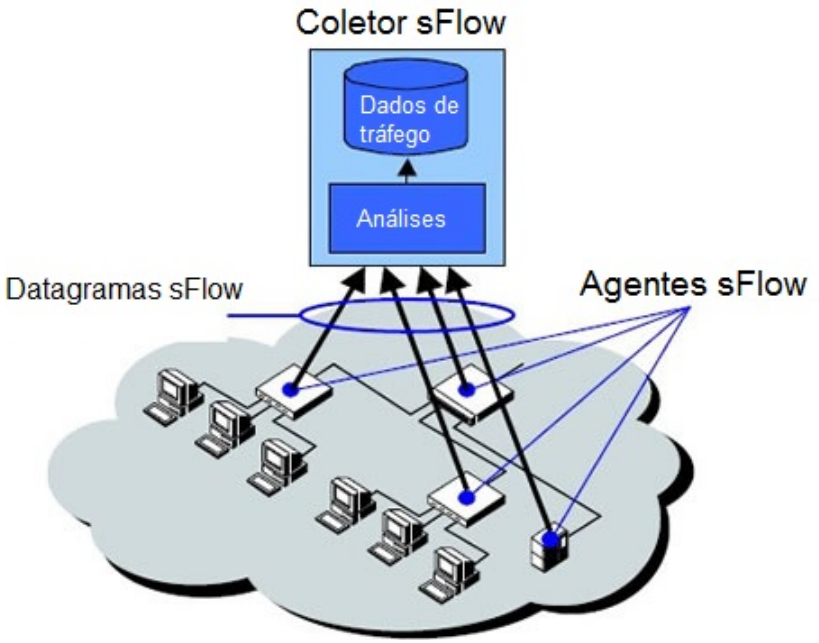

Figura 2 – Agentes e Coletores sFlow. (Adaptada de [2])

3.1.2.3 IPFIX

O *IP Flow Information Export protocol* (IPFIX) é um padrão de exportação de fluxo definido pelo *IETF* pela *RFC* 3917[22] e veio para suceder o Netflow v9, na qual a sua formulação foi baseada. Um fluxo definido pelo IPFIX é um conjunto de pacotes *IP* de um ponto de obervação da rede em um determinado espaço de tempo.

A arquitetura do IPFIX definida pela *RFC* 5470 é especificada por três processos, conforme ilustra a Figura 3: os processos de medição (*MPs*), que geram fluxos de pacotes observado; processos exportadores (*EPs*), que usam IPFIX para enviar os fluxos para a coleta de processos(*CPs*).

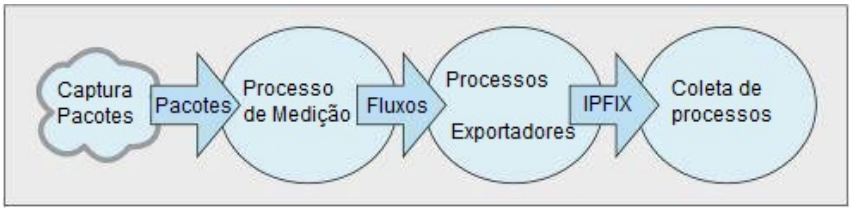

Figura 3 – Arquitetura do IPFIX. (Adaptada de [3])

3.2 Anomalias em Redes

Pode ser definido como anomalia em redes de computadores quando em uma determinada atividade da rede ocorre alguma alteração provocando com que o seu comportamento desvie do padrão. Conforme apresentado no trabalho de Thottan e Ji[23], diversos fatores podem afetar no desvio do comportamento da rede, tais como equipamentos com defeitos, sobrecarga no tráfego de rede, ataques de negação de serviço e intrusões.

Na literatura as anomalias de redes podem ser classificadas em duas categorias[23]. A primeira está relacionada com problemas de falhas e desempenho, também definida no trabalho de Zarpelão[24] como sendo anomalias em que não há presença de agentes maliciosos. Já a segunda são classificadas anomalias relacionadas a problemas de segurança, ou seja, são problemas ligados a ataques visando violar a segurança da rede.

3.2.1 Anomalias causadas por Falhas e Desempenho

Anomalias causadas por falhas e desempenho podem ocorrer, por exemplo, em casos em que muitos usuários fazem requisições a um determinado servidor de arquivo, quando algum nó da rede venha falhar sobrecarregando um outro nó da rede.

O trabalho de Zarpelão[24] apresenta como sendo as seguintes as principais causas que provocam este tipo de anomalia:

- ***Flash crowd***: ocorre quando um elevado número inesperado de usuários envia massivas solicitações a um serviço *Web*, provocando um pico no tráfego. Este tipo de situação geralmente ocorre quando grandes eventos mundiais ocorrem, fazendo com que inúmeros usuários realizem solicitações às plataformas de notícia em busca de informações[25][26].

- ***Babbling node***: é uma situação em que um nó envia pequenos pacotes para diversos nós da rede, entrando em loop infinito. Casos como este ocorrem quando o nó envia solicitações para verificar um relatório de status[23].

- **Tempestade de *Brodcast***: é uma reação em cadeia em que um grande volume de pacotes *brodcast* trafegam pela rede. Essa situação normalmente ocorre quando um

nó falha e inicia o envio de pacotes *brodcast* fazendo com que os demais nó repliquem a transmissão destes pacotes[27].

- **Congestionamento**: inúmeros pacotes sendo transmitidos podem provocar um pico no tráfego da rede. Quando um congestionamento ocorre pode provocar atrasos na transmissão e também a perda de pacotes[28]. Os itens mencionados anteriormente também causam congestionamento[24].

- ***Bugs* no *software* de roteamento**: pacotes que chegam até os equipamentos de roteamento podem apresentar alguma deformação em seu formato, muitas vezes os *softwares* dos equipamentos não estão preparados para lidar com esse tipo de situação e acabam causando erros de encaminhamento, afetando a carga de tráfego da rede monitorado[29][24].

- **Erros de configuração**: erros em configurações de servidores podem dificultar o acesso dos usuários a determinados serviços oferecidos pelo mesmo, o que pode acarretar em congestionamento nos canais de transmissão da rede. Conforme já mencionado o congestionamento é um dos fatores que levam a rede apresentar comportamentos anômalos[24][23].

3.2.2 Anomalias causadas por Segurança

Anomalias causadas por questões de segurança estão relacionadas com onde há a presença de agentes maliciosos sobrecarregando os níveis de tráfego da rede. Esta situação ocorre onde o agente sobrecarrega um determinado serviço com o objetivo de torná-lo indisponível. Também quando um alto volume de tráfego malicioso é injetado, o tráfego legítimo dos usuários é prejudicado, provocando congestionamento da rede[23].

Zarpelão[24] em seu trabalho apresenta como sendo as seguintes as causas deste tipo de anomalia:

- ***Ataque de negação de serviço***: nos ataques de negação de serviço (*DoS - Denial of Service*), o agente malicioso sobrecarrega o tráfego com objetivo de indisponibilizar um serviço. Este grande volume de tráfego gerado faz com que toda a largura de banda fique ocupada, gerando grande lentidão nos serviços de rede. Uma outra prática é constituída por ataques distribuídos (*DDoS - Distributed Denial of Service*), ou seja, é um ataque realizado em grupo [30].

- ***Worm***: é um programa que tem a capacidade de multiplicar-se automaticamente enviando cópias para outros computadores ao longo da rede. Devido a sua grande capacidade de gerar e propagar cópias de si mesmo, consequentemente afeta no desempenho da rede[30][31].

- ***Port scan***: esta técnica é utilizada por gerentes de redes para saber o status das portas, se elas estão abertas, escutando ou fechadas. No entanto, este tipo de técnica também é utilizada por agentes maliciosos para descobrirem alguma vulnerabilidade afim de realizarem invasões ao sistema [24][30].

3.3 Detecção de Anomalias

Técnicas para detecção de anomalias em redes são baseadas em padrões de assinatura e na caracterização do perfil normal da rede. A primeira delas possui uma base de dados contendo as informações sobre as anomalias conhecidas. Uma das vantagens deste tipo de abordagem é a diminuição da taxa de falso-positivo. Já a segunda técnica é baseada em gerar um perfil do tráfego da rede caracterizando como sendo normal, não dependendo de base para detecção de anomalias.

Um sistema de detecção de anomalias gera os seguintes resultados:

- tráfego normal.
- tráfego anômalo.
- tráfego normal detectado como anômalo (falso-positivo).
- tráfego anômalo detectado como normal (falso-negativo).

3.3.1 Detecção de anomalias baseado em padrões de assinatura

A detecção de anomalias baseado em padrões de assinatura é necessário uma grande base de dados contendo as assinaturas para determinar se uma anomalia veio à ocorrer. Para a detecção é necessário que o sistema monitore as atividades da rede e caso encontre um conjunto de atributos que estejam na base de assinaturas é disparado um alarme para o administrador da rede.

Uma das grandes vantagens deste tipo de abordagem é a diminuição da taxa de falsos-positivos que é um grande desafio enfrentado na detecção de anomalias. Pelo fato de que só será detectado uma anomalia se uma assinatura é pré-estabelecida, ou seja, se essa anomalia já tenha ocorrido antes.

A desvantagem desta técnica é que o tamanho da base de assinatura pode ser muito grande, podendo afetar no desempenho para a detecção em tempo real. Uma outra desvantagem é a constante atualização da base de assinaturas, pois uma anomalia que não esteja registrada não será detectada.

3.3.2 Detecção de anomalias baseado no perfil normal da rede

A abordagem de detecção de anomalias em que é caracterizado um perfil como sendo normal, conforme é demonstrado no trabalho de Proença[32], constitui-se em analisar o tráfego passado da rede para definir limiares máximos e mínimos do comportamento normal. Após gerado este perfil normal, uma eventual anomalia é detectada quando, no monitoramento de algum ponto do segmento, é ultrapassado um destes limiares pré-definidos.

Uma das principais vantagens deste tipo de metodologia é a detecção de anomalias não conhecidas pois os modelos criados são baseados no comportamento normal. Uma outra vantagem é que não há necessidade de uma base com informações das anomalias, isto faz com que a detecção em tempo real seja uma vantagem em relação a detecção de anomalias utilizando padrões de assinatura.

A principal desvantagem desta técnica é a taxa de falso-positivo ocorrida. Muitas vezes, tráfego de usuários legítimos são detectados como sendo anômalos, fazendo com que falsos alarmes sejam disparados ao administrador da rede. Diversos estudos na literatura vem sendo desenvolvidos para reduzir esta taxa.

4 TEORIA DOS JOGOS

Será apresentado neste capítulo um breve histórico do surgimento, as definições matemáticas, e alguns conceitos relacionados à classificação de um jogo. Por fim, é mostrado como é encontrada a solução de um jogo.

4.1 Histórico e Definição

Registros mostram que as primeiras discussões relacionadas ao campo de teoria dos jogos iniciaram-se em meados do século XVIII. No ano de 1973, em uma correspondência dirigida a Nicolas Bernoulli, James Waldegrave realizou uma análise em um jogo de cartas chamado "*le Her*" para dois jogadores e propôs uma solução que é um equilíbrio das estratégias mistas[33]. Entretanto, Waldegrave não deu continuidade nesta abordagem para uma formalização teórica geral. Nos anos inicias do século XIX, temos a publicação do importante trabalho de Augustin Cournot. Neste trabalho é proposto um modelo econômico com a função de modelar um cenário em que as empresas competem de acordo com a produção de seus concorrentes. Este modelo ficou conhecido como Competição de Cournot ou Modelo de Cournot [34].

Diversos autores acreditam que o conceito formal de teoria dos jogos foi iniciado pelo matemático e filósofo alemão Ernst Zermelo. Em 1913 Zermelo publicou o primeiro teorema matemático da teoria dos jogos. Neste teorema o autor demonstra que o jogo de xadrez é estritamente determinado, isto é, em cada estágio do jogo pelo menos um dos jogadores possui uma estratégia que pode levá-lo a dois caminhos, um deles poderá levá-lo a vitória ou conduzir para um empate.

Um outro trabalho que também possui grande destaque é o trabalho do matemático e político francês Emile Borel que foi responsável por reformular a solução do problema *minmax* e pulicou quatro artigos introduzindo os conceitos de estratégias puras e mistas. Borel acreditava que tanto a guerra quanto a economia poderiam ser estudadas de maneira semelhante[33].

Em 1928, o famoso matemático húngaro John von Neumann demonstrou em seu trabalho que todo jogo finito de soma zero composto por dois jogadores possui uma solução em estratégias mistas. Von Neumann, que contribuiu em muitas áreas do conhecimento com diversos trabalhos, também teve a sua contribuição no campo da economia. Em 1994, juntamente com o economista Oscar Morgenstern, publicou um dos clássicos da literatura econômica e da teoria dos jogos intitulado "*The Theory of Games and Economic Behaviour*", tornado-se portanto, um dos marcos da economia e da matemática aplicada, segundo diversos autores.

Um outro autor de suma importância e com diversas contribuições para área de Teoria do Jogos foi o matemático norte-americano John Forbes Nash Jr. No ano de 1950 John Nash publicou quatro notas importantes para a Teoria dos Jogos e para a teoria da barganha, também conhecida como Problema da Negociação. Nos artigos "*Equilibrium Points in n-Person Games*"e "*Non-cooperative Games*"o matemático demonstrou a existência de um equilíbrio de estratégias mistas para jogos não-cooperativos, este conceito é denominado como sendo o *equilíbrio de Nash* e é amplamente utilizado como solução na modelagem dos jogos. Os outros dois trabalhos são "*The Bargaining Problem*"e "*Two-Person Cooperative Games*"onde Nash propôs o Problema da Negociação e demonstrou a existência de uma solução para o problema.

A Teoria dos Jogos é uma ferramenta matemática criada para modelar fenômenos que podem ser observados no qual vários indivíduos (chamados jogadores ou agentes) tomam uma decisão. Tendo como objetivo analisar tais fenômenos de maneira lógica e determinar como os jogadores devem agir para solucionar o confronto buscando o melhor ganho possível, ela fornece a linguagem para a descrição de processos de decisão conscientes e objetivos envolvendo mais do que um indivíduo[33].

Um jogo basicamente é constituído por um conjunto de *jogadores*. Cada jogador possui um conjunto de *estratégias*. Quando um jogador escolhe uma estratégia, existe um conjunto chamado *função de utilidade* (ganho ou *payoff* do jogador) que atribui um número real em cada situação de jogo[33]. Os jogos podem ser cooperativos se os jogadores interagem cooperativamente e não-cooperativos se os jogadores interagem competitivamente.

Definicão 4.1.1 (Definição de um Jogo [35], [33])**.** *Seja n um inteiro positivo. Um jogo é representado por uma tripla (G, S, U), onde* $G = \{g_1, g_2, \ldots, g_n\}$ *representa o número finito de jogadores. Cada jogador* $g_i \in G$ *possui um conjunto finito* $S_i = \{s_{i1}, s_{i2}, \ldots, s_{mi}\}$ *denominadas estratégias puras do jogador,* $s = (s_1, s_2 \ldots s_n) \in a\ S$ *é o vetor de estratégias e* $U = \{u_1, u_2, \ldots, u_n\}$ *é o conjunto de função utilidade de* $S \to \mathbb{R}$ *com* $S = S_1 \times, \ldots, \times S_n$..

Em teoria dos jogos, quatro elementos básicos descrevem um jogo:

- **Jogadores**: são as entidades envolvidas em um jogo. Estas entidades podem ser pessoas, dispositivos, ou quaisquer outras coisas que interagem entre si.
- **Ação**: em cada movimento de um jogador, uma ação é tomada. É assumido que cada jogador conhece todas as possíveis ações de outro jogador.
- **Payoff**: após todos os jogadores terem tomado uma ação, cada jogador recebe um retorno positivo ou negativo. O retorno de cada jogador é o seu *payoff*.

- **Estratégia**: a estratégia de um jogador é seu plano de ação, que específica a ação que será tomada baseado em seu conhecimento. As estratégias podem ser puras ou mistas.

4.2 Classificação de um Jogo

Um jogo pode ser classificado em diferentes aspectos. Eles são: Baseado no número de estágios, informação perfeita ou imperfeita e baseado em informação completa ou incompleta [36].

4.2.1 Baseado no número de estágios

Esta classificação é se um jogo possui um ou múltiplos estágios.

- **Jogo Estático/Estratégico**: é um jogo em que as ações dos jogadores são tomadas no mesmo instante em apenas uma jogada[36].
- **Jogo Dinâmico/Extensivo**: é um jogo que consiste em múltiplos estágios.
- **Jogo Estocástico**: é um tipo de jogo dinâmico no qual tem-se um estado inicial e os estados possuem transições de um estado para o outro. No estado inicial, os jogadores tomam ações e recebem os *payoffs* com a transição do estado atual para o outro. Isso requer uma certa probabilidade com base no estado atual e a ação tomada.

4.2.2 Baseado em Informação Perfeita ou Imperfeita

A segunda classificação é se um jogo possui informação perfeita.

- **Jogo de Informação Perfeita**: cada jogador conhece todas as ações tomadas anteriormente de cada jogador.
- **Jogo de Informação Imperfeita**: pelo menos um dos jogadores não conhece as ações tomadas anteriormente pelos outros jogadores.

4.2.3 Baseado em Informação Completa ou Incompleta

A terceira classificação é se um jogo possui informação completa.

- **Jogo de Informação Completa**: todos os Jogadores conhecem as funções de *payoff* dos demais jogadores.
- **Jogo de Informação Incompleta**: pelo menos um dos jogadores não conhece a função de *payoff* dos outros jogadores.

4.3 Solução de um Jogo

Uma característica importante de um jogo é prever o desenvolvimento das ações para então determinar o seu resultado. Estas predições são descritas como sendo a solução de um jogo e também quais estratégias devem ser adotadas pelo jogador ao decorrer do jogo. Nesta seção será descrita dois conceitos fundamentais para a solução de um jogo: dominância e equilíbrio de Nash.

4.3.1 Dominância

Uma estratégia é dita estritamente dominante quando todos os seus ganhos perante uma outra estratégia de seu adversário é sempre maior. Jogadores racionais nunca devem escolher estratégias estritamente dominadas já que seu resultado sempre será pior. Recomenda-se ao jogador que elimine as estratégias dominadas[33].

Definicão 4.3.1 (Estratégia Pura Estritamente Dominada)**.** *Uma estratégia pura* $s_{ik} \in S_i$ *do jogador* $g_i \in G$ *é estritamente denominada pela estratégia* $s_{ik'}$ *se*

$$u_i(s_{ik'},\, s_{-i}) > u_i(s_{ik},\, s_{-i}),$$

para todo $s_{-i} \in S_{-i}$*. A estratégia* $s_{ik} \in S_i$ *é fracamente dominada pela estratégia* $s_{ik'} \in S_i$ *se* $u_i(s_{ik'},\, s_{-i}) \geq u_i(s_{ik},\, s_{-i})$ *para todo* $s_{-i} \in S_{-i}$*.*

4.3.2 Equilíbrio de Nash

O equilíbrio de Nash (*NE*), também conhecido como solução estratégica de um jogo, é a etapa onde nenhuma mudança unilateral de um jogador faz aumentar o seu ganho. Em outra palavras, se cada um dos jogadores escolher sua melhor estratégia, ou seja, aquele em que ele obtêm o maior retorno. Caso todos os jogadores cheguem a esta mesma conclusão, então as estratégias tomadas pelos jogadores definem como sendo um equilíbrio de Nash[33].

Definicão 4.3.2 (Equilíbrio de Nash)**.** *Um perfil de estratégia*

$$\boldsymbol{s}^* = (s_1^*,\, s_2^*,\, \ldots,\, s_n^*)$$

é um equilíbrio de Nash se

$$u_i(s_i^*,\, \boldsymbol{s}_{-i}^*) \geq u_i(s_{i\,j_i}^*,\, \boldsymbol{s}_{-i}^*)$$

para todo $i = 1, \ldots, n$ *e para todo* $j_i = 1, \ldots, m_i$*, com* $m_i \geq 2$*.*

5 APLICAÇÕES DE TEORIA DOS JOGOS EM IDS

Um sistema de detecção de intrusão é uma importante técnica que vem sendo explorada para defesa de ataques e também tem a função de manter a segurança de sistemas de informação. Este capítulo tem como objetivo realizar um detalhamento dos trabalhos nos quais foi aplicada a Teoria dos Jogos para a modelagem de *IDSs*.

5.1 Trabalhos estudados

Tabela 1 – Trabalhos com aplicações de Teoria dos Jogos

Artigo	Tipo de Jogo	Objetivo	Dado
Fictitious play with imperfect observations for network intrusion detection Nguyen et al. 2008	Soma de zero	Modelo de jogadores fictícios	Simulação númerica
Dynamic policy-based IDS configuration Zhu and Basar 2009	Estocástico	Configuração dinâmica e iterativa IDS	Simulação númerica
A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks Chen et al. 2009	Soma não-nula	Melhor ação perante um ataque	Simulação númerica
Intrusion Detection System Stiborek et al. 2012	Soma não-nula	Auto-configuração IDS	CAMNEP System
Optimal Thresholds for Intrusion Detection Systems Laszka et al. 2016	Soma não-nula	Encontrar limiares de detecção para múltiplos IDSs	ADFA-LD intrusion

5.1.1 Nguyen et al. 2008

No trabalho de Nguyen et al. [37], no cenário de detecção de intrusão foi modelado um jogo composto por dois jogadores fictícios, um atacante e o outro um sistema de detecção de intrusão. O jogo foi modelado utilizando uma matriz de soma não-nula. Cada um dos jogadores possuem duas possibilidades de ação, o atacante pode decidir atacar ou não e o *IDS* de monitorar ou não. Os jogadores não possuem acesso a função de *payoff* do outro jogador, logo é um jogo de informação incompleta.

As estratégias dos jogadores são ajustadas com base na observação das ações tomadas pelo outro jogador. No entanto, a observação não é precisa devido as limitações entre os canais de comunicação que conectam os jogadores, limitações estas que não foram mencionadas no trabalho. Foi analisado à convergência das estratégias dos jogadores para um Equilíbrio de Nash. Também foi abordado o efeito da imperfeição do meio de transmissão sobre a convergência para o NE e o resultado do jogo.

O conjunto de jogadores foi representado como sendo P_i e as funções de utilidade $U_i(p_i, p_{-i})$:

$$U_1(p_1, p_2) = p_1^T M_1 p_2 + H(p_1)$$

$$U_2(p_2,\, p_1) = p_2^T M_2 p_1 + H(p_2)$$

onde M_i é matriz de *payoff* do jogador P_i, $i = 1{,}2$; $H(p_i)$ é o vetor de entropia de probabilidade.

5.1.2 Zhu e Basar 2009

Zhu e Basar [38] propuseram um modelo de jogo soma de zero não cooperativo para solucionar o problema da configuração dinâmica e iterativa de um *IDS*, com o objetivo de balancear os níveis de segurança e o desempenho do sistema. Os tipos de jogadores modelados neste problema foram atacante e detector.

Primeiro foi modelado um jogo para especificar as funções de custo resultantes entre as interações do atacante e do detector. Em seguida foi modelado uma estrutura de jogo estocástica dinâmica para projetar políticas estacionárias ótimas ou estratégias para configuração do *IDS* em diferentes estados do sistema. Na estrutura do jogo estocástico, a modelagem das interações entre o atacante e o detector foram feitas como um processo de decisão Markov competitivo, no qual as transições entre os estados do sistema dependem das ações de cada jogador. Os autores também introduziram algoritmos *Q-Learning* para obter os *payoffs* no jogo estocástico no caso em que as probabilidades de transição são praticamente desconhecidas.

Para a construção do processo de decisão Markov competitivo é considerado que um sistema de computação pode estar em n estados, e um detector possui um conjunto finito de bibliotecas para detecção de ataques. Cada uma das bibliotecas possuem custo de configuração. Por outro lado, cada atacante possui diferentes tipos de estratégias de ataque. Quando ocorre um ataque é causado um dano caso o mesmo não seja detectado. Conforme foi considerado o jogo entre o detector e o atacante como sendo um jogo estocástico, em cada instante k o sistema encontra-se em um estado. As ações tomadas pelo detector e pelo atacante no tempo k determinam as transições de probabilidades para o próximo estado. A função de custo da interação entre os jogadores é dado pela combinação do dano causado pelo ataque e o custo para detecção em uma determinada política de configuração.

5.1.3 Chen et al. 2009

No trabalho de Chen et al. [39] foi abordado o problema de detecção de intrusão em ambiente de rede heterogêneas que consiste em um ambiente onde os nós possuem diferentes e não-correlacionadas questões de segurança. Os autores investigaram qual é o comportamento de um atacante racional e qual é a melhor estratégia a ser tomada pelo defensor perante um ataque. Foi desenvolvido um modelo de jogo teórico não-cooperativo para o problema de detecção de intrusão em redes.

As contribuições proposta pelos autores foram em fornecer um *framework* teórico de um jogo em uma rede heterogênea onde os alvos possuem diferentes abordagens de segurança e também tendo modelado o comportamento esperado do ataque, quais serão os recursos mínimos exigidos para o monitoramento e qual é a estratégia ótima a ser tomada pelo defensor.

Os autores consideram a rede como sendo um tripla

$$N = (S_d, S_a, T)$$

onde S_d é o conjunto de agente equipados com o módulo de *IDS*, nomeados como sendo defensores, S_a é o conjunto de atacantes e T é o conjunto de nós da rede que podem ser atacados, que foram nomeados como alvo.

Para exemplificar o jogo foi considerado apenas um atacante e um defensor. O objetivo do atacante é realizar o seu ataque sem ser detectado, portanto o atacante possui um vetor de distribuição de probabilidade de ataque sobre o conjunto de alvos da rede. Já o objetivo do defensor é detectar os ataques, para realizar tal atividade ele monitora os alvos com um vetor de probabilidade. Caso um ataque não seja detectado o atacante possui um *payoff* positivo, já o defensor negativo. Por outro lado, quando um ataque é detectado os *payoffs* invertem, a do atacante passa a ser negativa e do defensor positiva.

5.1.4 Stiborek et al. 2012

Stiborek et al. [4] propuseram um modelo de jogo teórico para melhorar o processo de auto-adaptação dentro de um sistema de detecção de intrusão que possibilite a configuração dinâmica do sistema. O processo do jogo foi modelado como uma seleção de estratégias em único estágio de soma não-nula, que é constituído por dois jogadores: atacante e defensor. As funções de utilidade e o modelo de jogo foram baseado no trabalho de Chen et al. [39]. O modelo de jogo é combinação entre as prioridades e as estratégias dos dois jogadores. O conjunto de estratégia para o defensor é definido como sendo a seleção de configuração do *IDS* e a do atacante é escolha de um ataque específico.

A integração entre o modelo teórico do jogo com o processo de adaptação foi definido com sendo o seguinte conjunto de passos: estimativa de parâmetros dinâmico do sistema, definição do jogo, solução do jogo e por fim a integração do resultados de volta ao sistema para reconfiguração. A Figura 4 ilustra a arquitetura prevista pelo autor para a realização deste processo de integração.

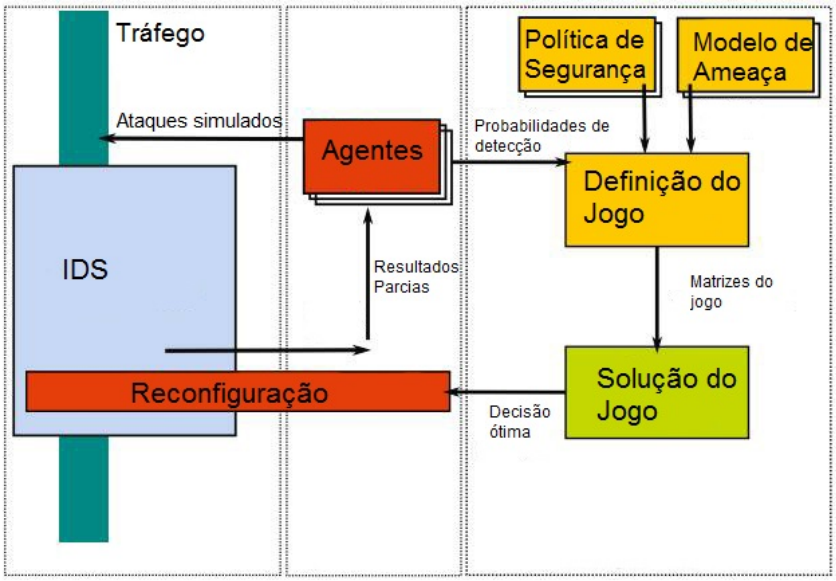

Figura 4 – Integração do jogo com o IDS. (Adaptado de [4])

O autor combinou duas formas de integração do processo entre o jogo e o IDS:

- Integração *offline*: Quando o jogo é definido e resolvido analiticamente e os parâmetros do sistema são configurados de acordo com os resultados.
- Integração direta *online*: Quando o jogo usa ações adversas previstas no tráfego da rede observado para definir o jogo. Esta definição é feita considerando as ações reais de um atacante perante a rede.

A combinação das duas técnicas foi nomeada como integração indireta online. Esta solução utilizou uma amostra controlada do comportamento do tráfego da rede legítimo e anômalo juntamente com o tráfego real. Neste caso o tráfego real é usado em conjunto com ataques hipotéticos, em que é utilizado como entrada para o *IDS* e a resposta do sistema é usada como entrada para a definição do jogo.

5.1.5 Laszka et al. 2016

Laszka et al. [40] realizaram um estudo para encontrar limiares de detecção para múltiplos *IDSs* perante a ataques estratégicos. Foi modelado ataques racionais contra um conjunto de sistema de computador que são equipados com *IDSs* como um jogo entre duas classes de jogadores: Atacantes e Defensores. O trabalho buscou estudar a complexidade computacional de encontrar ataques e estratégias de defesa ótima. O autor também demonstrou matematicamente que encontrar uma estratégia de defesa ótima é um problema NP-difícil.

Para a modelagem do jogo foi assumido que um defensor tem que proteger um conjunto de sistemas de computador S, em que cada um deles é equipado com um *IDS*. Os *IDSs* podem gerar dois tipos de erros: o primeiro, gerar alarmes para tráfego legítimos da rede, ou seja, um erro de falso-positivo; já o segundo é não disparar alarmes quando um ataque ocorreu, gerando portanto, um erro de falso-negativo. A estratégia do defensor é selecionar uma taxa de probabilidade de falso positivo para cada sistema S, definindo o limiar de detecção. Já do atacante é escolher um conjunto de sistemas A para atacar. Em relação as funções de *payoff*, foi modelado para o defensor a quantidade de dano causado pelo ataque não detectado e a quantidade de recursos desperdiçados ao investigar falsos alarmes. E a do atacante é o dano causado por ataque bem sucedido.

Para encontrar o limiar de detecção do *IDS* foi proposto um algoritmo iterativo em que o limiar é inicializado de forma aleatória e a cada iteração é gerada uma nova solução, se esta nova solução foi melhor em termos de minimizar a perda do defensor, então a solução anterior é substituída pela nova. No entanto se a solução aumentar a perda do defensor a nova solução substitui a anterior com uma pequena probabilidade. As substituições são feitas com o intuito de evitar que a solução seja um mínimo local.

O sistema proposto foi avaliado numericamente utilizando o ADFA-LD um *daset* público de detecção de intrusão contendo registros de chamadas de sistema. O teste foi realizado utilizando três sistemas de computação e a partir de 2000 iterações a taxa de perda do defensor estabilizou.

6 MODELO DE UM JOGO TEÓRICO PARA ENCONTRAR LIMIARES DE UM DSNSF

Neste capítulo será apresentado um modelo de jogo teórico para encontrar limiares para assinatura digital de segmentos de redes utilizando análises de fluxos (*Digital Signature of Network Segment using Flow Analysis - DSNSF*). Esta definição é considerada como sendo o comportamento normal da rede.

6.1 Caracterização do tráfego

O comportamento normal do tráfego é gerado com base em dados históricos coletados da rede. Nesta aplicação é gerado um *DSNSF* para cada dia da semana separadamente, pois o tráfego de rede é baseado em ciclos. Esta análise resulta em uma diminuição de erro na geração da assinatura para um determinado dia. Cada arquivo a ser analisado é representado por uma matriz composta por M x N dimensões, M representa cada segundo do tráfego coletado, já N representa as dimensões a serem analisadas.

Os dados utilizados neste trabalho para a geração do *DSNSF* foram coletados do tráfego da Universidade Estadual de Londrina referente às datas de 10 de setembro de 2012 a 12 de outubro de 2012, totalizando portanto, cinco semanas de coletas de dados. Para cada dia da semana, foram analisadas as quatros semanas anteriores para criação do *DSNSF* utilizando média ponto-a-ponto do tráfego. Cada dia da semana possui um arquivo no qual contêm 86400 pontos, ou seja, cada ponto representa um segundo de observação daquele dia.

6.2 Definição do jogo

O jogo é composto por um conjunto G de dois jogadores: o *DSNSF* e o *tráfego*. Cada um dos jogadores possui um conjunto S de estratégia. O *DSNSF* possui duas estratégias, aumentar ou diminuir o limiar do tráfego aceito como normal. As estratégias do *tráfego* são: tráfego com anomalia e normal. O objetivo do *DSNSF* é diminuir a taxa de falso-positivo, portanto o modelo de jogo aplicado busca encontrar limiares para diminuir esta taxa.

O modelo aqui apresentado é um jogo dinâmico, ou seja, as ações são tomadas em múltiplos estágios. Todos os jogadores conhecem as ações anteriores tomadas e a função de ganho de cada jogador, logo podemos classificá-lo como sendo um jogo de informação perfeita e completa, conforme já foram apresentadas as definições no Capítulo 4.

Os limiares de aceitação do *DSNSF* inicialmente são valores aleatórios entre 5% e

30% em cada ponto de observação, com objetivo de eliminar ótimos locais. As correções destes limiares são realizadas iterativamente no decorrer do jogo e das ações tomadas pelos jogadores. Quando o tráfego é normal e o *DSNSF* toma decisão de aumentar o limiar o seu ganho é positivo, mas caso o *tráfego* possuía anomalia seu ganho é negativo. Já quando o *tráfego* possuir um comportamento normal e o *DSNSF* tomar a decisão de diminuir esse limiar o seu ganho é negativo, no entanto se o comportamento for anômalo seu ganho é positivo. As ações do *DSNSF* possuem como base as ações anteriores tomadas pelo *tráfego*. As ações e os ganhos de cada jogador é ilustrada na Tabela 2.

Tabela 2 – Ganho e Ações do Jogo

		Tráfego	
		Normal	Anomalia
DSNSF	aumentar	(positivo, negativo)	(negativo, positivo)
	diminuir	(negativo, positivo)	(positivo, negativo)

Uma modificação realizada na modelagem do jogo foi o fato de tomar como premissa que apenas o *DSNSF* busca o melhor ganho. Pois na modelagem convencional ambos os jogadores buscam otimizar o seu ganho. No entanto como o foco deste trabalho é otimizar o limiar do *DNSNF*, o ganho *tráfego* não foi considerado.

6.3 Resultados do jogo teórico proposto

Para a geração de todos os testes foi utilizado o intervalo de tempo das 7 às 21 horas, ou seja, este intervalo de tempo representa um dia de trabalho na universidade. O *DSNSF* foi gerado utilizando quatro semanas para otimizar um instante que representa um ponto do tráfego da rede no intervalo de observação.

O *DSNSF* foi gerado para os dias 08, 09, 10, 11 e 12 de Outubro de 2012. Um ponto que dever ser considerado, no dia 12 é um feriado nacional, que resultou um DSNSF com pouco ajuste.

No tráfego real dos dias 08 à 12 foram injetados anomalias de *DoS* utilizando a ferramenta "*Scorpius - sflow anomaly simulator*"[41] no intervalo de tempo das 15 às 16 horas. Essas anomalias foram injetadas ao tráfego com objetivo de atender a formulação do jogo proposto, em que as estratégias do *tráfego* é *anomalia* ou *normal*.

Quando ocorre uma anomalia de *DoS* ocorre um pico no aumento de pacotes que trafegam pela rede, logo a dimensão analisada foram o número de pacotes para a geração do *DSNSF*, conforme pode ser observados nas figuras 5, 6, 7, 8, 9. A área hachurada em verde representa o tráfego real, a curva em vermelho é o *DSNSF* gerado e a área hachurada em azul representa os limiares encontrados com o modelo de jogo teórico proposto neste trabalho.

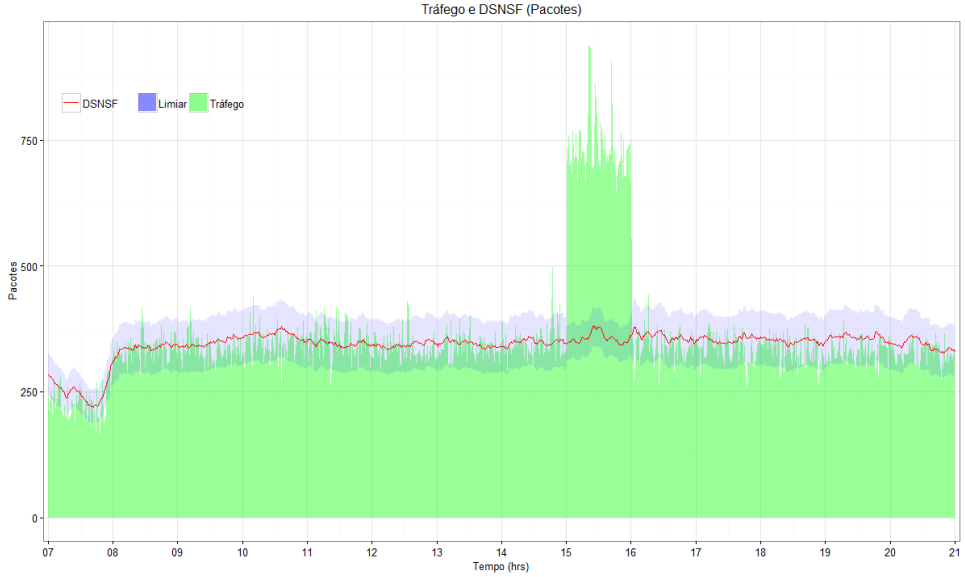

Figura 5 – Tráfego real de Pacostes/s e DSNSF gerado do dia 08 de Outubro de 2012.

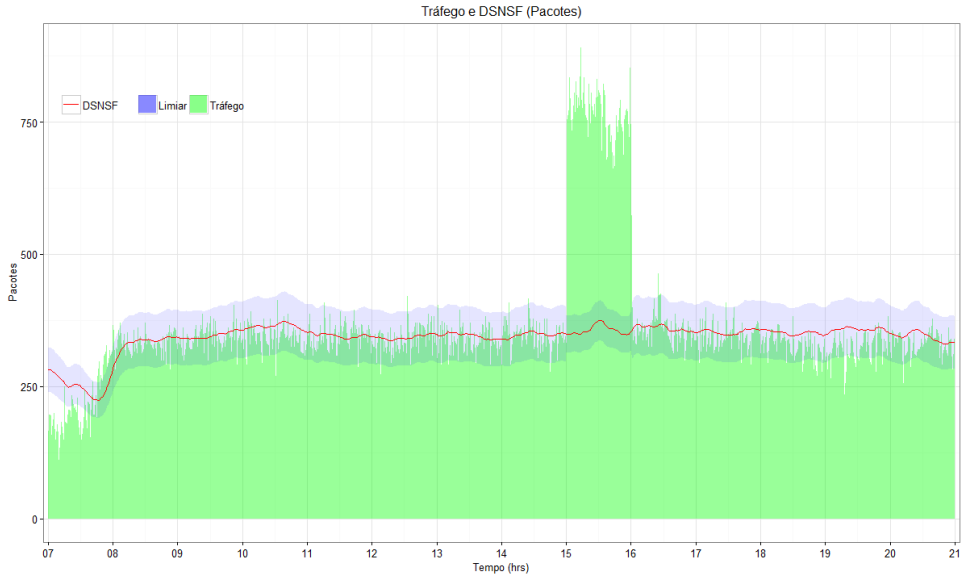

Figura 6 – Tráfego real de Pacostes/s e DSNSF gerado do dia 09 de Outubro de 2012.

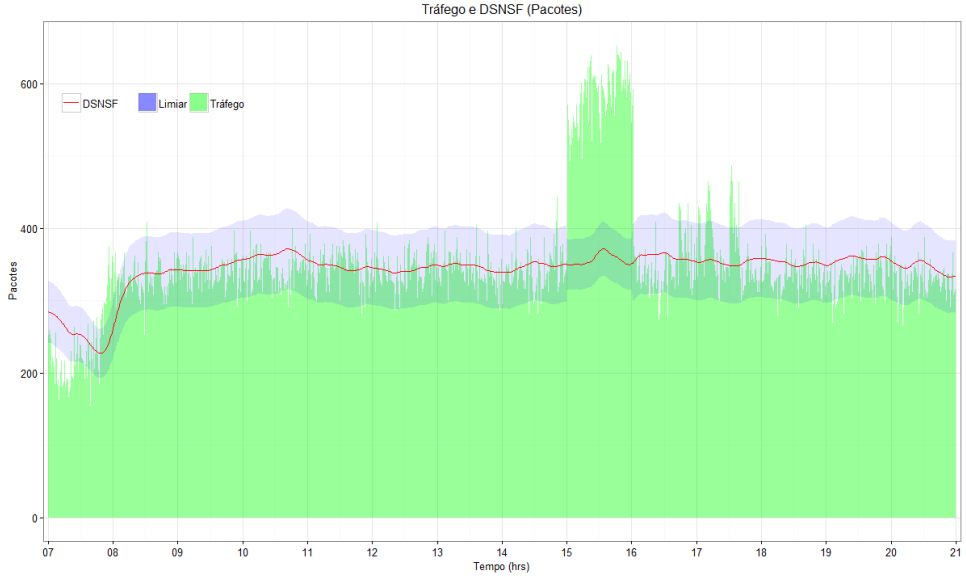

Figura 7 – Tráfego real de Pacostes/s e DSNSF gerado do dia 10 de Outubro de 2012.

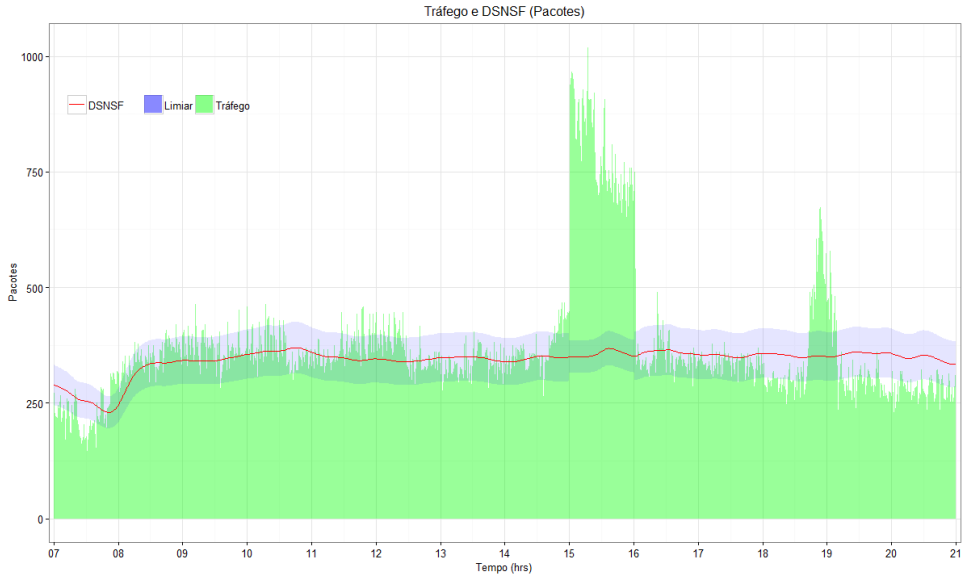

Figura 8 – Tráfego real de Pacostes/s e DSNSF gerado do dia 11 de Outubro de 2012.

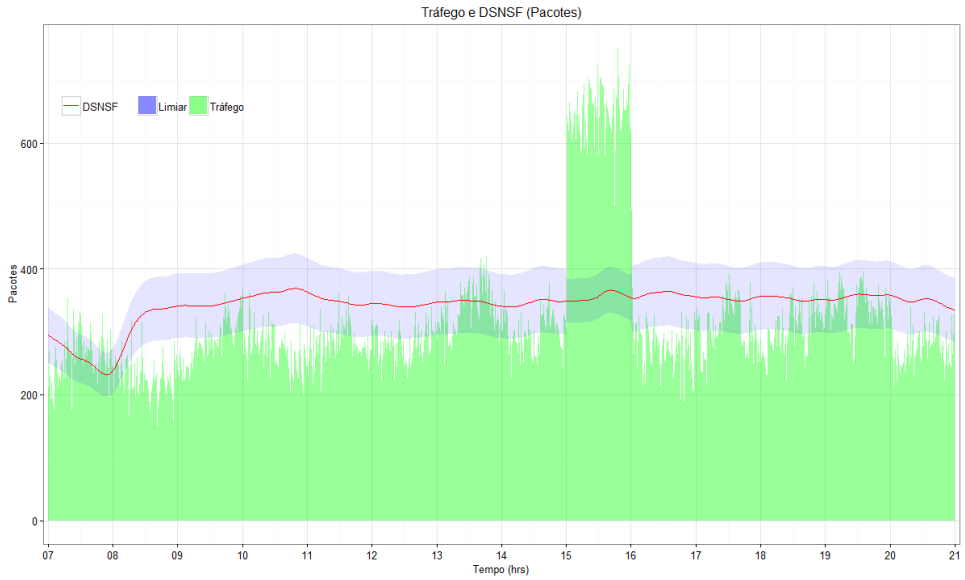

Figura 9 – Tráfego real de Pacostes/s e DSNSF gerado do dia 12 de Outubro de 2012.

Os limiares encontrados com a solução do jogo variaram entre 10% à 15%. Os limiares com menor valor foram aqueles que ocorreram quando o tráfego era anômalo. Justificando o fato de que quando o tráfego estivesse com anomalia a melhor decisão a ser tomada pelo *DSNSF* era reduzir o limiar de aceitação. Por outro lado, os limiares com valores próximos a 15% foram aqueles em que o tráfego não possuía nenhum tipo de anomalia. Em consequência desse fato há uma redução na taxa de falsos-positivos.

7 CONCLUSÃO

No campo de estudo de redes de computadores, a gerência de redes é uma área de pesquisa que vem sendo explorada amplamente por inúmeros pesquisadores, com o objetivo de desenvolver técnicas para auxiliar nesta complexa atividade. O trabalho aqui apresentado buscou realizar um estudo no qual fosse aplicada a Teoria dos Jogos nesta área de pesquisa. Para o desenvolvimento deste estudo foi realizada uma análise de alguns trabalhos presentes na literatura. O foco principal foi realizar o estudo de trabalhos nos quais a Teoria dos Jogos fosse aplicada em sistemas de detecção de Intrusão.

O *framework* matemático Teoria dos Jogos vem sendo utilizado para modelar problemas relacionados a segurança de redes, fornecendo modelos teóricos para auxiliar no processo de gerenciamento de redes de computadores no que diz respeito a tomada de decisões. No entanto, o *framework* não propõe uma solução ao problema, mas sim ele é utilizado para modelar e formalizar problemas em que existe o conflito entre duas ou mais partes. Cada uma das partes envolvidas busca obter o máximo de ganho possível, para melhorar o seu ganho os jogadores devem escolher a melhor estratégia. É neste sentido que a Teoria dos Jogos é utilizada para dar suporte no momento da escolha da melhor decisão.

De acordo com o que foi apresentado no Capítulo 5 notou-se que nos trabalhos analisados os jogos foram modelados entre dois tipos de jogadores, o atacante e o defensor. O defensores apresentados nos trabalhos eram os sistemas de detecção de intrusão, em que ações eram monitorar ou não monitorar. Também foi utilizada a Teoria dos Jogos para modelar a melhor configuração a ser tomada por um a *IDS*. Uma outra abordagem adotada, era que a solução do jogo fosse utilizada para auto-configuração de um *IDS*. O objetivo dos atacantes é realizar um ataque sem ser detectado. Para isso foi modelado em alguns dos trabalhos um vetor de probabilidade para cada atacante e seu ataque. As soluções dos jogos geralmente são dadas pelo equilíbrio de Nash.

No Capítulo 6 foi apresentado um modelo de jogo teórico utilizando a técnica de geração de um perfil normal do tráfego da rede. O objetivo do jogo proposto foi encontrar limiares de aceitação desta assinatura gerada. Foram aplicadas anomalias de *DoS* ao tráfego da rede com o intuito de comparar com a assinatura gerada através das quatros semanas de observação. Como trabalho futuro espera-se fazer uma análise utilizando outras dimensões disponíveis em fluxos de rede, por exemplo, *bit*, *IP* e porta de origem e destino.

Em relação as contribuições esperadas com o estudo realizado neste trabalho, espera-se contribuir com aqueles que buscam compreender um pouco mais da aplicação

de Teorias dos Jogos em redes de computadores e detecção de anomalias, principalmente na área de detecção de intrusão. Que os conceitos aqui abordados possam servir como base de consulta para aqueles que possuem interesse em desenvolver trabalhos nesta área de pesquisa.

REFERÊNCIAS

[1] SOFTWARE, C. Introduction to cisco ios netflow - a technical overview. 2012. Disponível em: <http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html>.

[2] SFLOW. Traffic monitoring using sflow. 2003. Disponível em: <http://www.sflow.org/sFlowOverview.pdf>.

[3] TRAMMELL, B.; BOSCHI, E. An introduction to IP flow information export (IPFIX). *IEEE Communications Magazine*, v. 49, n. 4, p. 89–95, 2011. ISSN 01636804.

[4] STIBOREK, J. et al. Game Theoretical Adaptation Model for Intrusion Detection System. *Proceedings of 10th International Conference on Practical Applications of Agents and Multi-Agent Systems*, p. 291–294, 2012.

[5] ZHANG, W.; YANG, Q.; GENG, Y. A survey of anomaly detection methods in networks. *Proceedings - 1st International Symposium on Computer Network and Multimedia Technology, CNMT 2009*, p. 9–11, 2009.

[6] FUCHSBERGER, A. Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report*, v. 10, n. 3, p. 134–139, 2005. ISSN 13634127.

[7] MANSHAEI, M. H. et al. Game theory meets network security and privacy. *ACM Comput. Surv.*, ACM, New York, NY, USA, v. 45, n. 3, p. 25:1–25:39, jul. 2013. ISSN 0360-0300. Disponível em: <http://doi.acm.org/10.1145/2480741.2480742>.

[8] ROY, S. et al. A survey of game theory as applied to network security. In: *2010 43rd Hawaii International Conference on System Sciences*. [S.l.: s.n.], 2010. p. 1–10. ISSN 1530-1605.

[9] LIANG, X.; XIAO, Y. Game Theory for Network Security. *IEEE Communications Surveys & Tutorials*, v. 15, n. 1, p. 472–486, 2013. ISSN 1553-877X. Disponível em: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6238282>.

[10] GHORBANI, M.; GHORBANI, H. R.; HASHEMI, M. R. Configuration Strategies For Collaborative IDS Using Game Theory. p. 261–266, 2016.

[11] LIU, P.; ZANG, W.; YU, M. Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security*, v. 8, n. 1, p. 78–118, 2005. ISSN 10949224.

[12] SPYRIDOPOULOS, T. et al. A game theoretic defence framework against dos/ddos cyber attacks. *Computers Security*, v. 38, p. 39 – 50, 2013. ISSN 0167-4048. Cybercrime in the Digital Economy. Disponível em: <http://www.sciencedirect.com/science/article/pii/S016740481300059X>.

[13] FERNANDES, G. et al. Network anomaly detection using IP flows with Principal Component Analysis and Ant Colony Optimization. *Journal of Network and Computer Applications*, Elsevier, v. 64, p. 1–11, 2016. ISSN 10848045. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1084804516000618>.

[14] HAMAMOTO, A. H.; CARVALHO, L. F.; PROENÇA Jr., M. L. ACO and GA metaheuristics for anomaly detection. *Proceedings - International Conference of the Chilean Computer Science Society, SCCC*, v. 2016-February, 2016. ISSN 15224902.

[15] CHEN, Z. et al. Combining MIC Feature Selection and Feature-based MSPCA for Network Traffic Anomaly Detection. p. 176–181, 2016.

[16] ZHAO, X.; WANG, G.; LI, Z. Unsupervised network anomaly detection based on abnormality weights and subspace clustering. In: *2016 Sixth International Conference on Information Science and Technology (ICIST)*. [S.l.: s.n.], 2016. p. 482–486.

[17] STALLINGS, W. *SNMP, SNMPv2 and RMON Practical NetworkManagement*. 2st. ed. [S.l.]: Addison-Wesley, 1993.

[18] CASE J. CASE, M. S. J. D. J. A simple network management protocol (snmp). 1990. Disponível em: <https://www.ietf.org/rfc/rfc1157.txt>.

[19] LI, B. et al. A survey of network flow applications. *Journal of Network and Computer Applications*, Elsevier, v. 36, n. 2, p. 567–581, 2013. ISSN 10848045. Disponível em: <http://dx.doi.org/10.1016/j.jnca.2012.12.020>.

[20] COUTO, A. V. do. *Uma abordagem de Gerenciamento de Redes baseado no Monitoramento de Fluxos de Tráfego Netflow com o suporte de Técnicas de Business Intelligence*. Dissertação (Mestrado) — Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica, Brasília, 2012.

[21] PHAAL S. PANCHEN, N. M. P. Inmon corporation's sflow: A method for monitoring traffic in switched and routed networks. 2001. Disponível em: <hhttps://www.ietf.org/rfc/rfc3176.txt>.

[22] QUITTEK T. ZSEBY, B. C. S. Z. J. Requirements for ip flow information export (ipfix). 2004. Disponível em: <https://tools.ietf.org/html/rfc3917>.

[23] THOTTAN, M.; JI, C. Anomaly Detection in IP Networks. v. 51, n. 8, p. 2191–2204, 2003.

[24] ZARPELAO, B. B. *Detecção de Anomalias em Redes de Computadores*. Tese (Doutorado) — Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, 2010.

[25] STADING, T.; MANIATIS, P.; BAKER, M. Peer-to-peer caching schemes to address flash crowds. In: _____. *Peer-to-Peer Systems: First InternationalWorkshop, IPTPS 2002 Cambridge, MA, USA, March 7–8, 2002 Revised Papers*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002. p. 203–213. ISBN 978-3-540-45748-0. Disponível em: <http://dx.doi.org/10.1007/3-540-45748-8_19>.

[26] ARI, I. et al. Managing flash crowds on the internet. In: *Modeling, Analysis and Simulation of Computer Telecommunications Systems, 2003. MASCOTS 2003. 11th IEEE/ACM International Symposium on*. [S.l.: s.n.], 2003. p. 246–249. ISSN 1526-7539.

[27] TSENG, Y.-C.; NI, S.-Y.; SHIH, E.-Y. Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network. *IEEE Transactions on Computers*, v. 52, n. 5, p. 545–557, May 2003. ISSN 0018-9340.

[28] SINGH, A. K.; MEENU. A survey on congestion control mechanisms in packet switch networks. In: *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*. [S.l.: s.n.], 2015. p. 902–906.

[29] ROUGHAN, M. et al. Ip forwarding anomalies and improving their detection using multiple data sources. In: *Proceedings of the ACM SIGCOMM Workshop on Network Troubleshooting: Research, Theory and Operations Practice Meet Malfunctioning Reality*. New York, NY, USA: ACM, 2004. (NetT '04), p. 307–312. ISBN 1-58113-942-X. Disponível em: <http://doi.acm.org/10.1145/1016687.1016703>.

[30] CERT.BR. *Cartilha de Segurança para Internet, versão 4.0*. Comitê Gestor da Internet no Brasil, 2012. ISBN 978-85-60062-54-6. Disponível em: <http://cartilha.cert.br/livro/>.

[31] SRIDHARAN, A.; YE, T.; BHATTACHARYYA, S. Connectionless port scan detection on the backbone. In: *2006 IEEE International Performance Computing and Communications Conference*. [S.l.: s.n.], 2006. p. 10 pp.–576. ISSN 1097-2641.

[32] PROENÇA Jr, M. L. *Baseline Aplicado a gerência de redes*. Tese (Doutorado) — Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, 2005.

[33] BA, G. G. S. *Uma introdução a teoria dos jogos*. 1st. ed. [S.l.]: II Bienal da SBM, 2004.

[34] VARIAN, H. R. *Intermediante Microeconomics*. [S.l.]: W. W. Norton Company, 2005. ISBN 0-393-92702-4.

[35] SCHOUERY O. LEE, F. K. M. E. C. X. R. C. S. *Tópicos da teoria dos Jogos em Computação*. [S.l.: s.n.], 2015.

[36] GIBBONS, R. *Game Theory for Applied Economists*. 1st. ed. [S.l.]: Princeton University Press, 1992.

[37] NGUYEN, K. C.; ALPCAN, T.; BASAR, T. Fictitious play with imperfect observations for network intrusion detection. *Urbana*, v. 51, p. 61801, 2008.

[38] ZHU, Q.; BAşAR, T. Dynamic policy-based IDS configuration. *Proceedings of the IEEE Conference on Decision and Control*, p. 8600–8605, 2009. ISSN 01912216.

[39] CHEN, L. C. L.; LENEUTRE, J. A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks. *IEEE Transactions on Information Forensics and Security*, v. 4, n. 2, p. 165–178, 2009. ISSN 1556-6013.

[40] LASZKA, A. et al. Optimal Thresholds for Intrusion Detection Systems. *Symposium and Bootcamp on the Science of Security (HotSoS)*, p. 72–81, 2016. Disponível em: <http://aronlaszka.com/papers/laszka2016optimal.pdf>.

[41] SCORPIUS - sflow anomaly simulator. Disponível em: <http://redes.dc.uel.br/scorpius>.