MANFRED HEIL JUNIOR

PROPOSTA DE UM SISTEMA DE DETECÇÃO DE INTRUSÃO UTILIZANDO UMA ABORDAGEM COLABORATIVA

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática.

Curitiba
2013

MANFRED HEIL JUNIOR

PROPOSTA DE UM SISTEMA DE DETECÇÃO DE INTRUSÃO UTILIZANDO UMA ABORDAGEM COLABORATIVA

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Pontifícia Universidade Católica do Paraná como requisito parcial para obtenção do título de Mestre em Informática.

Área de Concentração: Ciência da Computação

Orientador: Prof. Dr. Manoel C. de O. Penna Neto

Curitiba
2013

Heil Jr, Manfred
PROPOSTA DE UM SISTEMA DE DETECÇÃO DE INTRUSÃO UTILIZANDO UMA ABORDAGEM COLABORATIVA. Curitiba, 2013.

Dissertação - Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Informática.

1. Segurança da informação 2. Sistemas de detecção de intrusão (IDS) 3. Sistema de detecção de intrusão colaborativo (CIDS) I.Pontifícia Universidade Católica do Paraná. Centro de Ciências Exatas e Tecnologia. Programa de Pós-Graduação em Informática.

Dedico a minha esposa, Priscila de Oliveira Vargas e meus amigos da Pós-Graduação.

Agradecimentos

Gostaria de agradecer primeiramente ao meu orientador prof^o Dr. Manoel C. de O. Penna Neto pela dedicação, apoio e motivação durante todo este tempo em que passei no PPGiA.

Aos professores do Programa de Pós Graduação em Informática Aplicada da PUCPR, principalmente aqueles que convivi. Ao meu amigo Mauricio Henning que me apoio na conclusão dessa etapa de minha vida, a Carol Fung que disponibilizou informações importantes sobre seu projeto, que ajudaram a construir esse projeto. A minha esposa Priscila de Oliveira Vargas por sempre estar ao meu lado me apoiando para que não desistisse no meio do caminho. Também agradeço a todos que de alguma forma contribuíram para que eu alcançasse meus objetivos.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Devido ao aumento do uso de computadores nas últimas décadas cada vez mais os usuários de sistemas informatizados vem utilizando a Internet. Nos últimos anos o ataque à estrutura da Internet vem se tornando mais sofisticados e difíceis de detectar. As intrusões podem ser de várias formas como: *worms, spamwares, vírus, spyware, DDoS* e outros. Causando prejuízos incalculáveis para a sociedade como em casos de invasões a sistemas que possuem milhares de informações pessoais de usuários, como dados bancários. E há também a indisponibilidade de sistemas deixando de atender a milhares de requisições de seus usuários. Na academia muitos trabalhos estão sendo desenvolvidos para tratar esses tipos de incidentes, classificados de IDS (Sistemas de Detecção de Intrusão), aplicadas a estruturas locais ou distribuídas. Um dos problemas envolvidos nos estudos é a detecção de intrusão, que geram decisões falsas positivas ou verdadeiras negativas que podem degradar a utilização do IDS. Uma proposta para resolver esse problema é o CIDS (IDS Colaborativos), onde os nós colaboram entre si para melhorar a precisão e diminuir o índice de decisões falsas positivas ou verdadeiras negativas. Esse projeto apresenta uma proposta de uso de CIDS com o modelo matemático de *Dempster-Shefer* para colaboração dos nós participantes utilizado para avaliar o custo na detecção de intrusão. Após o resultado foi possível identificar que a proposta apresentada gera um valor satisfatório na análise dos resultados, podendo ser aplicado no uso de detecção de intrusão.

Palavras-chave: Segurança da Informação. Sistemas de Detecção de Intrusão (IDS). Sistema de Detecção de Intrusão Colaborativo (CIDS).

Abstract

Because of the increased use of computers in the last decades more and more users of computer systems has been using the Internet. In recent years the attack on the Internet structure is becoming more sophisticated and hard to detect. Intrusions can be in various forms such as worms, spamwares, viruses, spyware, and other DDoS. Causing enormous damage to society as in the cases of invasions systems that have thousands of users' personal information such as bank details. And there is also the unavailability of systems failing to meet the thousands of requests from its users. At the academy many works are developed to deal with these kinds of incidents, classified IDS (Intrusion Detection Systems), applied to local structures or distributed. One of the problems involved in these studies is the intrusion detection decisions which generate false positive or true negative that may degrade the use of IDS. A proposal to solve this problem is the CIDS (Collaborative IDS), where nodes work together to improve accuracy and reduce the number of false positive decisions or true negative. This project presents a proposal for use of CIDS with the mathematical model of Dempster-Shefer for collaboration of participating nodes used to evaluate the cost in intrusion detection. After the resultit was identified that the proposal generates a satisfactory analysis of the results, it can be applied in the use of intrusion detection.

Keywords: Information System. Intrusion Detection Systems (IDS). Collaborative Intrusion Detection System (CIDS).

Capítulo 1

Introdução

O avanço tecnológico esta cada vez mais presente em nossa sociedade fornecendo uma quantidade considerável de dispositivos para acesso a Internet. Porém novas ameaças à segurança estão aparecendo causando preocupações a comunidade. Assim pesquisas vem surgindo para estudar soluções para proteger os usuários e seus equipamentos.

Recentemente a Sony sofreu uma invasão ao seu sistema com os dados dos usuários. Segundo (MAGAZINE, 2011) os invasores conseguiram ter acesso aos dados pessoais de mais de 70 milhões usuários que utilizam o dispositivo Playstation 3. O governo brasileiro também sofreu com ataques aos sites da Presidência da República e do Governo do Brasil no ano de 2011 causando uma sobrecarga nos sistemas (GLOBO, 2013). Tais ameaças segundo (CENTER, 2003), tiveram um aumento de ordem exponencial em 10 anos.

Diversas propostas como Fung (FUNG; ZHANG; BOUTABA, 2010) sugerem uma aplicação de IDS colaborativa baseado em HIDS (*Host IDS*), com ênfase em gestão do conhecimento utilizando aprendizagem *Baysiana* para agregação de opinião sobre intrusão. Outros trabalhos utilizados como o (FARROUKH et al., 2008) utilizam de técnicas de IDS centralizado e colaborativos para detecção de intrusão, onde seus resultados mostraram-se comparáveis ao método centralizado. Verifica-se que há muitas soluções, mas que não há uma solução definitiva para o problema de intrusão de sistemas, devido a vários fatores como a identificação precisa de intrusos (ZHOU; LECKIE; KARUNASEKERA, 2010).

O Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC) faz uso de colaboração como característica determinante desse projeto. Seu principal objetivo é detectar de forma eficaz e eficiente uma intrusão, utilizando técnica de colaboração, que consistem na análise, consulta e atualização de base de intrusão entre seus colaboradores. Os resultados obtidos indicam que o SIDIAC tem um bom desempenho em relação as demais propostas utilizadas como (FUNG; ZHANG; BOUTABA, 2010) e (FARROUKH et al., 2008), apresentando um desempenho promissor.

1.1 Desafio

Atualmente existem milhões de dispositivos conectados à Internet e suas aplicações dependem do funcionamento da rede para utilização de serviços como email, navegação nos websites, redes sociais, chats dentre outros utilizados todos os dias. Ao mesmo tempo, intrusões nessa rede estão se tornando uma grave ameaça aos usuários, e nos últimos anos tais intrusões estão se tornando cada vez mais sofisticadas. Invasores tentam controlar grupos de computadores para lançar ataques distribuídos, diante disso, um sistema de detecção de intrusão isolado (local) pode não solucionar o problema da rede, mantendo-se as vezes desatualizado aos tipos de ataques.

Nos últimos anos pesquisas tem buscado soluções para sistemas de detecção de intrusão, onde novos projetos pretendem tratar essas novas ameaças com uma solução distribuída, tentando melhorar a eficiência da detecção. Desenvolver uma solução colaborativa que vise tratar de forma mais eficiente e precisa os tipos de intrusão foi um desafio interessante em comparação às abordagens locais que hoje são encontradas. Este projeto demonstrou ser um grande desafio e estudos nesta linha de pesquisa deveriam surgir para corroborar à academia.

1.2 Motivação

A motivação dos hackers nos últimos anos vem mudando, ao invés de buscar popularidade estão visando lucro, no lugar de aumentar seu prestígio por desfigurar sites, agora eles utilizam o spam (envio de mensagens não solicitadas indiscriminadamente em massa), phishing (forma de roubo da identidade de um web site no intuito de obter informações privilegiadas) ou Negação de Serviços Distribuídos (Distributed Denial of Service - DDoS), como extorsão para ganho monetário ou até mesmo como espionagem empresarial (TZI-CKER, 2007).

Também o tipo de ataques à estrutura da Internet está se modificando. O uso de automação para atingir todos os computadores vulneráveis é um tipo de ataque em larga escala que pode ocorrer em vários domínios, e é uma tarefa extremamente difícil de ser detectada imediatamente. Um processo típico de ataque utilizando essa técnica são os ataques coordenados que usam as vulnerabilidades de software conhecidas que serviram para espalhar um *worm* (vírus) e assim comprometer os computadores, conhecidos como máquinas zumbis (*botnets*) que poderão ser controlado pelo atacante ou até vendidas no mercado *underground* (submundo) (ZHOU; LECKIE; KARUNASEKERA, 2010).

Utilizar uma solução colaborativa para detectar tais ataques de forma eficiente e

eficaz é a maior motivação desse trabalho, pois atuando dessa forma procura-se melhorar a precisão do descobrimento do ataque e colaborar com os demais membros da rede para que possam se proteger de tal investida.

1.3 Proposta

Conforme pesquisa realizada por (RICHARDSON, 2008), 25% dos entrevistados relataram ataques de negação de serviço (*Denial of Service sigla DOS*), que causaram uma perda média de quinze mil dólares por entrevistado, isso se soma a cerca de três milhões de prejuízos devidos ataques de DOS em 2006 nos Estados Unidos. Os ataques que utilizam uma arquitetura distribuída são difíceis de se detectar. Os atuais sistemas não estão preparados para a detecção distribuída causando aumento nas taxas de alarmes falsos positivos e falsos negativos causando efeito negativo na credibilidade do sistema de detecção (RICHARDSON, 2008). Investigar uma solução viável para sistema de detecção de intrusão usando uma abordagem colaborativa para solucionar os problemas de detecção de forma eficiente e eficaz é a proposta desse projeto.

Os objetivos específicos desse trabalho são:

- Analisar os projetos de sistemas de detecção de intrusão que utilizam abordagem distribuída.
- Definir a arquitetura do sistema de detecção de intrusão colaborativa;
- Implementar um sistema de detecção de intrusão que utilize a abordagem colaborativa;
- Avaliar o desempenho do sistema proposto com os demais sistemas apresentados pela literatura através de simulações.

1.4 Organização do Trabalho

O Capítulo 2 descreve o referencial conceitual através da fundamentação teórica, contendo três seções, onde são apresentados os conceitos de sistema de detecção de intrusão, suas classificações quanto a origem dos dados, pelo processamento da informação, o tempo de detecção, o meio ambiente e a classificação pela arquitetura dos sistemas. No capítulo 2 também apresenta-se a revisão da literatura de artigos que apresentam a abordagem distribuída para detecção de intrusão, onde ao final do capítulo apresenta-se uma tabela com a classificação desses trabalhos.

O capítulo 3 apresenta o Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC) com suas características, sua arquitetura e suas funcionalidades.

O capítulo 4 descreve os experimentos e resultados obtidos através de um modelo de simulação com a descrição dos cenários utilizados e a análise do desempenho do SIDIAC. Seguido do Capítulo 5 que descreve as conclusões e perspectivas em trabalhos futuros.

Capítulo 2

Fundamentação Teórica

2.1 Sistema de Detecção de Intrusão

Normalmente na literatura os Sistemas de Detecções de Intrusões (*Intrusion Detection System*) são chamados de IDS. Muito conhecido atualmente, devido ao crescimento da rede mundial de computadores e aos dispositivos a ela ligados. Os IDS´s possuem basicamente três funcionalidades: *Anti-malwares, Firewall* e IDS. Uma analogia de um IDS é compará-lo a um sistema de alarme monitorado de uma residência. O proprietário ao sair de sua residência, tranca todas as portas e janelas, e liga o alarme, ao contrário em uma casa sem alarme onde o ladrão tem toda a liberdade de testar todas as trancas. Na casa monitorada ao tentar abrir uma porta ou janela irá disparar o alarme, e consequentemente irá informar a segurança monitorada dessa atividade e assim impossibilitando que o ladrão tenha sucesso em sua atividade criminosa, diferente da casa sem alarme que ele poderá furtar o que quiser.

Em um sistema de computação o IDS é um software que monitora a rede ou computador para procurar identificações de intrusão e alertar os ocorridos aos responsáveis, como o sistema de alarme. Para conhecer um pouco sobre IDS vamos ao início onde tudo começou. Em 1980 James Anderson escreveu um artigo *"Computer Security Threat"* onde tinha o objetivo de motivar o governo dos Estados Unidos a introduzir e organizar noções de auditoria das informações, assim podendo monitorar os usuários quando utilizassem recursos computacionais indevidamente. Em 1984 a Dra. Dorathy Denning publicou seu trabalho *"An Intrusion Detection Model"* que apresentou o primeiro modelo para detecção de intrusão chamado de IDES (*Intrusion Detection Expert System*) e no mesmo ano o projeto de IDES foi desenvolvido (INNELLA et al., 2001).

A partir desse ponto iniciaram-se estudos para melhorar a eficiência dos IDS´s.

Consequentemente foram criados muitos IDS´s com diversas empregabilidades, nas seções seguintes serão apresentadas as classificações para os tipos de IDS´s.

2.2 Classificação de IDS´s

Segundo estudo realizado por (SABAHI; MOVAGHAR, 2008) apresentam as diversas pesquisas para o desenvolvimento de IDS´s e suas abordagens, que elas são capazes de detectar vários tipos de ataques às redes. Atualmente há várias abordagens para IDS, classificadas em cinco grandes grupos, quanto a origem dos dados, pelo processamento das informações, pelo tempo de detecção, pelo meio ambiente e pela arquitetura. A Figura 2.1 ilustra um diagrama desses grupos, juntamente com suas classificações para cada grupo de IDS.

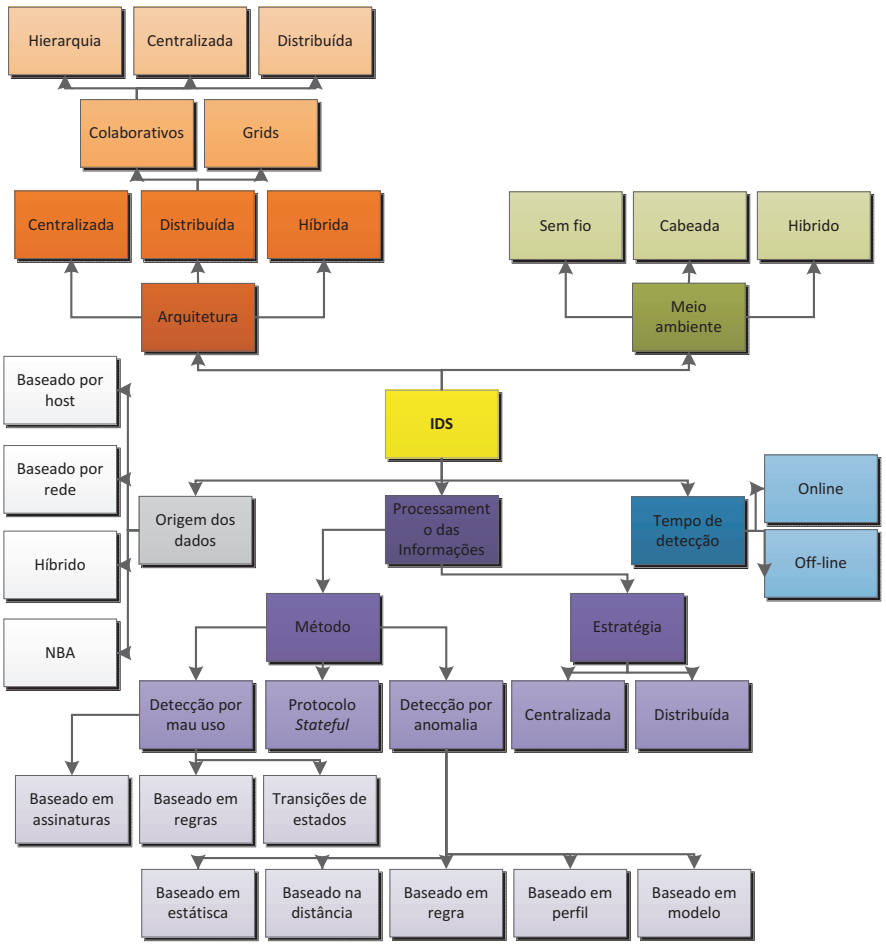

Figura 2.1: Diagrama de classificação dos tipos IDS. Adaptado de Sabahi and Movaghar (SABAHI; MOVAGHAR, 2008).

2.2.1 Classificação pela origem dos dados

Normalmente os IDS´s executam leitura de arquivos de dados para relacionar com os eventos de detecção de intrusão, esses dados podem ser usados para confirmar a validade dos alertas, investigar os incidentes e correlacionar os eventos entre o IDS (SCARFONE; MELL, 2007). A Figura 2.2 ilustra a classificação pela origem dos dados, criando quatro subclasses, que são:

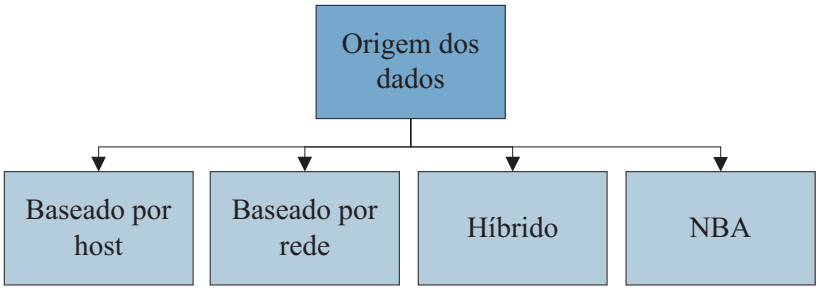

Figura 2.2: Classificação pela origem dos dados. Adaptado de Scarfone and Mell (SCARFONE; MELL, 2007).

- **Baseado por host**: foram um dos primeiro tipos de IDS que surgiram, são chamados de HIDS (Host IDS), composto por um software que monitoram arquivos de logs do sistema, tendo como objetivo de policiar os usuários que estão conectados a um *host* (MAGALHAES, 2006).

- **Baseado por rede**: devido à necessidade de detectar ameaças no âmbito das redes surgiram os NIDS (*Network* IDS), qual objetivo é de monitorar os pacotes que trafegam dentro das redes e também aplicar filtro no tráfego (MAGALHAES, 2006).

- **Híbrido**: esse tipo de IDS utiliza simultaneamente o tipo HIDS e o NIDS promovendo em conjunto uma melhor eficiência na detecção.

- **NBA (Netwok Behavior Analysis)**: são analisadores do tráfego da rede com a intenção de identificar ameaças que geram fluxos incomuns como negação de serviço distribuída (DDoS), certas formas de malwares e violações de políticas de segurança (SCARFONE; MELL, 2007).

2.2.2 Classificação pelo processamento das informações

Esse processo é formado da coleta dos dados, os quais serão analisados por um mecanismo para identificar atividades mal intencionas que podem ser realizados de várias

formas. A Figura 2.3 ilustra de forma hierárquica o processamento das informações. A classificação pode ser realizada por um método sendo divididos em três subclasses, a detecção por mau uso, a detecção por anomalia e protocolo *stateful*, que será detalhado a seguir ou pela estratégia, onde pode ser de forma centralizada ou de forma distribuída.

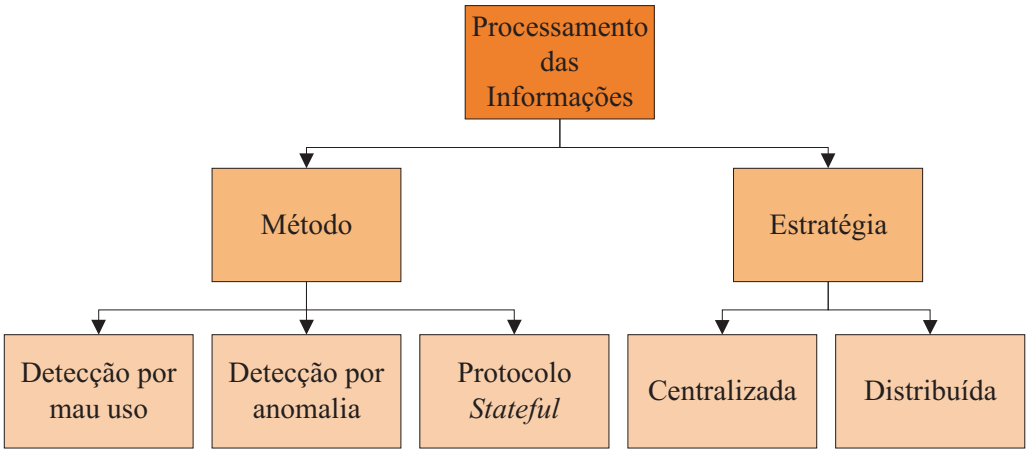

Figura 2.3: Classificação pelo processamento das informações. Adaptado de Scarfone and Mell (SCARFONE; MELL, 2007).

2.2.2.1 Classificação por método de detecção por mau uso

A detecção por mau uso é um método que utiliza a identificação do uso indevido através de um sistema especializado, podendo detectar atividades mal intencionadas, sendo definido por uma base de conhecimento pré-determinada (BRADEN, 1989). Dentro dessa classificação temos três subclasses conforme é ilustrado na Figura 2.4.

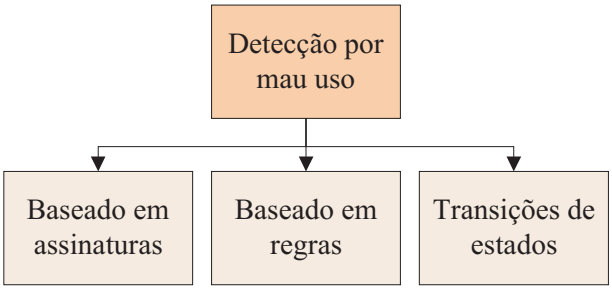

Figura 2.4: Subclassificação pela detecção por mau uso. Adaptado de Braden (BRADEN, 1989).

- **Baseada em assinaturas**: são informações disponíveis em um banco de dados coletados a partir de atividades com intenção de identificar intrusões (SABAHI; MOVAGHAR, 2008).

- **Baseado em regra**: são sistemas que usam um conjunto de estruturas condicionais (*IF/THEN*) na implicação para caracterizar ataques a computadores (LAZAREVIC; KUMAR; SRIVASTAVA, 2005).

- **Transições de estados**: é uma abordagem do IDS identificando a intrusão usando máquinas de estado finito (SABAHI; MOVAGHAR, 2008).

2.2.2.2 Classificação pelo método de detecção por anomalia

O método de detecção por anomalia é uma maneira de avaliar as informações da base de conhecimento como normais ou anormais. O algoritmo se baseia em controlar as diferenças das informações utilizadas da análise do comportamento de uma atividade normal. A Figura 2.5 ilustra todas as subclasses utilizadas por esse método, descritas a seguir (LAZAREVIC; KUMAR; SRIVASTAVA, 2005).

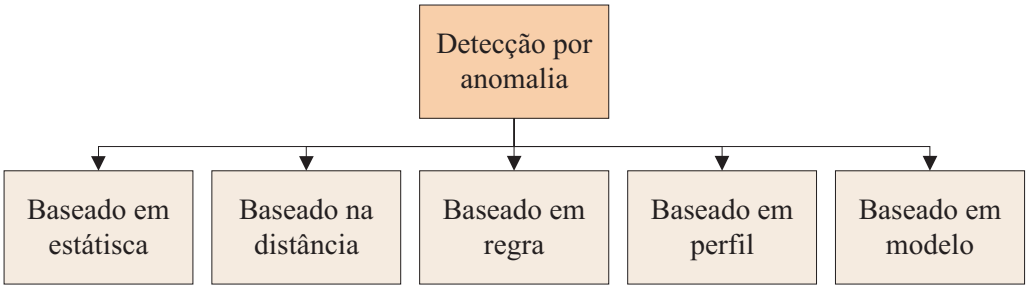

Figura 2.5: Subclassificação pela detecção por anomalia. Adaptado de Lazarevic et al. (LAZAREVIC; KUMAR; SRIVASTAVA, 2005).

- **Baseado em estatística**: são métodos que monitoram o comportamento do usuário ou da rede medindo as estatísticas ao longo do tempo (LAZAREVIC; KUMAR; SRIVASTAVA, 2005).

- **Baseado na distância**: são métodos que superam as limitações da abordagem da estatística na detecção de *outlier* quando os dados são difíceis de estimar em uma distribuição (SCARFONE; MELL, 2007).

- **Baseado em regras**: são métodos que define o conhecimento do comportamento normal do usuário ou da rede, os quais são comparados com o comportamento de uma intrusão (SABAHI; MOVAGHAR, 2008).

- **Baseado no perfil**: esse método é muito similar ao baseado em regra, mas o tratamento do comportamento é construído para diferentes tipos de tráfegos, os de

rede, os de usuários e todos os dispositivos. Esse método baseia-se no desvio do perfil, assim identificando uma intrusão (SABAHI; MOVAGHAR, 2008).

- **Baseado em modelo**: esse método é definido com outras abordagens no comportamento normal e anormal, podendo ser modelados para criar perfis de várias maneiras (SCARFONE; MELL, 2007).

2.2.2.3 Classificação por método de protocolo Stateful

Esse método é comparado com perfis pré-determinados que geralmente aceitam atividade inicial do protocolo. Cada estado do protocolo é comparado contra os eventos observados para identificar um desvio (SCARFONE; MELL, 2007).

2.2.2.4 Classificação pela estratégia

A classificação pela estratégia está diretamente relacionada ao método que será abordado, por exemplo, se escolher o método detecção por mau uso poderá usar a abordagem centralizada ou distribuída. Nas estratégias centralizadas as informações são tratadas em um ponto central, já nas estratégias distribuídas as informações são tratadas em vários nós, de uma forma distribuída.

2.2.3 Classificação pelo tempo de detecção

Os IDS podem ser classificados de duas formas, o tempo da detecção online ou off-line. Nos IDS online a detecção da intrusão é realizada tempo real, normalmente os NIDS tem essa abordagem. Nos IDS off-line a detecção de intrusão é realizada após a intrusão, pois os dados para análise só estarão disponível posteriormente, os HIDS normalmente são off-line (LAZAREVIC; KUMAR; SRIVASTAVA, 2005).

2.2.4 Classificação pelo meio ambiente

Essa classificação está relacionada à camada física do modelo TCP/IP, onde a condição do meio físico causa vulnerabilidade para rede. Nos últimos anos muitas redes sem fio foram implementadas, causando um tipo específico de vulnerabilidades dessas redes. Essa classificação pelo meio ambiente pode ser dividida em três subclasses conforme é ilustrado na Figura 2.6 e descritos abaixo: (SABAHI; MOVAGHAR, 2008).

- **Sem fio**: são as redes sem fio (*Bluetooth, WIFI* ou *WINMAX*) que nos últimos

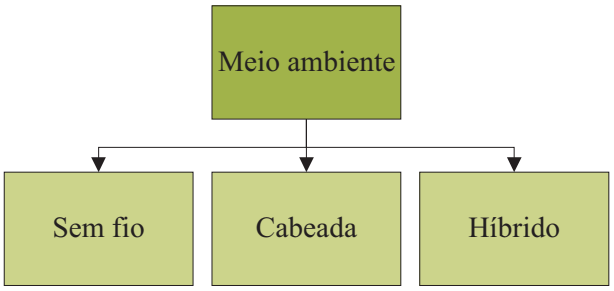

Figura 2.6: Classificação pelo meio ambiente. Adaptado de Sabahi and Movaghar (SABAHI; MOVAGHAR, 2008).

anos se tornou uma categoria especifica de IDS, chamada de WIDS (*Wireless IDS*. Os WIDS possuem mecanismos específicos para monitorar o tráfego das redes sem fio e assim podem analisar atividades suspeitas (SABAHI; MOVAGHAR, 2008).

- **Cabeada**: são as redes conectadas por cabos (par trançados, coaxial ou fibra ótica) e devido a sua condição física promove um baixo índice de vulnerabilidades comparadas pelas redes sem fio (SABAHI; MOVAGHAR, 2008).

- **Híbrido**: hoje devido a muitos dispositivos móveis uma solução hibrida é comum nas organizações. Essa abordagem implementa as duas soluções em conjunto.

2.2.5 Classificação por arquitetura

A maioria dos IDS são implementados em uma arquitetura centralizada visando à detecção das intrusões que ocorrem em um único ponto. Porém a arquitetura distribuída vem aparecendo na literatura nos últimos anos devido a sua eficiência na coleta dos dados e facilidade de detectar ataques distribuídos. Em uma arquitetura centralizada não é possível detectar os ataques distribuídos (SABAHI; MOVAGHAR, 2008). Nessa classificação por arquitetura foi dividido em três subclasses conforme é ilustrado na Figura 2.7 e descritos a seguir.

- **Centralizado**: são IDS que analisam os dados de forma centralizada em um lugar fixo (SABAHI; MOVAGHAR, 2008).

- **Distribuído**: são IDS que analisam os dados de forma distribuída e proporcionam uma maior disponibilidade do sistema.

- **Híbrida**: é uma solução que usa as duas abordagens para obter o melhor resultado no sistema.

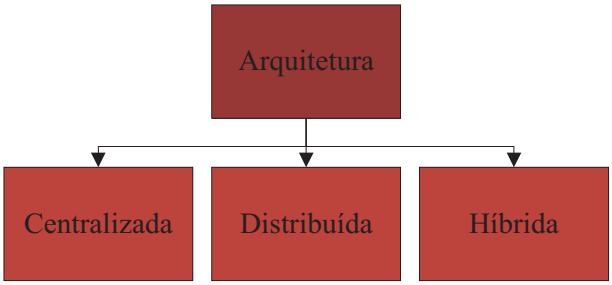

Figura 2.7: Classificação por arquitetura. Adaptado de Sabahi and Movaghar (SABAHI; MOVAGHAR, 2008).

2.3 Sistemas de Detecção de Intrusão Distribuídos

Os sistemas de detecção de intrusão distribuídos são conhecidos pela sigla DIDS que significa *Distributed* IDS. Na literatura um sistema distribuído é uma coleção de computadores independentes que fornece um sistema único na visão do usuário. Nessa abordagem dois aspectos deve-se levar em consideração, primeiro o hardware que ira suportar o sistema, e por segundo, o software do sistema que irá trabalhar em uma estrutura distribuída de nós, independendo se a estrutura é homogênea ou heterogênea. Existem vários tipos de sistemas distribuídos, mas um dos melhores exemplos é a própria Internet (TANENBAUM; STEEN, 2002). Na arquitetura de um sistema distribuído cada nó executa sua própria instância, permitindo de forma transparente ao usuário um sistema único de alto desempenho (DANTAS, 2005).

Atualmente o conceito da computação em nuvem, ou *Cloud Computer*, está em alta, vários produtos na Internet estão usando essa estrutura, como: Amazon Web Services, o Google AppEngine e Microsoft Azure. Quando fala-se em computação em nuvem entende-se sobre um sistema distribuído, que os serviços são fornecidos por demanda como: processamento, armazenamento e outras aplicações. Basicamente a computação em nuvem é o uso da Internet compartilhando serviços por demanda.

Segundo (MENASCÉ; NGO, 2009), a computação em nuvem tem muitos significados diferentes, no entanto, uma definição básica que engloba praticamente todas as definições é a seguinte, a computação em nuvem é uma modalidade de computação distribuída que caracteriza a disponibilidade de recurso por demanda de uma forma dinâmica e escalável. O termo recurso pode ser usado para representar infraestruturas, plataformas, software, serviços ou armazenamento. Um provedor de nuvem é responsável por disponibilizar os recursos necessários sob a demanda para os usuários, e por garantir os recursos de forma eficiente para as necessidades dos usuários. Por exemplo, uma nuvem de infraestrutura oferece serviços de infraestrutura computacional normalmente sob uma forma de máquinas

virtuais em servidores físicos e são cobrados pela quantidade de recursos consumidos.

Na arquitetura de um DIDS combina-se o monitoramento distribuído com a redução dos dados da análise. Basicamente essa arquitetura possue três componentes: o diretor IDS, o monitor do host e monitor da rede. A Figura 2.8 ilustra a arquitetura de um DIDS.

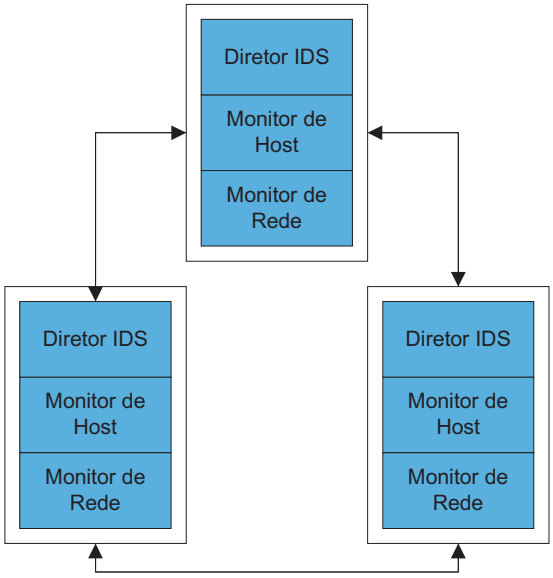

Figura 2.8: Arquitetura de um DIDS. Adaptado de Snapp et al. (SNAPP et al., 1991).

Nessa arquitetura os monitores de *hosts* ou monitores de redes possuem uma capacidade independente, não necessitando um dos outros desde que possa enviar seus relatórios para o diretor do IDS. Os monitores de *hosts* e de redes são os principais responsáveis para coletar evidências de atividades suspeitas, enquanto o diretor do IDS é responsável pela avaliação das atividades. O diretor do IDS envia relatórios das atividades para os monitores de hosts ou redes de forma independente, usando a infraestrutura de comunicação. A comunicação entre os nós são baseado no modelo da ISO/OSI, também prevê um comunicação bidirecional entre os diretores dos IDS´s. O diretor do IDS pode solicitar informações mais detalhadas sobre uma intrusão a outros nós, assim aumentando a capacidade de identificação de uma intrusão. Também prevê que os monitores de *hosts* ou de redes realizem filtros de nível baixo para minimizar o uso da largura da banda de comunicação entre passagem das informações para os diretores dos IDSs (SNAPP et al., 1991).

Recentemente novos métodos apareceram na classificação de IDS´s Distribuídos como os Grids, que são chamados de GIDS (Grid IDS) que usam recursos da computação em Grid, para detectar as intrusões (LEU et al., 2005) e os Colaborativos que são chamados de CIDS (*Collaborative* IDS), que trabalham em cooperação entre os nós garantido uma melhor eficiência na detecção da intrusão (ZAMAN; KARRAY, 2009), que serão apresentados

nas subseções a seguir.

2.3.1 IDS Distribuídos baseado em Grid

O artigo de Rana et al. (RANA; GUJRAL; SINGH, 2007) propõe o uso do IDS para segurança em Computação em Grid. Basicamente ele afirma que um ambiente em computação em Grid não tem como ser implementado sem considerar a questão de segurança. O gerenciador de segurança no GIDS são sistemas que exportam as informações sobre alertas para outros gerenciadores de segurança podem ser HIDS e NIDS dependendo de como foi implementado o ambiente em Grid. No entanto o sistema detecta uma atividade maliciosa baseado na suposição de uma atividade normal ou anormal.

Em Vieira et al. (VIEIRA et al., 2010), descreve-se uma proposta para o uso de GIDS para computação em nuvem e afirma que o uso dessa arquitetura promove um IDS que cobre ataques que não são possíveis de detectar em uma arquitetura de HIDS. Na sua proposta cada nó identifica eventos locais que podem representar violações da segurança e alerta os outros nós. Cada IDS individual cooperam no conjunto para detecção de uma intrusão. A Figura 2.9 ilustra o compartilhamento das informações entre os nós.

O nó contém os recursos que são acessados de forma homogênea através do middleware onde são definidas as políticas de controle de acesso e suporte ao ambiente, o serviço do IDS oferece a sua funcionalidade através do middleware que facilita a comunicação. Uma das partes mais importantes é o auditor de evento, é o responsável por captar os dados de várias fontes. O serviço do IDS analisa esses dados e aplica técnicas de detecção baseada no comportamento do usuário e no conhecimento de ataques anteriores, se detectar uma intrusão o middleware comunica os outros nós através de alertas e sincroniza os ataques em um banco de dados de comportamento, o serviço de armazenamento contém os dados para que o serviço do IDS possa analisar. É importante que todos os nós possuam acesso aos mesmos dados (VIEIRA et al., 2010).

2.3.2 IDS Distribuídos baseado em colaboração

Os estudos iniciados para os IDS´s baseado em colaboração partiu dos projetos CAIDS (HWANG; LIU; CHEN, 2004) e DOMINO (YEGNESWARAN; BARFORD; JHA, 2004). Atualmente conhecido como CIDS (*Collaborative* IDS), têm sido muito pesquisados pela comunidade acadêmica para detecção de ataques coordenados, pois as propostas atuais são deficientes. A proposta de um CIDS é abordada pela correlação entre as evidências suspeitas entre outros CIDS, melhorando assim a eficiência na detecção, pois possui um potencial superior para detectar intrusões que ocorrem na Internet por correlacionar com

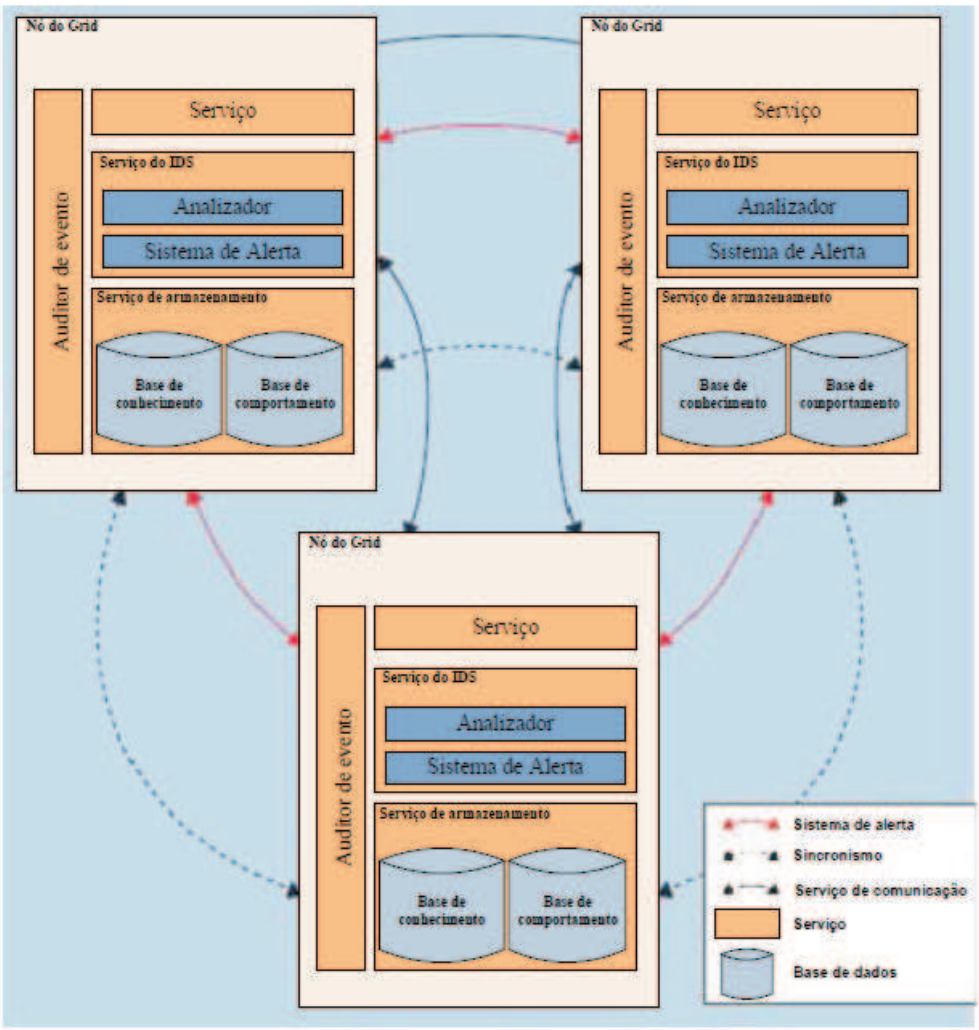

Figura 2.9: A arquitetura da rede e detecção de intrusão em computação em nuvem (VIEIRA et al., 2010).

uma base de assinaturas de ataques em diferentes sub-redes e também têm o potencial de reduzir os custos operacionais através do compartilhamento de recursos. O principal objetivo do CIDS é reduzir o número de falsos alarmes e alertas irrelevantes que são gerados por outras abordagens de IDS e assim produzindo uma alta abstração do nível de segurança nas redes (ZHOU; LECKIE; KARUNASEKERA, 2010).

Basicamente os CIDS contem duas unidades funcionais. A primeira é a unidade de detecção, que consistem de sensores de detecção onde cada sensor monitora a sua própria sub-rede ou *host* separadamente e em seguida geram alertas de baixo nível. E a segunda é a unidade de correlação que transforma os alertas de baixo nível em um relatório de alto nível confirmando os ataques.

Os CIDS pode ser classificados em três arquiteturas baseado na abordagem, conforme ilustrado na Figura 2.10 e descritas a seguir:

- **Centralizada**: todas as informações coletadas de cada IDS são relatadas para um único local para análise.
- **Hierarquias**: as informações locais são pré-processadas, e então as selecionadas são indicadas para a próxima camada da hierarquia para a partilha de análise mais aprofundada.
- **Distribuída**: onde as informações de cada IDS são compartilhadas e processadas de uma forma completamente distribuídas sem um coordenador centralizado.

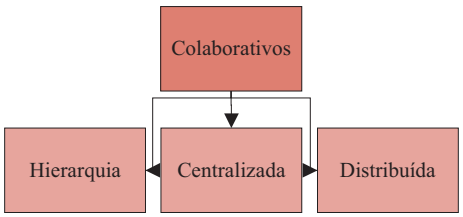

Figura 2.10: Classificação para os CIDS (ZHOU; LECKIE; KARUNASEKERA, 2010).

Nas subseções a seguir serão explicadas as três arquiteturas: centralizada, hierarquia e distribuída para a abordagem de um CIDS.

2.3.2.1 CIDS com arquitetura centralizada

A Figura 2.11 ilustra um CIDS com arquitetura centralizada. Nessa abordagem cada IDS desempenha um papel como uma unidade de detecção do CIDS, onde produzem alertas localmente e em seguida são enviados para um servidor central que funciona como uma unidade de correlação. Geralmente esse tipo de abordagem é mais adequado para estruturas em pequena escala e não para IDSs independente dentro da estrutura da Internet. Existem duas falhas nessa abordagem, a primeira falha está relacionada à unidade central, pois ela tornar-se um ponto único de falha, se a comunicação com o centralizador for interrompida ira acontecer um colapso no sistema causando sua paralisação já a segunda falha acontece quando há uma sobrecarga no sistema central, isso acontecerá quando todas as unidades de detecção simultaneamente enviar alertas para a unidade de correlação (ZHOU; LECKIE; KARUNASEKERA, 2010).

2.3.2.2 CIDS com arquitetura hierárquica

Para solucionar o problema nos CIDS com arquitetura centralizadas foi abordada uma arquitetura hierárquica que soluciona o problema de escalabilidade dessa arquitetura.

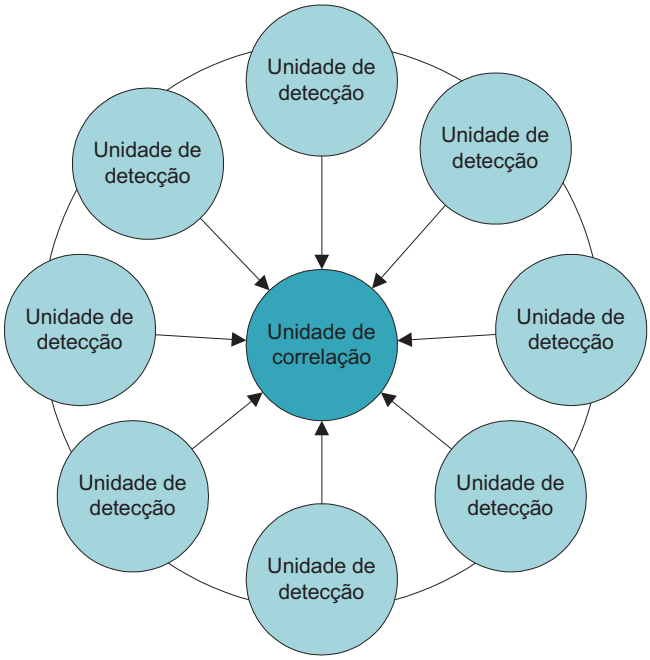

Figura 2.11: CIDS com arquitetura centralizada (ZHOU; LECKIE; KARUNASEKERA, 2010).

Nessa abordagem é dividida em vários pequenos grupos de comunicação, baseado nas seguintes características geográficas: o controle administrativo, coleta de plataformas de software similar e tipos de intrusões. Cada grupo de comunicação é um subconjunto da hierarquia. Em cada grupo existe um nó de análise que é responsável para correlacionar todos os dados coletados neste grupo. O nó de análise é o nó pai do grupo e seus dados processados serão enviados para cima em um nó de nível superior da hierarquia para análise posterior (ZHOU; LECKIE; KARUNASEKERA, 2010).

A Figura 2.12 ilustra um CIDS com arquitetura hierárquica sendo dividido em três grupos de comunicação: o nível mais baixo são as unidades de detecção que seus alertas são passados para um nível acima, as unidades de correlação estão equipadas com uma unidade de detecção e unidade de correlação, neste nível existe a possibilidade de se correlacionar com os próximos níveis ou os níveis inferiores (ZHOU; LECKIE; KARUNASEKERA, 2010).

Essa arquitetura é melhor do que a abordagem centralizada, no entanto os nós dos níveis mais altos possuem limitação referente à escalabilidade e também pode haver o inter-rompimento da função detecção devido a uma falha do centralizador do grupo. Além desse problema os nós mais elevados na hierarquia tem limitação na detecção devida o alto nível de abstração dos dados de entrada (ZHOU; LECKIE; KARUNASEKERA, 2010).

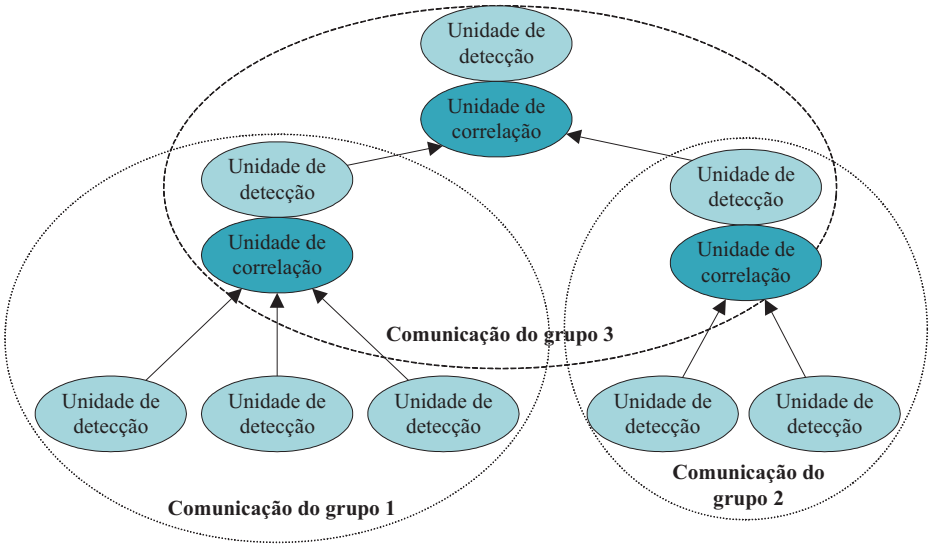

Figura 2.12: CIDS com arquitetura hierarquia (ZHOU; LECKIE; KARUNASEKERA, 2010).

2.3.2.3 CIDS com arquitetura distribuída

Outro tipo de abordagem seria os CIDS com arquitetura distribuída assim resolveria os problemas da abordagem hierárquica. A Figura 2.13 ilustra uma visão geral dessa arquitetura. Em um CIDS distribuído cada participante IDS tem duas funções, uma unidade de detecção que é responsável pela coleta de dados localmente e outra uma unidade de correlação que é uma parte do plano da correlação distribuída. O participante se comunica com os outros IDS´s usando um protocolo de distribuição de dados, como *peer-to-peer* (P2P), *multicast* e outros (ZHOU; LECKIE; KARUNASEKERA, 2010).

2.4 Revisão da Literatura com CIDS

O objetivo dessa seção é apresentar uma revisão sistemática de projetos que utilizam CIDS. De acordo com os estudos realizados para o desenvolvimento pode-se afirmar que as abordagens colaborativas proporcionam uma melhor precisão na detecção em relação às abordagens individuais com isto foram revisados alguns artigos com esta abordagem.

O artigo (BYE; CAMTEPE; ALBAYRAK, 2010) afirma que os sistema de detecção de intrusão colaborativos (CIDS) fornecem uma solução promissora onde esse utiliza várias fontes de informações para obter uma melhor compreensão dos ataques mais complexos realizados na Internet, mas tem que ser levado em conta os riscos dessa solução. Ele apresenta duas contribuições para os estudos sobre CIDS, a primeira abordagem faz uma

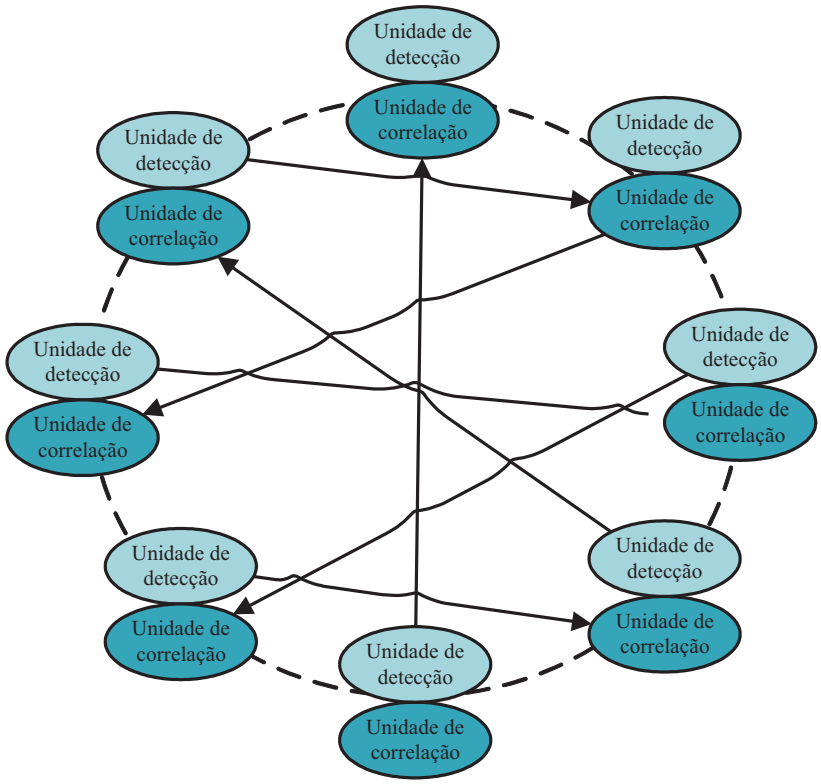

Figura 2.13: CIDS com arquitetura distribuída (ZHOU; LECKIE; KARUNASEKERA, 2010).

pesquisa para compreender as vulnerabilidades para construção de um framework, onde foram identificados cinco blocos de construção que são relevantes para CIDS os quais são:

- Esquema da Comunicação;
- Estrutura da Organização;
- Formação do Grupo;
- Compartilhamento das informações e Interoperabilidade; e
- Sistema de Segurança.

E sua segunda contribuição é o problema da troca de mensagem em uma conexão *peer-to-peer* dentro de uma estrutura descentralizada onde deve garantir o anonimato acima de qualquer suspeita, isso implica que o adversário não pode supor que o IDS de origem é a fonte da mensagem envida (BYE; CAMTEPE; ALBAYRAK, 2010). Na proposta do SIDIAC usa-se o recurso de tabela hash para garantir a deficiência mencionada pelo trabalho, assim garantindo que a origem das mensagens fique no anonimato.

Em (FARROUKH et al., 2008) propõem em seu artigo um sistema detecção de intrusão distribuído e colaborativo chamado DaCID que se baseia na teoria de Dempster

Shafer, onde as evidências para os incidentes dos diferentes nós fazem uma junção melhorada e precisa na detecção da intrusão, onde não há a existência do conhecimento prévio da rede e nem de medidas probabilística quantitativas para os diferentes estados do sistema, incluindo probabilidade de falso alarmes e incerteza da informação enviados pelos outros nós. Esse sistema permite que um nó da rede troque informação mínima com um pequeno subconjunto de outros nós a fim de melhorar o desempenho da detecção, sendo uma arquitetura descentralizada e não sobre um único ponto de falha independente do número de ataques. Os resultados das simulações mostraram que foi comparável a um método centralizado sob ataques simples ou múltiplos e demonstrando que DaCID é mais robusto do que outros sistemas e eficaz em sua abordagem tanto em grandes como em pequenas redes. Baseado neste projeto foi definido o modelo matemático a ser usado na proposta do SIDIAC, onde difere na empregabilidade da aplicação do algoritmo que é usado o algoritmo proposto por (FUNG; ZHANG; BOUTABA, 2010).

Já (FUNG et al., 2009) apresentam em seu artigo um quadro de simulação que incorpora diferente componentes como: modelo de perícia, modelo de engano, modelo de ataque e métricas de avaliações para oferecer flexibilidade para o usuário ajustar os parâmetros de simulação de acordo com suas necessidades. No quadro de simulação abstraímos as propriedades de cenários do mundo real na concepção de diferentes componentes. O resultado nesse ambiente de pesquisa tornou-se flexível para que o usuário ajusta-se os parâmetros para as avaliações de seus próprios modelos de confiança e comparar com outros modelos existentes utilizando métricas de avaliação unificada. Também foi demonstrado que o uso dessa estrutura é eficaz comparado com três modelos de confiança existentes, que são:

- Eficiência do modelo de confiança;
- Robustez do modelo de confiança; e
- Escalabilidade do modelo de confiança.

A avaliação da confiança é projetada para permitir que os pares de IDS possam confiar em outros com base em suas interações diretas com eles no histórico.

No artigo de (FUNG; ZHANG; BOUTABA, 2010) apresenta-se uma proposta do uso de um sistema de detecção de intrusão colaborativo (CIDS) baseado em host (HIDS) onde os colaboradores mantem informações sobre os invasores que pode ser cooperado com seus vizinhos melhorando a precisão na detecção e diminuindo a taxa de falsos positivos (FP) e a taxa de falsos negativos (FN). Para fazer a troca de opiniões entre os vizinhos propõem-se o uso de aprendizagem *Bayesiana* para agregação das opiniões sobre os intrusos, onde a técnica de aprendizagem ajuda identificar os nós desonestos e remover de sua lista de

colaboradores, o modelo de decisão *Bayesiana* agrega aos seus colaboradores um custo minimizado de falsas decisões se no sistema for adicionado um nó desonesto. Em termos de seleção de colaboradores um nó pode adicionar outro quando quiser em sua lista de colaboradores uma maior precisão de detecção maximizada no entanto incluir uma grande lista de colaboradores pode resultar em um custo alto de manutenção. (FUNG; ZHANG; BOUTABA, 2010) afirma que o algoritmo alcança um desempenho semelhante mas sua abordagem é gulosa que pode requerer muito tempo de computação.

(FUNG; ZHANG; BOUTABA, 2010) afirma que um componente crítico para colaboração é o mecanismo de agregação de feedback baseado nessa afirmação propõem um quadro de colaboração para redes de detecção de intrusão (CIDN) usando uma abordagem *Bayesiana* para agregação de feedback e assim minimizando os custos nos alarmes falso da detecção. A abordagem *bayesiana* concebe um mecanismo de agregação de *feedback* descentralizado onde cada nó do CIDN pode contribuir com a detecção que foi usado para modelar as taxas de falsos positivos (FP) e taxas de verdadeiros positivos (TP) para cada nó. Neste projeto estimado que o custo de todas as decisões possíveis da agregação dos *feedbacks* é escolhido pelo menor custo. Foram avaliados os modelos de agregação com simulações para comparar com outras abordagens existentes, onde a simulação é representada por dois parâmetros de nível de especialização, cada nó recebe uma lista de familiaridade inicial contendo todos os seus nós vizinhos, onde o processo de detecção de intrusão colaborativa envia as informações para um nó conhecido para solicitar uma análise da intrusão. Os *feedbacks* coletados dos outros nós são usado para tomar a decisão final e disparar um alarme se houver a intrusão. Os resultados experimentais indicam que a abordagem *Bayesiana* reduz o custo de riscos de falsas decisões em relação aos modelos de agregação média e média ponderada simples.

Nesse artigo (FUNG et al., 2011b) apresentam uma taxonomia para classificar redes de detecção de intrusão colaborativas (CIDN) com base no critério de topologia, escopo, especialização, privacidade de dados e vulnerabilidade a ataques internos. Afirmam em seu artigo que a cooperação entre sistema de detecção de intrusão (IDS) permite ao sistema usar informações coletivas que fornece uma detecção de intrusão mais precisa, tanto localmente quando em todo o CIDN. A rede do CIDN pode ser comprometida por alguns nós e afetar a colaboração do sistema, nós maliciosos podem fazer uso de alguns tipos de ataque comuns, como:

- Sybil é um ataque que um nó malicioso cria uma grande quantidade de identidades falsa para comprometer a colaboração do sistema;
- Newcomer é um tipo de ataque que um nó se registra na rede como um novo usuário

e depois passa a ter um mau comportamento na rede e assim prejudicado a colaboração do sistema;

- Betrayal é um ataque que um nó que já havia adquirido confiança na rede se transforma em um nó malicioso e assim envia informações falsas para outros nós;
- Collusion é um ataque distribuído quando um grupo de nós da rede cooperar para fim de comprometer a rede do CIDN.

Portando para que um projeto de CIDN seja robusto tem que haver mecanismos para se defender contra ataques internos. No seu artigo oferece uma revisão de literatura para os modelos de CIDN existentes como: Indra, DOMINO, DShield, NetShield, Worminator, CRIM, ALPACAS, HBCIDS e ABDIAS analisando suas propriedades onde será útil para construção de novos CIDN (FUNG et al., 2011b).

No artigo de (FUNG et al., 2011) apresentam uma proposta de uma rede de detecção de intrusão (IDN) baseado em host onde usa um modelo de Dirichlet para medir o nível de confiabilidade dos nós com sua experiência mútua. O modelo Dirichlet é baseado em crenças iniciais sobre um evento desconhecido representado por uma distribuição prévia de informações, onde as crenças iniciais combinadas com os dados recolhidos de uma amostra podem ser representadas numa distribuição posterior que se adapta ao modelo de confiança e assim atualizando a base de histórico, mostrando o comportamento futuro para um nó do IDN com base em sua história passada. Foi avaliado o sistema baseado em uma rede colaborativa de detecção de intrusão (CIDN) simulada, onde os nós são distribuídos e tem níveis diferentes de pericia na detecção de intrusões. E os resultados dos experimentos demostraram que o sistema produz uma melhoria significativa na detecção de intrusões sendo robusto contra vários ataques como: Sybian, Newcomer, Betrayal, Collusion e Incossitency em comparação com outros sistemas colaborativos existentes.

(FUNG et al., 2011a) propõem em seu artigo um quadro baseado na confiança para a colaboração segura e eficaz dentro de uma rede de detecção de intrusão (IDN). O modelo de confiança permite que cada nó do IDN possa avaliar a confiabilidade entre outros nós baseado na experiência adquirida. Assim desenvolveram um modelo de gestão de confiança robusto e adequado para a colaboração distribuída, que permite que cada nó possa avaliar a confiabilidade de outros com base em sua própria experiência e também colabora de forma eficiente com a rede *peer-to-peer* e o algoritmo proposto controla a admissão dos novos nós para selecionar e administrar seus colaboradores. Contudo avaliaram o sistema baseado em uma rede simulada onde os nós podem ter diferentes níveis de perícia na detecção de intrusões e também tornar-se mal-intencionado no caso de ter sido comprometido por uma ameaça potencial. Nos resultados dos experimentos afirmam que

o sistema proporciona uma melhoria significativa na detecção de intrusões e é robusto a vários ataques em comparação com os outros trabalhos.

O artigo (FUNG, 2011) afirma que em uma rede de detecção de intrusão colaborativa (CIDN) existem trocas de dados de intrusões que preocupa os usuários com a privacidade dessas informações. Uma proposta de desenvolvimento de um algoritmo foi criado para troca de regas em um CIDN chamado SMURFEN, onde o conhecimento da detecção de intrusão é compartilhado entre os nós baseado em uma conexão *peer-to-peer* que mantém uma lista de colaboradores e envia seus feedbacks através desse sistema. Smurfen é uma plataforma para que os nós compartilhem suas regras de detecção com os outros de forma eficaz. Sendo assim evitar o ataque *man-in-the-middle* (homem do meio) a comunicação entre todos os nós utiliza um algoritmo de chave assimétrica. Foi concluído que o sistema é eficaz e melhora a precisão de detecção de intrusão em todo o CIDN na simulação.

Neste artigo (FUNG; ZHANG; BOUTABA, 2012) propõem um algoritmo para gerenciamento de conhecimento dinâmico para os nós de uma estrutura de rede de detecção de intrusão colaborativa (CIDN), sendo avaliados os resultados dos experimentos simulado em uma algoritmo usando o Java referente a estabilidade e robustez do sistema. Os resultados obtidos revelaram que o modelo de decisão *Bayesiano* proposto no artigo supera em termos de custo de falsa decisão e também que o algoritmo de gerenciamento de conhecimento dinâmico supera as abordagens estáticas que defini um comprimento conhecido fixo ou limite de precisão. As principais contribuições do seu trabalho são: modelo de decisão *Bayesiana* para a agregação de *feedback* em sistemas de detecção de intrusão de colaboração para atingir o mínimo custo decisão falso e o algoritmo de seleção de conhecimento é concebido para selecionar colaboradores de forma otimizada o que leva ao custo total mínimo, incluindo o custo decisão falsa e custo de manutenção; e o algoritmo de gestão de conhecimento dinâmico para integrar o conceito de período de estágio para a negociação sistema.

Fung (FUNG, 2013) em seu artigo informa que foi projetada uma rede de detecção de intrusão colaborativa (CIDN) que foi focado em um quadro para investigação dos seguintes problemas: gerenciamento de confiança, colaboração na decisão de intrusão, gestão de recursos e seleção de colaboradores. Na literatura sobre rede de detecção de intrusão (IDN) pode ser dividido em dois tipos de abordagem: a primeira é baseada na informação onde os nós compartilham suas observações e conhecimento de detecção com os outros nós da rede; e a segunda baseada em consulta quando um nó detecta atividades suspeitas e não tem confiança suficiente para tomar uma decisão sozinha e envia pedidos para outros nós e assim avalia a intrusão ou não. O projeto concentra-se no foco de um

IDN baseado em consulta onde os diferentes nós ligado em uma rede *peer-to-peer* mantém uma lista de colaboradores conhecidos para realizar uma consulta seletiva e assim melhorar a detecção. O resultado do seu projeto contempla várias propriedades desejadas por uma solução CIDS onde garante eficiência, robustez, escalabilidade e compatibilidade.

Nos trabalhos citados acima define uma arquitetura de um IDS Colaborativo chamado HBCIDS que é robusto e eficaz em seu algoritmo para fazer a detecção de intrusão usa o modelo matemático *Bayesiano*. O projeto proposto difere no modelo matemático que é usado *Dempster-Shafer* para fazer esta atividade.

(LIN et al., 2008) propôs em um sistema de detecção de intrusão (IDS) distribuído e colaborativa para NIDS (*Network* IDS) que pode ser implementado nos roteadores dentro dos backbone em um ISP (*Internet Service Provider*) ou mesmo em um AS (*Autonomous System*), o projeto usa base de assinatura para poder compartilhar entre outros nós de IDS. Assim usam uma abordagem que o pacote transmitido dentro da rede só é verificado uma vez, para isso usam três técnicas: a marcação de pacotes, o anel lógico (ILR) e o cache do LRU (*Least Recently Used*) em cada roteador, com isto melhora-se o rendimento geral da rede. Além disso, é usado um esquema de *caching* para manter a chegada da sequência ao destino para os pacotes pertencentes ao mesmo fluxo. Afirmar que os resultados da simulação quando a relação de implementação do método colaborativo é de 1% e não é tão eficiente com uma implementação com 50% dos IDS tradicionais e IDS distribuído e colaborativo são robusto com uma resposta rápida a um ataque aumento significativo na taxa de detecção. A proposta difere no modelo da arquitetura empregando em uma arquitetura de HIDS ao invés de NIDS.

(RAN, 2012) propõe em seu artigo um modelo de detecção de intrusão baseado em múltiplos agentes onde a define uma arquitetura hierárquica que é dividida em quatro tipos de agentes que são: Agentes de Detecção Básica (BA): estão localizados na parte mais inferior da estrutura hierárquica, são independentes e autônomos, capazes de trabalhar simultaneamente e podem detectar ataques simples; Agente Locais de Coordenação (LCA): estão localizados no meio da estrutura hierárquica, têm um conhecimento mais local para poder cooperar com os agentes de nível mais baixo e pode detectar ataques mais complicados; Agentes de Coordenação Global (GCA): estão localizados no nível mais alto da estrutura hierárquica e são capaz de cooperar com os agentes locais para detectar os ataques mais complexos com conhecimento global; Agente de Interface (IA): são as consoles que irão interagir com o usuário de acordo com sua exigência. O artigo estabelece uma base teórica para construção de um sistema de detecção de instrução usando um modelo colaborativo com múltiplos agentes. Na proposta definida neste trabalho usa uma arquitetura distribuída que cada agente consulta seus colaboradores atráves de um

gerenciador de confiança.

Em seu artigo (SHEN; XUE, 2010) propõem que à análise colaborativa deve ser incorporada em sistemas de detecção de intrusão distribuídos, pois as informações dos vários componentes melhoram a questão da segurança melhorando as taxas de detecções do sistema e diminuído as taxas de falsos alarmes que são produzidos pelo IDS. Em seu projeto nomeado DCIDS (*Distributed Collaborative Intrusion Detection System*) apresentam sua arquitetura hierarquia composta por quatro camadas, quais são:

- Componente de Detecção que é responsável por coletar os dados de auditoria;
- Colaboração da Análise de Detecção que é o núcleo dos IDS internos e realiza detecção colaborativa;
- Gerente de Colaboração é uma componente chave para fornecer os pontos de detecção com a informação de todo o sistema e fazer o DCIDS ser escalável;
- E Gerente de Detecção de intrusão que toma a decisão dos componentes de resposta do DCIDS.

No final da simulação do DCIDS foi demonstrado que há uma melhoria evidente nas taxas de detecção do sistema e assim diminuindo as taxas de falsos alarmes. Eles afirmam que a análise colaborativa pode melhorar a detecção para novos ataques. Na proposta difere na questão do repasse de mensagem pois cada nó define se é invasor ou não baseado nas análises dos outros nós colaboradores.

(SIRIVIANOS; KIM; YANG, 2011) apresentam em seu artigo um modelo de detecção colaborativo para spam em uma arquitetura centralizado que nomeia o projeto em *SocialFilter* baseado na utilização de uma rede social para avaliar a confiança na precisão da detecção. O projeto proposto permite que os nós com nenhuma funcionalidade de classificação de e-mail possam consultar a base de *spammer* na rede para validar se a origem (host) é *spam*. *SocialFilter* emprega *Sybil-Resilient* para avaliar a confiança entre os nós colaboradores na detecção de *spam* para submeter ao sistema. Os autores afirmam que o *SocialFilter* é o primeiro sistema de colaboração que avalia a confiabilidade dos nós repórteres de *spam* e aproveita a rede social para gerenciar os administradores. Foi avaliado o projeto usando uma amostra de 50k nós da rede social Facebook onde foi possível verificar que é possível suprir o trafego de *spam* de uma forma confiável. Também foram comparados os resultados com o projeto Ostra (MISLOVE et al., 2008) que mostrou que abordagem escolhida é menos eficaz na supressão de *spam* quando a rede está sobrecarregada, no entanto o Ostra pode resultar uma porcentagem expressiva de e-mail legitimo sendo bloqueado (falsos positivos) que é altamente indesejável para um sistema de controle

de *spam*, já o projeto *SocialFilter* não produz falsos positivos que sugere que o sistema é uma melhor alternativa. Na proposta do SIDIAC usa uma arquitetura distribuída onde difere do projeto pois usa uma arquitetura centralizada.

No artigo (SOUSA et al., 2010) propõem uma abordagem colaborativa centralizada para compartilhar e combinar filtro de *spam* (e-mail mau intencionado) de uma forma flexível e aumentando o nível de precisão em técnicas anti-*spam*, no qual os usuários com seus cliente de e-mail executam está atividade. Neste artigo afirmam que hoje para tratamento de *spam* existe duas grandes abordagens: a de filtragem por colaboração (CF) que se baseia na partilha de informações sobre mensagens de *spam*; e filtragem baseado em conteúdo (CBF) que usa conceitos de *Data Minig* (DM) que o classificador aprende a discriminar quais são as mensagens de *spam*. No modelo proposto pelos autores de tratamento de *spam* usa uma perspectiva colaborativa que se baseia na partilha de modelos de filtragens dos usuários onde as informações sobre algumas mensagens de *spam* são compartilhadas com outros colaboradores e assim melhorando a filtragem a nível pessoal dos colaboradores. Para avaliar a proposta colaborativa foi implementado com cinco usuários no compartilhamento das assinaturas de *spam* em que afirma que superou as abordagens locais de filtragem e melhorando a robustez do sistema de detecção de *spam*. No trabalho de (SOUSA et al., 2010) usam uma arquitetura centralizada para fazer a colaboração já no SIDIAC usa arquitetura distribuída.

No artigo (WU et al., 2003) iniciam a investigação sobre as arquitetura de IDS colaborativos, assim propõem em seu artigo uma abordagem de uma implementação de um CIDS centralizado para tratamento de sistemas web em um ambiente de *e-commerce*. Apesar da tecnologia cgi para um *e-commerce* ser ultrapassada hoje em dia a abordagem é uma boa solução para iniciar estudos sobre a tecnologias colaboração de IDS. Na implementação do CIDS é aplicado em três camadas distintas: rede, sistema operacional e aplicação. No qual um gerente agrega os alarmes para os diferentes detectores de intrusão e combina um algoritmo de rede *Bayesiana*. Para validar o projeto usa esses softwares: Snort, Libsafe e kernel Sysmon, onde é testado em três tipos de ataque: *buffer overflow, flooding* e ataques baseado em *scripts*. E assim consegue avaliar que os CIDS reduzem a incidência de alarmes falsa devido à colaboração do algoritmo. A proposta difere na questão da arquitetura pois o SIDIAC usa uma arquitetura distribuída para colaboração em quanto a proposta de (WU et al., 2003) usa uma arquitetura centralizada.

O projeto TRINETR (YU et al., 2005) é um IDS colaborativo centralizado sendo formado de uma arquitetura de três camadas que são: colaboração da agregação de alertas, base de dados dos eventuais alertas e a correlação entre os alertas, onde é destinada a reduzir a sobrecarga dos alertas correlacionando ao resultados de vários sensores do IDS e

assim reduzindo os falsos positivos nas avaliações. No artigo é realizado experimento com dois IDS, o Snort e o Prelude para avaliar os falsos positivos, em sua análise com uma base de 54 ataques. O Snort gerou 467 aletas e o Prelude gerou 744 alertas, onde dos 54 ataques 46 o Snort detectou e o 39 o Prelude. O algoritmo de agregação gerou 68 junções validando 40 falso positivos para o Snort e 8 falsos positivos para Prelude. Assim eles afirmam que os resultados dos experimentos com o TRINETR é muito satisfatório provando que a solução colaborativa é uma combinação vantajosa para produtos heterogênicos de IDS. O SIDIAC difere na questão da arquitetura distribuída, pois o TRINETR usa uma arquitetura centralizada.

(ZAMAN; KARRAY, 2009) afirmam que os sistemas de detecção de intrusões distribuídos (DIDS) sofre muitas limitações como a falta de um analisador central e uma carga pesada na rede, com isto propuseram um C-IDS usando uma arquitetura colaborativa para superar essas limitações. C-IDS proposto é organizado em um processo de cooperação entre os diferentes nós que estão distribuídos em diferentes pontos das redes com níveis hierárquicos, cada nó precisa receber um bit de informação para o módulo de IDS anterior para poder realizar sua decisão na detecção, se o bit for 0 indica que o trafego é normal, se for 1 indica que o trafego da rede tem um ataque e se for 2 indica que o trafego é indefinido, então os tráfegos normais e indefinidos são autorizados a passar para o próximo módulo IDS e os tráfegos de ataque são bloqueados imediatamente. Assim afirmam que os resultados da arquitetura proposta reduz a carga de trafego de rede, melhorando o desempenho geral do sistema e além disso não há nenhuma administração central nos processamentos dos dados de modo que não há chance para um único ponto de falha. Na proposta do SIDIAC difere na forma de detecção de uma intrusão que usa uma forma de consulta aos seu nós colaboradores para detecção a intrusão, enquanto o processo de (ZAMAN; KARRAY, 2009) usa uma forma hierarquia para esta detecção.

No artigo (ZARGAR; TAKABI; JOSHI, 2011) apresentam uma proposta de um sistema de detecção de intrusão colaborativo (CIDS) centralizado que é nomeado DCDIDP (*Distributed, Collaborative and Data-driven Intrusion Detection and Prevention System*) que tem por objetivo fornecer um CIDS para os provedores de serviços em nuvem onde é composto de três camadas lógicas: rede, host e global. No artigo é apresentado um quadro para integrar as três camadas: IaaS (camada de infraestrutura), PaaS (camada de plataforma) e SaaS (camada de software) em um sistema de detecção de intrusão (IDS) melhorando a precisão e a eficiência do sistema para cada camada. É proposto pelos autores que todos os provedores de serviços em nuvem usem uma infraestrutura colaborativa (DCDIDP) para colabora de forma distribuída em diferentes níveis de operações para responder aos ataques e proporcionar uma melhor segurança para todos os envolvidos.

Sua contribuição está no quadro que foi descrito sobre IaaS, PaaS e SaaS, pois ainda não foi implementado um protótipo para essa solução. A proposta difere na questão da arquitetura de análise onde na proposta do SIDIAC uma análise por host em quanto o projeto de (ZARGAR; TAKABI; JOSHI, 2011) faz por network.

Zhong et al. (ZHONG; RAMASWAMY; LI, 2008) apresenta um artigo onde usam uma abordagem colaborativa implementada no mundo real para um problema de *spam*, eles nomeiam o projeto como ALPACAS (*A Large-scale Privacy-Aware Collaborative Anti-spam System*). O Projeto APLCAS tem duas contribuições: a primeira e uma técnica de geração de impressão digital que efetivamente captura as informações semelhantes dos e-mails em suas respectivas codificações de modo que é possível realizar comparações de similaridades com outros nós da rede de colaboração de detecção; e a segunda aplica proteção na privacidade usando um protocolo de preservação de privacidade que eles criaram para controlar a quantidade de informações a serem compartilhada entre os outros nós colaboradores. Também fizeram uma comparação com duas abordagens populares de *spam*, a filtragem por o método *bayesiano* e a filtragem colaborativa baseado em *hash* simples onde mostraram que o projeto tem uma melhor eficiência na filtragem de *spam*, tem melhor resistência para ataques e fornece uma forte proteção da privacidade para as entidades participante. No projeto do SIDIAC difere no processo de análise em que usa o modelo matemático *Dempster-Shafer*, já na proposta usa o modelo matemático *bayesiano*.

Zhou et al. (ZHOU; KARUNASEKERA; LECKIE, 2005) afirmam que as soluções colaborativas têm demonstrado uma maneira eficaz para detecção de intrusões comparada com uma solução centralizada e propõem um algoritmo de sistema de detecção de intrusão colaborativa (CIDS) para comunicações *peer-to-peer* evitando um ponto único de falha, possibilitando a escalabilidade da solução e garantido que os dados estejam seguros no compartilhamento entre os participantes em diferentes organizações usando uma tabela *hash* distribuída (DHT). Afirmam que o Chord com o mecanismo DHT tem sido proposto para muitas aplicações distribuídas em larga escala, pois dos resultados de seus experimentos revelou que possuem um desempenho superior em comparações aos demais. A arquitetura da DHT é uma solução do CIDS para superar os desafios da colaboração como: o roteamento de dados, balanceamento de carga, escalabilidade e pontos centrais de falhas. Fica evidente que a latência da detecção no sistema proposto a uma diferença entre o sistema centralizado com o sistema descentralizado, onde a latência da detecção faz prejudicar o resultado do sistema centralizado. Em seus resultados comprovam que a arquitetura distribuída é mais eficaz do que uma abordagem centralizada.

Zhou et al. (ZHOU; KARUNASEKERA; LECKIE, 2007) em seu artigo propõem um grande teste para redes reais chamado de LarSID (*Large Scale Intrusion Detection*) com

o propósito de otimizar o *trade-off* entre a precisão da detecção e o tempo que o sistema não demostra reação. LarSID visa proporcionar um serviço de detecção de intrusão em grande escala na Internet. No seu desenvolvimento foi dividido em cinco parte: a primeira define o escopo dos problema para detecção de intrusão a qual ele foi projetado; segunda descreve os serviços de detecção de intrusão fornecido por eles; terceira descreve a construção e o mecanismo de detecção; quarta caracteriza os principais atributos que afetam a qualidade de serviço; e quinta detecta as principais funções do projeto. LarSID fornece um serviço para a defesa contra ataques através da arquitetura da tabela *hash* distribuída (DHT) e trabalha em uma arquitetura distribuída. Onde apresentou um resultado significativamente mais eficiente do que uma abordagem totalmente centralizada, o LarSID foi implementado em 128 nós da PlanetLab para testar a intrusão em grande escala.

Zhou et al. (ZHOU; LECKIE; KARUNASEKERA, 2009) criaram um proposta para uma algoritmo de correlação de alerta descentralizado e multidimensional, pois os algoritmos atuais de sistema de detecção de intrusão colaborativo (CIDS) são simples de mais para capturar as características importantes de ataques ou muito custosos computacionalmente para detectar ataques em tempo hábil. Afirmar que o algoritmo de correlação de alerta é eficiente e que tem uma melhor precisão na detecção para os CIDS no qual a descentralização do algoritmo multidimensional é essencial para haver uma escalabilidade do sistema. Foi introduzida no algoritmo uma abordagem probabilística para estimar a correlação e melhorar a precisão na detecção em comparação com um sistema de seleção simples. Em suas simulações o algoritmo centralizado foi avaliado pela abordagem descentralizada que reduziu significamente as mensagem de alertas e não degradando a precisão na detecção dos cenários proposto. Para avaliar o experimento em grande escala usaram 100 nós do PlanetLab que confirmou que a arquitetura descentralizada e mais escalável do que a abordagem centralizada.

Zhou et al. (ZHOU; LECKIE; KARUNASEKERA, 2010) propõem um desenvolvimento de um modelo de incentivo com base na gestão de confiança usando a teoria dos jogos para os colegas a colaborar com sinceridade em um ambiente de uma rede de detecção de intrusão (IDN). Em que um regime de incentivos faz alocação de recursos para rede colaborativa de IDS baseado nas confianças a quantidade de recursos que cada IDS aloca para ajudar seus vizinhos que é proporcional à credibilidade e a quantidade de recursos alocados por eles. Nos seus experimentos foi introduzindo um nó no jogo onde não cooperava para investigar a compatibilidade dos incentivos do sistema, que mostrou em determinas condições que o sistema controlava o equilíbrio pelo Nash, onde o algoritmo iterativo converge para o equilíbrio de Nash que é proporcional à sua utilidade para os ou-

tros nós. Os resultados experimentais mostram que o algoritmo converge para o equilíbrio de Nash, a uma taxa geométrica, o que confirmam ainda os resultados teóricos.

Nas propostas (ZHOU; KARUNASEKERA; LECKIE, 2007), (ZHOU; LECKIE; KARUNASEKERA, 2009) e (ZHOU; LECKIE; KARUNASEKERA, 2010) diferem na questão do algoritmo, pois cada nó tem que definir com qual nó poderá se colaborar em quanto na proposta do SIDIAC usa um gestor de confiança para definir quais são os nós que devem serem colaborados assim removendo esta função de análise do nó.

Zhu et al. (ZHU et al., 2010) apresentam um método de teste de hipóteses sequenciais para a agregação de *feedback* para cada nó da rede de detecção de intrusão (IDN). Foram investigados quatro resultados possíveis para uma decisão: falso positivo (FP), falso negativo (FN), verdadeiro positivo (TP) e verdadeiro negativo (TN), onde cada resultado está relacionado com um custo. A hipótese do feedback no teste de agregação sequencial proporcionou uma maior eficiência no custo em comparação com outros métodos heurísticos como: modelo de média simples e modelo de média ponderada. O algoritmo proposto reduziu a sobrecarga na comunicação dos *feedbacks* usando o modelo analítico. O mecanismo de consulta sequencial do IDS usa um diagnóstico de pares até que ele é capaz de tomar a decisão de agregação que satisfaça o critério *bayesiano* do custo otimizado, onde a decisão é tomada com base em uma regra de limite com uma taxa de probabilidade aproximada pela distribuição beta e limiares por taxa de alvo. Os resultados dos experimentos mostram que o modelo de agregação de feedback é superior a outros modelos proposto na literatura.

Em (ZHU et al., 2011) afirmam que as redes de detecção de intrusão colaborativas (CIDN) existentes tem que contar cada vez mais com o intercâmbio das informações o que causa preocupação com a privacidade dos participantes. Para isto propõem uma rede de detecção de intrusão (IDN) baseada no conhecimento assim fornecendo uma plataforma para os nós do IDS compartilhar seu conhecimento de detecção para todos os nós do IDN. O artigo contribui para o desenvolvimento de um protocolo de disseminação de redes baseado em uma estrutura descentralizada em que determina taxas de propagação das informações para cada destinatário, na aprendizagem *Bayesiana* onde cada nó estima a razão da compatibilidade com base de dados dos outros nós e o algoritmo distribuído para encontrar o equilíbrio de Nash e demostrar a eficiência do sistema. Em seus resultados foi possível demostrar através de simulações onde o equilíbrio do sistema tem as propriedades da compatibilidade e robustez a ataques de negação de serviço, além disto, o sistema também provou ser justo, eficiente e escalável.

Nos projetos de (ZHU et al., 2010) e (ZHU et al., 2011) difere em duas questões, no algoritmo matemático *Bayesiana* para definir as intrusões e no modelo de gestão de

confiança para saber quais são os nós confiáveis para fazer a colaboração, na proposta do SIDIAC usa o modelo matemático *Dempster-Shafer* para definir as intrusões e usa um gestor de confiança para saber quais os nós são confiáveis.

Para melhor compreender dos trabalhos pesquisados na Tabela 2.1 apresenta uma classificação pelos autores, relacionado seus resultados, se é simulado ou implementado, a arquitetura do CIDS, se é distribuído ou centralizado, o método de processamento da detecção de intrusão, se é por anomalia ou por assinatura e por último classificamos os métodos matemáticos usados para detecção da intrusão.

Tabela 2.1: Classificação dos projetos pelo tipo de CIDS

Artigos	**Resultados**	**Arquitetura**	**Processamento**	**Método**
[BYE et al., 2010]	Simulado	Distribuído	Anomalia e Assinatura	- -
[FARROUKH et al., 2008]	Simulado	Centralizado	-	Dempster-Shafer
[FUNG et al., 2009]	Simulado	Distribuído	Assinatura	Bayesiana
[FUNG et al., 2010]	Simulado	Distribuído	Assinatura	Bayesiana
[FUNG et al., 2010]	Simulado	Distribuído	Assinatura	Bayesiana
[FUNG, 2011]	Simulado	Distribuído	Assinatura	Bayesiana
[FUNG et al., 2011]	Simulado	Distribuído	Assinatura	Bayesiana
[FUNG et al., 2011]	Simulado	Distribuído	Assinatura	Dirichlet e Bayesiana
[FUNG et al., 2011]	Simulado	Distribuído	Assinatura	Bayesiana
[FUNG et al., 2012]	Simulado	Distribuído	Assinatura	Bayesiana
[FUNG e BOUTABA, 2013]	Simulado	Distribuído	Assinatura	Bayesiana
[LIN et al., 2008]	Simulado	Distribuído	Assinatura	-
[RAUN, 2012]	Simulado	Distribuído	-	-
[SHEN e XUE, 2010]	Simulado	Distribuído	Assinatura	
[SIRIVIANOS et al., 2011]	Implantando	Centralizado	Assinatura	-
[SOUZA et al., 2010]	Implantando	Centralizado	Assinatura	
[WU et al., 2003]	Simulado	Centralizado	Assinatura	Bayesiana
[YU et al., 2005]	Implantando	Centralizado	Anomalia e Assinatura	- -
[ZAMAN e KARRAY, 2009]	Simulado	Distribuído	Anomalia	-
[ZARGAR et al., 2011]	Simulado	Distribuído	Anomalia e Assinatura	- -
[ZHONG et al., 2008]	Implantando	Centralizado	Assinatura	Bayesiana
[ZHOU et al., 2005]	Simulado	Centralizado	Assinatura	
[ZHOU et al., 2007]	Simulado	Centralizado	Assinatura	
[ZHOU et al., 2009]	Simulado	Distribuído	Assinatura	
[ZHU et al., 2009]	Simulado	Distribuído	Assinatura	Bayesiana
[ZHU et al., 2010]	Simulado	Distribuído	Assinatura	Bayesiana
[ZHU et al., 2011]	Simulado	Distribuído	Assinatura	Bayesiana

Também foram pesquisados trabalhos importante sobre CIDS onde relaciona-se quatro trabalhos que abordam a segurança para arquitetura CIDS, esquemas para comparar arquitetura de CIDS e as revisões de literatura. A Tabela 2.2 descreve um quadro apresentado de forma sucinta da abordagem dos artigos.

O artigo (CHEUNG, 2011) vem alertar que ataques de injeção incorreta no sensor de segurança que pode comprometer um sistema detecção de intrusão colaborativa (CIDS) e para solucionar essa ameaça é necessário haver uma abordagem robusta para a prevenção. Apresentam algumas ameaças como:

- *Denial of Service* (DoS) pode-se empregar ataques baseados em *flooding* para esgotar recursos das máquinas enviando uma grande quantidade de pacotes para consumir toda a largura de banda da rede de um CIDS e assim evitando que os outros hosts comunicam-se com os CIDS;

- *Denail of Input* em que os ataques enviam pacotes para um espaço de endereço IP selecionado e interferem nos sensores que utilizam estatísticas para os CIDS publicados;

Cheung (CHEUNG, 2011) afirma que sua pesquisa é diferente das pesquisas anteriores pois se concentra em técnicas de computação robusta para estatísticas de CIDS, onde os adversários não possam distorcer os resultados ou controlar uma pequena fração dos contribuintes estimulando a geração falsos relatórios.

Em (ELSHOUSH; OSMAN, 2010) afirmam em seu artigo que uma solução de IDS tradicional (assinatura ou anomalia) não tem eficiência na detecção de invasão em ataques por diferentes computadores. Para resolver esse problema propõem o desenvolvimento de um sistema de detecção colaborativo usando as duas abordagens que chamam de CIIDS (Sistema de Detecção de Intrusão Inteligente Colaborativo). O artigo faz uma revisão da literatura sobre CIDS onde definem as seguintes arquiteturas:

- Centralizada : é uma abordagem que cada IDS desempenha um papel como uma unidade de detecção do CIDS, onde produzem alertas localmente e em seguida são enviados para um servidor central que funciona como uma unidade de correlação;

- Hierárquica: é dividido em vários pequenos grupos de comunicação, baseado em características geográficas, o controle administrativo e outras; e

- Distribuída: que é responsável pela coleta de dados localmente e possuem uma unidade de correlação onde gerencia a distribuição.

Também definem que um CIDS consiste em duas unidades funcionais principais que são:

- Unidade de Detecção que consiste de vários componentes de detecção, onde cada componente controla a sua própria sub-rede ou anfitriões separadamente e, em seguida, gera alertas de intrusão de baixo nível;
- Unidade de Correlação que transforma os alertas de intrusão de baixo nível em um relatório de intrusão alto nível de ataques confirmados.

Ao final da revisão da literatura o artigo sugere o uso da lógica de fuzzy e técnicas de inteligência artificial para reduzir taxas de falsos alarmes e mantendo alta detecção.

No artigo (JIA; CHEN, 2009) afirmam que não existe um método eficiente para avaliar o desempenho de sistema de detecções colaborativo (CIDS) e que é necessário criar um modelo matemático para fazer essa analise, perante esse problema eles propõem sua contribuição para os CIDS, onde mostram um modelo matemático que faz uma comparação entre CIDS. No experimento realizado para avaliar o modelo matemático foi usado dois CIDS, um baseado em anomalia e outro baseado em assinatura, os CIDS utilizado podem ser considerados com uma caixa preta onde recebem informações de entrada e avaliam se o estado é normal ou intrusivo, para modelar a entrada foram usadas variáveis aleatórias binárias, onde o dígito "um"representa intrusão e "zero"representa tráfego normal. Em seus resultados provam que CIDS baseado em anomalia é melhor do que o CIDS baseado em assinatura, pois devido à colaboração reduz a taxa de falso negativo assim melhorando a segurança do sistema.

No artigo (ZHOU; LECKIE; KARUNASEKERA, 2010) citam uma revisão de literatura sobre ataques e arquiteturas para sistemas de detecção de intrusão colaborativo (CIDS). Definem que os CIDS estão vulneráveis a três tipos de ataques:

- Ataque de *large-scale sealthy scans*;
- Ataque de *worm oubreaks*; e
- Ataque negação de serviço distribuído (DDoS).

Também define três tipos de arquiteturas para CIDS:

- Arquitetura centralizada: onde cada nó desempenha um papel como uma unidade de detecção do CIDS, onde produzem alertas localmente e em seguida são enviados para um servidor central que funciona como uma unidade de correlação.

- Arquitetura hierárquica: é dividida em vários pequenos grupos de comunicação, baseado nas seguintes características geográficas, o controle administrativo, coleta de plataformas de software similar e tipos de intrusões e cada grupo de comunicação é um subconjunto da hierarquia, onde existe um nó de análise que é responsável para correlacionar todos os dados coletados neste grupo.

- Arquitetura distribuída: cada participante do CIDS tem duas funções, uma unidade de detecção, que é responsável pela coleta de dados localmente e uma unidade de correlação que é uma parte do plano da correlação distribuída, os participantes se comunicam com os outros nós usando um protocolo de distribuição de dados, como peer-to-peer (P2P), multicast entre outros.

Tabela 2.2: Projetos de CIDS

Artigos	**Abordagem do artigo**
[CHEUNG, 2011]	Segurança a ataque em CIDS
[JAI e CHEN, 2009]	Avaliação de CIDS
[ZHOU et al., 2010]	Revisão de literatura
[ELSHOUSH e OSAMAN, 2010]	Revisão de literatura

2.5 Considerações finais

Muitos sistemas detecção estão sendo desenvolvidos nos últimos anos, conforme os trabalhos relacionados pela seção anterior é possível identificar que muitos desses projetos estão convergindo para uma abordagem colaborativa para sistema de detecção distribuído, devido esta abordagem ser mais eficiente na escalabilidade, confiabilidade e no sigilo da informação entre seus colaboradores (ZHOU; LECKIE; KARUNASEKERA, 2010).

Nos últimos anos os ataques distribuídos em redes de computadores são mais comuns e os sistemas individuais de IDS tem uma maior dificuldade de identificar intrusões. Após a revisão sistemática dos trabalhos notou-se que muitos pesquisadores estão optando pela solução de CIDS. Segundo, os rumos das pesquisas de IDS estão convergindo para soluções colaborativas ou distribuídas devido aos novos tipos de ataques coordenados ou distribuídos. Conclui-se que as abordagens de CIDS é uma boa solução para garantir a eficiência de um IDS, porém deve ser investigado os algoritmos da arquitetura para melhorar a precisão na detecção de intrusão.

Capítulo 3

Proposta de um Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa - CIDS

Verifica-se na literatura que sistemas de detecção de intrusão apresentam diversos tipos de soluções propostas, e todas apresentam soluções para as quais foram concebidas. Como já mencionado por (ZHOU; LECKIE; KARUNASEKERA, 2010) as pesquisas rumam para IDS distribuídos ou colaborativos.

Todavia o estudo de IDS que usem a abordagem colaborativa caminham para uma solução eficiente em diagnosticar as intrusões, demonstrando que essa é uma área que possui muito campo a ser desbravado. Desenvolver um projeto que contemple um sistema de detecção de intrusão com utilização de abordagem colaborativa e compará-lo com propostas da comunidade acadêmica é uma das contribuições desse estudo.

O embasamento teórico referencial para esse trabalho está descrito no Capítulo 2, onde verifica-se as diversas categorias de IDS e suas principais características que foram utilizadas para implementação dessa proposta que atendesse aos objetivos propostos por esse trabalho.

Esse capítulo apresenta as premissas e requisitos para o sistema proposto, sua arquitetura, sua estrutura de funcionamento e seus componentes.

A seção 3.1 trata da arquitetura do Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC), seus componentes e suas funcionalidades a secção seguinte apresenta o funcionamento dessa arquitetura e seu desenvolvimento.

3.1 Arquitetura Proposta do CIDS

A arquitetura proposta para o CIDS baseou-se em três trabalhos (FUNG, 2013), (ZHU et al., 2011) e (SIRIVIANOS; KIM; YANG, 2011), os quais propuseram sistemas para

detecção de intrusão colaborativos com características distintas.

O projeto HBCIDS de Fung et. al (FUNG, 2013), desenvolveu um protótipo em duas camadas: a primeira camada trata da detecção por assinatura baseada em HIDS, na segunda camada trata da colaboração usando uma rede *peer-to-peer*. Zhou et al. (ZHU et al., 2011) utiliza uma arquitetura centralizada para tratar a colaboração entres os nós participante e afirmam que a colaboração melhora muito a eficiência na detecção de intrusão.

A proposta de (SIRIVIANOS; KIM; YANG, 2011) propõem um algoritmo de colaboração entre os nós baseado na idéia para tratamento de *spam* avaliou-se empiricamente um servidor de e-mail (Postfix) no qual foi identificado um comportamento que poderia ser aplicado, este comportamento baseia em um servidor mal intencionado que envia vários e-mails usando uma base de dados de nomes para acertar e-mails válidos no servidor.

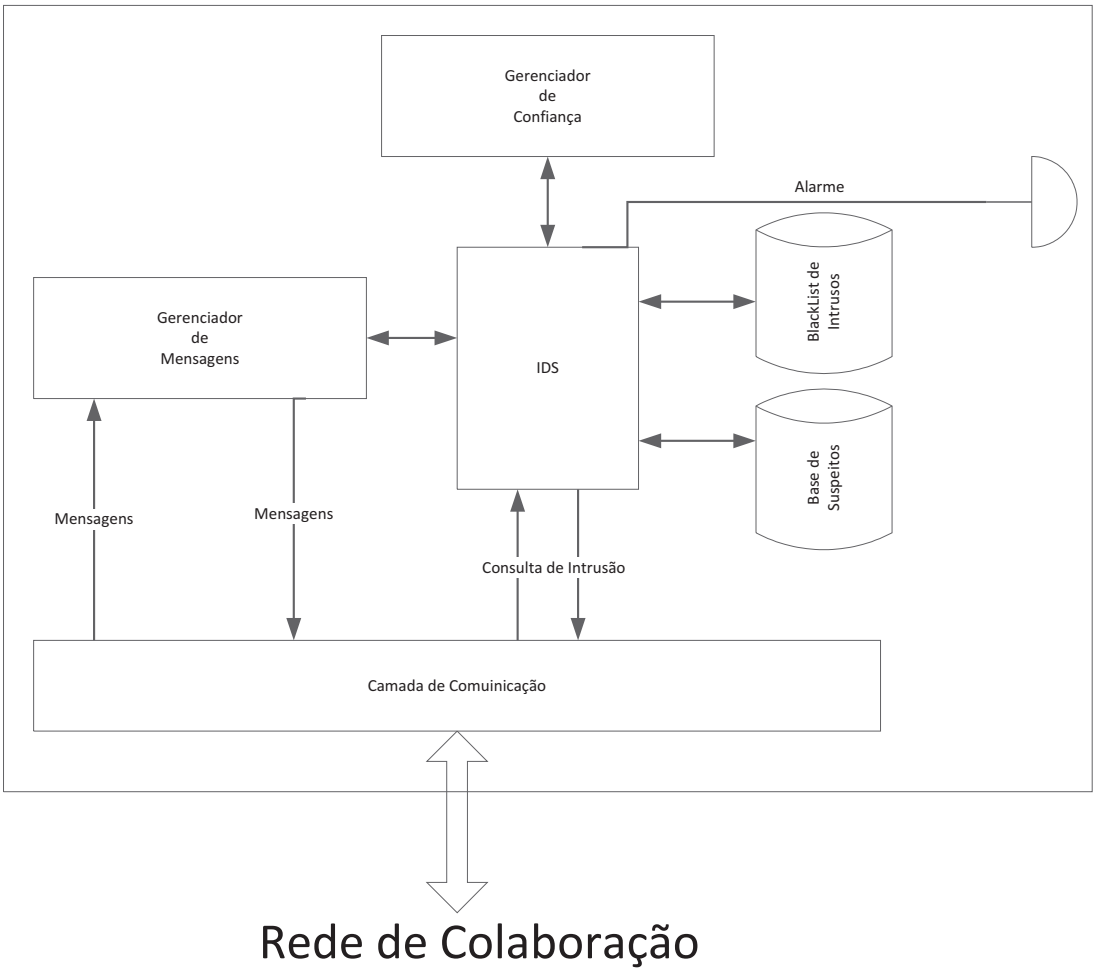

Figura 3.1: Arquitetura do CIDS Proposto

A arquitetura de um sistema de detecção colaborativo é uma proposta para diminuir os falsos positivos comprados com soluções locais conforme identificado nos artigos

de (WU et al., 2003), (ZHOU; KARUNASEKERA; LECKIE, 2005), (ELSHOUSH; OSMAN, 2010) e outros. Foi proposto para o projeto a concepção da arquitetura distribuída para colaboração entre os nós usando uma conexão *peer-to-peer* e o processo de análise dos dados entre os nós foi usado o modelos matemático de Dempster-Shefer (FARROUKH et al., 2008), onde os nós colaboram para definir se a suspeita é uma intrusão. O sistema proposto de CIDS foi implementado com base na arquitetura proposta por Fung et al. (FUNG; ZHANG; BOUTABA, 2010).

O sistema possui uma camada de comunicação que é responsável por receber e transmitir mensagens de comunicação e encaminhar ao gerenciador de mensagens, que tem por finalidade tratar as mensagens a serem entregues ao IDS, que ao receber a mensagem fará uso e utilizará sua base de dados de *BlackList*, podendo solicitar a sua lista de colaboradores que são tratados pelo gerenciador de confiança. A Figura 3.1 descreve essa arquitetura, que será descrita nas seções seguintes.

3.1.1 Gerenciador de Mensagens

O componente responsável por gerenciar todas as mensagens utilizadas pelo CIDS, que tratando de um sistema de colaboração, é parte importante da arquitetura. Na arquitetura proposta existem três tipos de mensagens utilizadas para que haja colaboração entre os CIDS:

- Mensagem de Consulta (*Query*): uma mensagem do tipo consulta é utilizada pelo sistema para verificar se os colaboradores possuem em seus bancos de dados o suspeito da consulta.
- Mensagem de Resposta (*Reply*): uma mensagem do tipo resposta é encaminha ao solicitante quando vem de uma consulta.
- Mensagem de Atualização (*Update*): uma mensagem do tipo atualização é encaminhada aos colaboradores para que todos atualizem suas bases de dados (*BlackList*).

A Figura 3.2 descreve esse tratamento de mensagens, quando o Gerenciador de Mensagens ao receber um tipo de mensagem verifica se essa é uma mensagem do tipo consulta (*Query*), essa mensagem é encaminhada ao componentes IDS que fará uma consulta a base de dados e caso o retorno seja positivo irá disparar o alarme de intrusão, caso contrário, encaminhará uma mensagem do mesmo tipo (consulta) aos seus colaboradores para que verifiquem em suas bases o suspeito. Ao receber uma mensagem de resposta (*Reply*) o gerenciador encaminha ao IDS que irá verificar se houve a identificação do suspeito, caso seja confirmada, ele irá atualizar a base de dados e emitirá um sinal de alerta,

em caso negativo descarta a possibilidade de intrusão. O último tipo de mensagem é o de atualização (*Update*), no qual a rede de colaboração trocam suas atualizações de base de dados (*BlackList*).

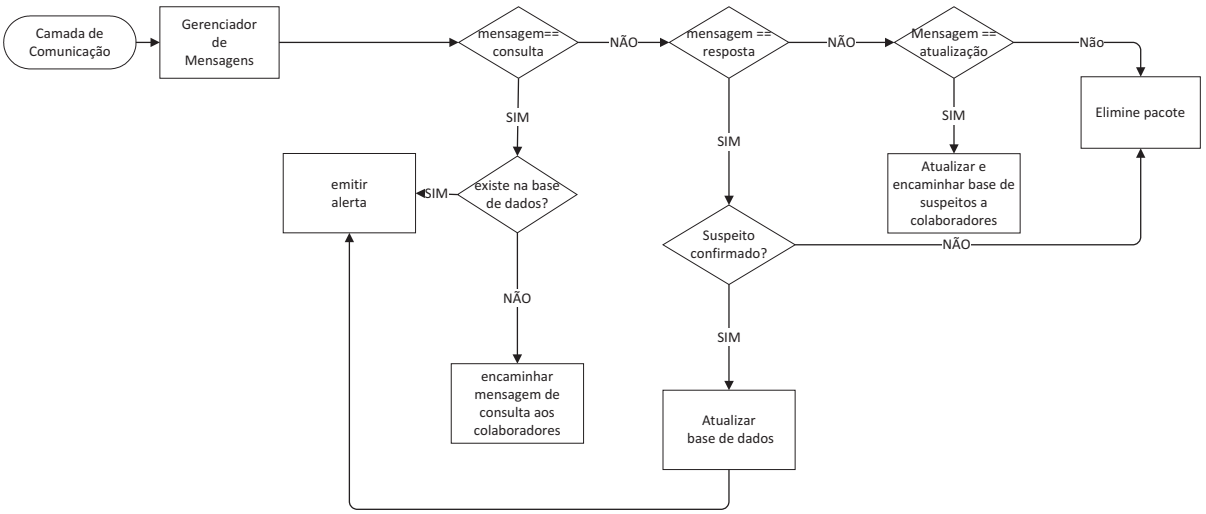

Figura 3.2: Fluxo de controle de Mensagens

3.1.2 Gerenciador de Confiança

O conceito de confiança é recente, há pouco mais de duas década atrás discutia-se sobre a definição desse tema. (AZZEDIN; MAHESWARAN, 2002) descrevem a confiança como sendo a crença em uma entidade e seu comportamento previsto, ou seja, sua ação é determinística. Em sistemas que envolvem a tomada de decisão envolvendo a confiança a certas entidades, é fácil associar isso considerando o histórico dessa entidade.

Esse componente é responsável por gerenciar os nós colaboradores em uma lista de confiança. No sistema proposto utiliza o modelo de reputação distribuído com a utilização de gerentes de reputação que determinam o grau de confiança dos colaboradores. O gerenciador de confiança armazena essa reputação e antes de estabelecer uma nova relação pode consultar outros gerentes sobre a reputação dessa entidade em questão. A Figura 3.3 ilustra várias redes com gerentes de reputação que compartilham seus valores de confiança entre si.

A adoção de gerentes de reputação e o compartilhamento dos valores de reputação pelos gerentes entre si introduzem um modelo de gerência de confiança. O modelo utiliza os gerentes de confiança como um serviço provido no sistema e por esse motivo, possui uma proteção é um diferencial em relação a sistemas centralizados, os quais possuem um único ponto de falha para comunicação, armazenamento, disponibilização e atualização

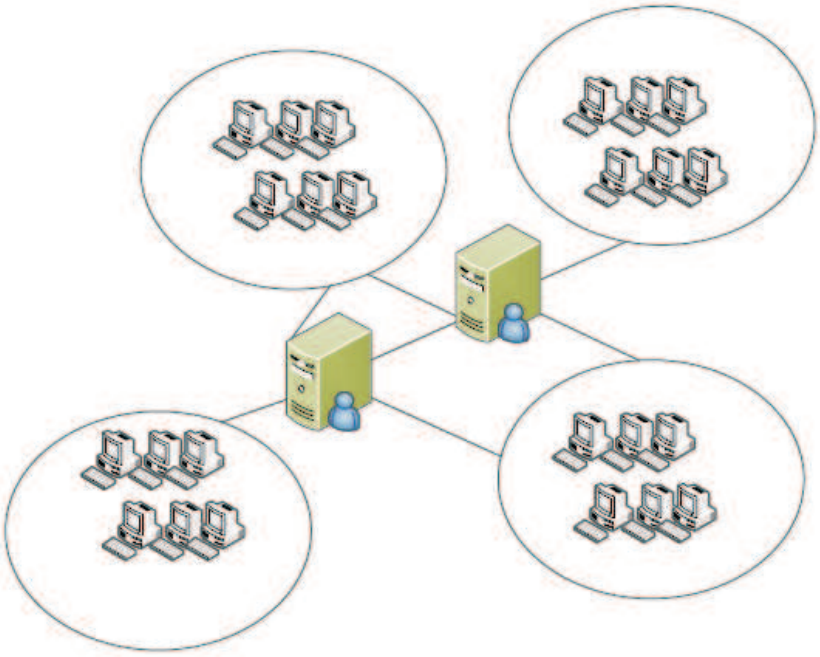

Figura 3.3: Modelo utilizado no Gerenciador de Confiança

dos valores de reputação.

3.1.3 IDS

Atualmente existe uma grande variedade de sistemas de IDS no mercado, devido a isso foi proposto por (KAHN et al., 1998) um modelo chamado CIDF (*Common Intrusion Detection Framework*) que agrupa um conjunto de componentes que definem uma ferramenta de IDS, o qual o sistema proposto utiliza em sua implementação. São características desejáveis destes componentes:

- Ser reutilizáveis, ou seja, devem ser configuráveis de forma a adaptarem-se a ambientes distintos;
- Ser modulares com funções distintas;
- Compartilhar/trocar informações entre si, para uma melhor precisão na identificação de intrusões;
- Auto reconhecimento de Componentes, ou seja, novos componentes devem identificar os demais componentes;

Existe um modelo de linguagem para troca de informações entre os componentes, chamada de CISL (*Common Intrusion Specification Language*) sendo o formato referenciado como *Generalized Intrusion Detection Objects*.

3.1.3.1 Componentes do Sistema IDS proposto

A seguir será descritos os componentes do sistema IDS proposto e suas funções no sistema.

- O Gerador de Eventos

  A função deste componente é obter os eventos a partir da camada de comunicação, ou seja, ele recebe os eventos mas não os processa isso fica a cargo do componente especializado na função de processamento que por sua vez após analisar os eventos (violação de política, anomalias, intrusão) envia os resultados para outros componentes.

- O Analisador de Eventos

  Este componente basicamente recebe as informações de outros componentes, as analisa e as envia de forma resumida para outros componentes, ou seja, recebe os dados de forma bruta, faz um refinamento e envia para outros.

- A Unidade de Resposta

  Este componente é responsável pelas ações, ou seja, gerar o alerta, reinicializar a conexão e notificar as estações de gerência e gravar informações na Base de Dados.

A Figura 3.4 demonstra o funcionamento do componente IDS proposto pelo sistema, onde o Gerador de Eventos receber um registro de acesso e encaminha ao Analisador de Eventos para verificação desse na base de dados (*BlackList*), a resposta da consulta é encaminhada a Unidade de Resposta, que dependendo do valor emitirá um alerta indicando intrusão.

Se a consulta não for encontrada o Analisador de Eventos fará uma análise do registro de acesso comparando essas informações com uma lista de regras de assinaturas, que são valores empíricos de intrusões e que podem representar tentativas de ataque a um sistema.

Caso a análise do registro esteja contido nessa lista de regras, ele encaminhará as informações a Unidade de Resposta que gravará esse registro em uma base de suspeitos e encaminhará uma mensagem de consulta aos colaboradores de seu gerenciador de confiança, os quais irão consultar em suas bases de dados de suspeitos em sua *BlackList*.

Ao receber a mensagem de resposta do tipo *Reply* e se ela for positiva, ou seja, o registro identificado é um suspeito já identificado na rede de colaboradores, a Unidade de Resposta incluirá esse registro na *BlackList* retirando esse sujeito da lista de suspeitos e emitirá um alerta.

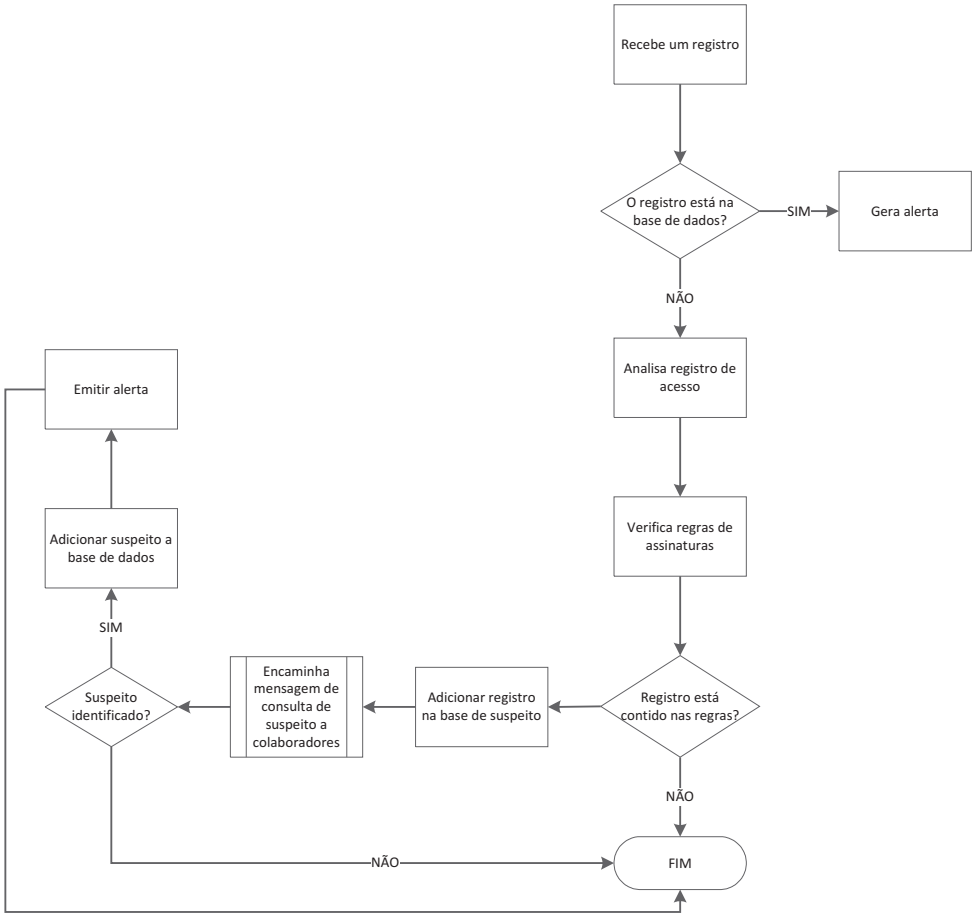

Figura 3.4: Diagrama de identificação de suspeitos pelo componente IDS do sistema proposto.

3.2 Funcionamento da Arquitetura

O diagrama de sequência da Figura 3.5 apresenta as iterações de mensagens trocadas pelo sistema proposto de CIDS com o gerente de reputação e seus colaboradores. O IDS recebe uma consulta de verificação de suspeito, e procura em sua base de dados para verificar se esse já não existe, caso a consulta retorne um valor encontrado ele emitirá um alerta de intrusão. Caso a pesquisa retorne um valor não encontrado, o IDS fará analise do registro confrontando com sua base de assinaturas de possíveis intrusões. Se esse registro for positivo, ele irá inserir o registro em uma base de suspeitos, e solicitará ao gerente de reputação uma lista de colaboradores, aos quais fará uma consulta da análise por ele realizada.

Após receber a lista de colaboradores o IDS emitirá uma consulta a esses, que verificarão em suas bases se o suspeito em questão é um intruso e retornaram a consulta.

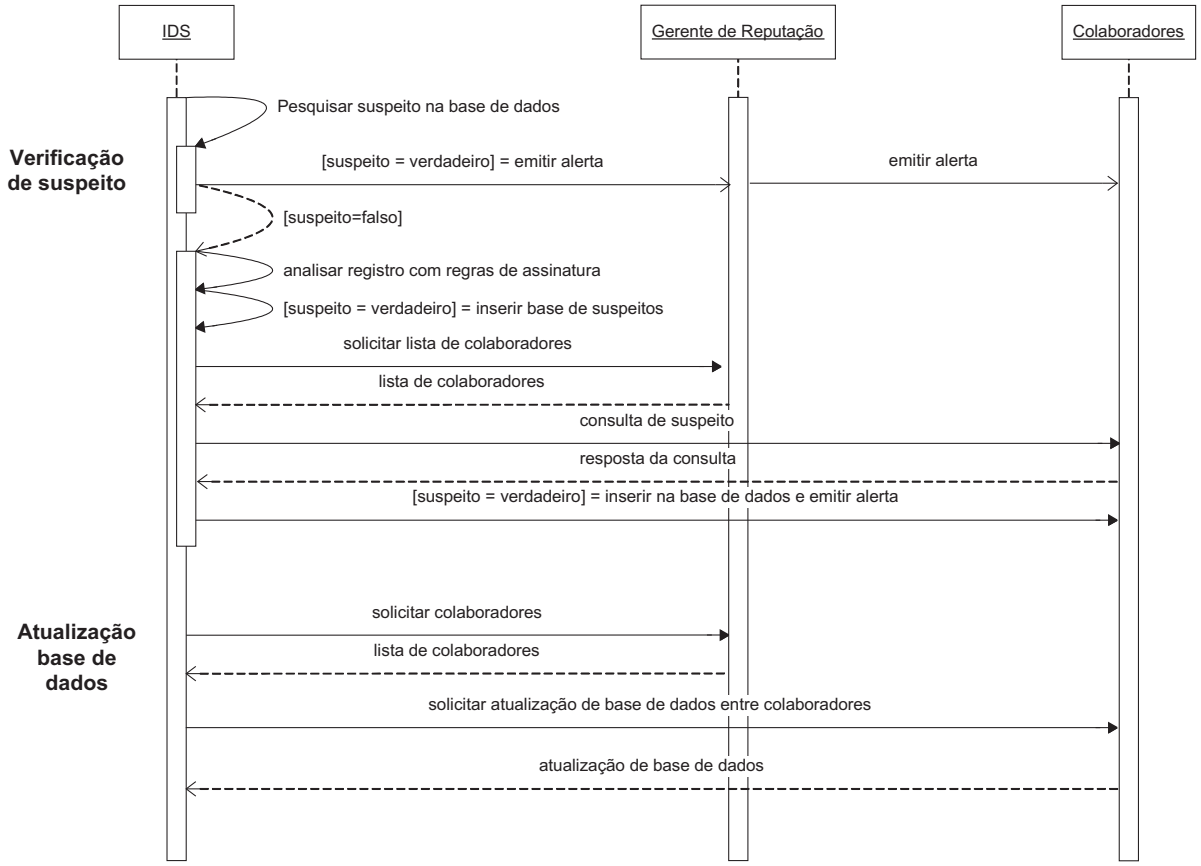

Figura 3.5: Diagrama de sequência do Sistema.

O IDS utiliza a fórmula derivada da estatística Baysiana (Equação 3.1), descrito abaixo

$$P(A \mid B) = \frac{P(B \mid A)\, P(A)}{P(B)} \tag{3.1}$$

onde $P(A)$ e $P(B)$ são as probabilidade a priori, ou seja, as probabilidades antes do evento acontecer. E $P(B \mid A)$ e $P(A \mid B)$ são as probabilidade a posteriori de B condicional a A e de A condicional a B respectivamente, ou seja, a probabilidade depois do evento acontecer.

O sistema proposto utilizou abordagem Dempster-Shafer, conhecida como teoria da evidência, que foi introduzida nos anos 60 com base nos trabalhos de Dempster e prorrogado por Shafer, ao contrário da teoria Bayesiana a teoria da evidência não precisa de conhecimento prévio da distribuição de probabilidade, e é capaz de atribuir valores de probabilidade para os conjuntos de possibilidades ao invés de apenas os eventos individuais. Também outra diferença é que não há necessidade de dividir toda a probabilidade entre os eventos, já que uma vez a probabilidade restante é atribuída para o ambiente e não para os eventos restantes (CAMPOS; CAVALCANTE, 2003).

A Equação 3.2 é utilizada pelo IDS para definir se o suspeito é um intruso, conforme as mensagens de resposta encaminhadas pelos colaboradores.

$$P(A \mid B) = P(B \mid A) \tag{3.2}$$

Também pode ser descrita como na Equação 3.3:

$$P(A \mid B) = B \cap A = A \cap B \tag{3.3}$$

Algoritmo 1 Algoritmo de consulta a colaboradores

```
1: //listCollaborators(nID);
2: //queryIntrusion (SID, query);
3: //Consulta suspeito na lista de colaboradores
4: pA = 0.5;
5: i = 0;
6: j = 1;
7: //collaborators recebe lista do gerente de reputação
8: collaborators = listCollaborators(nID)
9: while i < listCollaborators.size() do
10:    //DID recebe colaborador da lista
11:    DID = collaborators.get(i);
12:    //encaminha consulta para colaborador
13:    aux = reply(DID, query);
14:    //verifica se consulta retornou verdadeiro
15:    if aux = 1 then
16:       //adiciona intruso a base de dados de intrusos
17:       addListIntrusion(SID, query);
18:       //remove registro da lista de suspeito
19:       removeListSuspect(query);
20:    else
21:       if aux = 2 then
22:          j = j + 1;
23:       end if
24:    end if
25:    //verifica a probabilidade de registro ser suspeito
26:    if (j/listCollaborators.size()) > pA then
27:       //adiciona intruso a base de dados de intrusos
28:       addListIntrusion(SID, query);
29:       //remove registro da lista de suspeito
30:       removeListSuspect(query);
31:    end if
32: end while
```

Os Algoritmos 1 e 2 descrevem os métodos de consulta (*query*) e resposta (*reply*) respectivamente. Após o IDS consultar sua base de dados de intrusão e não encontrar

o suspeito, solicita a lista de colaboradores e encaminha a mensagem de consulta. E ao receber essa mensagem os colaboradores verificam em sua base de dados e em sua base de suspeitos retornando o valor da consulta ao IDS.

Algoritmo 2 Algoritmo de resposta de consulta de intrusão

```
1: //reply (DID, query);
2: // Mensagem de resposta sobre consulta de suspeito
3: // busca suspeito na base de dados de intrusão
4: if ListIntrusion.contents(query) then
5:    // retorna verdadeiro se encontrou
6:    return 1;
7: else
8:    //consulta na lista de suspeito
9:    if ListSuspect.contents(query) then
10:      // encontrou suspeito
11:      return 2;
12:   else
13:      // não encontrou suspeito
14:      return 0;
15:   end if
16: end if
```

Capítulo 4

Experimentos e Resultados

Nesse capítulo descreve-se a investigação da avaliação de desempenho do Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC) através de um conjunto de experimentos, utilizando a linguagem de programação Java. Os resultados são comparados a outros sistemas utilizados IDS, como em Fung (FUNG; ZHANG; BOUTABA, 2010) e o sistema proposto por Farroukh (FARROUKH et al., 2008).

O texto desse capítulo organiza-se da seguinte maneira. A seção 4.1 descreve o cenário das simulações e apresentam as métricas utilizadas para comparação, sendo que na seção 4.2 apresenta-se o desempenho do SIDIAC em a projetos propostos na literatura como Fung et al. (FUNG; ZHANG; BOUTABA, 2010), Farroukh (FARROUKH et al., 2008) e Oberheide et al. (OBERHEIDE; COOKE; JAHANIAN, 2008) . A seção 4.3 apresenta a aplicação prática do sistema SIDIAC em uma ambiente real.

4.1 Cenários das Simulações

Para realizar a simulação dos experimentos foi utilizado os parâmetros citados por (FUNG; ZHANG; BOUTABA, 2010) e comparados ao sistema proposto para avaliar a eficácia na detecção de intrusão em sistemas colaborativos. Na tabela 4.1 apresenta os parâmetros usados no projeto de Fung et al. que foi possível simular os resultados das Figuras: 4.1, 4.2 e 4.3.

Foi simulado em um ambiente com vários HIDS colaborando em conjunto com os mesmos e foram adotados dois parâmetros: taxa falsos positivos (FP) e taxas de falso negativo (FN).

Assim podendo avaliar a precisão da detecção dos HIDS. Para diagnóstico dessa simulação foram gerados dados através de um processo aleatório de Bernoulli.

Se as mensagens representar atividades suspeitas para os HIDS levanta um alarme

Tabela 4.1: Parâmetros de Simulação por Fung et al. (FUNG; ZHANG; BOUTABA, 2010)

Parâmetros	**Valores**	**Descrição**
R	10	Taxa de mensagens de teste
λ	0,95	Fator de esquecimento
Cfp/Cfn	20/100	Custo da decisão positivas e falsas
Tp	10	Período de estagio
Tu	1	Conhecimento do intervalo de atualização da lista
$Lini$	10	Comprimento inicial
$Lmax$	20	Número total máximo de conhecidos
$Lmin$	2	Comprimento mínimo da probabilidade da lista
Tmin	0,5	Taxa mínima de verdadeiro positivo aceitável
$Fmax$	0,2	Taxa máxima de falso positivo aceitável
q	0,5	Comprimento da liberdade condicional da lista de conhecimento
$\pi 1$	0,1	Probabilidade previa de intrusos

com uma probabilidade de FP, da mesma forma se representar atividades intrusas aciona um alarme FN.

O algoritmo foi desenvolvido em Java na versão 1.7 e executado em um computador com processador Intel Core i5-2400 de 3.10GHz com 4GB de RAM. Na Tabela 4.2 apresenta os parâmetros complementares utilizados para realização o experimento da 4.4.

Tabela 4.2: Parâmetros de Simulação Complementar

Parâmetros	**Valores**	**Descrição**
Registros aleatórios	10000	Número de registros aleatório
Suspeitos	0.2	Máximo aceitável de taxa de falso positivo
Intrusos	0.1	Mínimo aceitável de taxa de verdadeiro positivo
Avaliados	0.5	Taxa de probabilidade de conhecimento da lista de colaboradores

A métrica de eficiência de colaboração foi utilizada para avaliar o sistema proposto e o modelo utilizado por Fung et al. (FUNG; ZHANG; BOUTABA, 2010), o qual utiliza o modelo matemático Bayesiana (WASSERMAN, 2000) para decisão dos nós colaboradores na detecção de intrusão. O sistema proposto utiliza o modelo matemático Dempster-Shafer (FARROUKH et al., 2008) que não utiliza o conhecimento inicial do evento, onde pode-se verificar nos experimentos que em redes com um número reduzido de nós colaboradores sua eficiência é superior.

4.2 Resultados Obtidos

Inicialmente foi simulado um cenário com oito nós de HIDSs com suas taxas de falsos positivo (FP) e falso negativo (FN) utilizando probabilidades aleatórios contidas em um intervalo de 0,1 a 0,5. A Figura 4.1 ilustra a comparação do custo da detecção de falsa intrusão analisando os modelos de Fung et al. (FUNG; ZHANG; BOUTABA, 2010) comparado com o modelo de Oberheide et al. (OBERHEIDE; COOKE; JAHANIAN, 2008) e o sistema proposto.

É possível notar que o projeto de Fung et al. (FUNG; ZHANG; BOUTABA, 2010) prevalece perante o modelo de Oberheide et al. (OBERHEIDE; COOKE; JAHANIAN, 2008) e o sistema proposto nos primeiros nós da rede, melhorando significativamente ao número que os nós colaboram de forma mais eficientes.

Pode-se avaliar que a decisão de Oberheide et al. trata todos os participantes de forma igual enquanto o método Dempster-Shafer e Bayesiana reconhece os participantes com suas capacidades diferentes na detecção o que gera processos de baixo custo de decisões falsas.

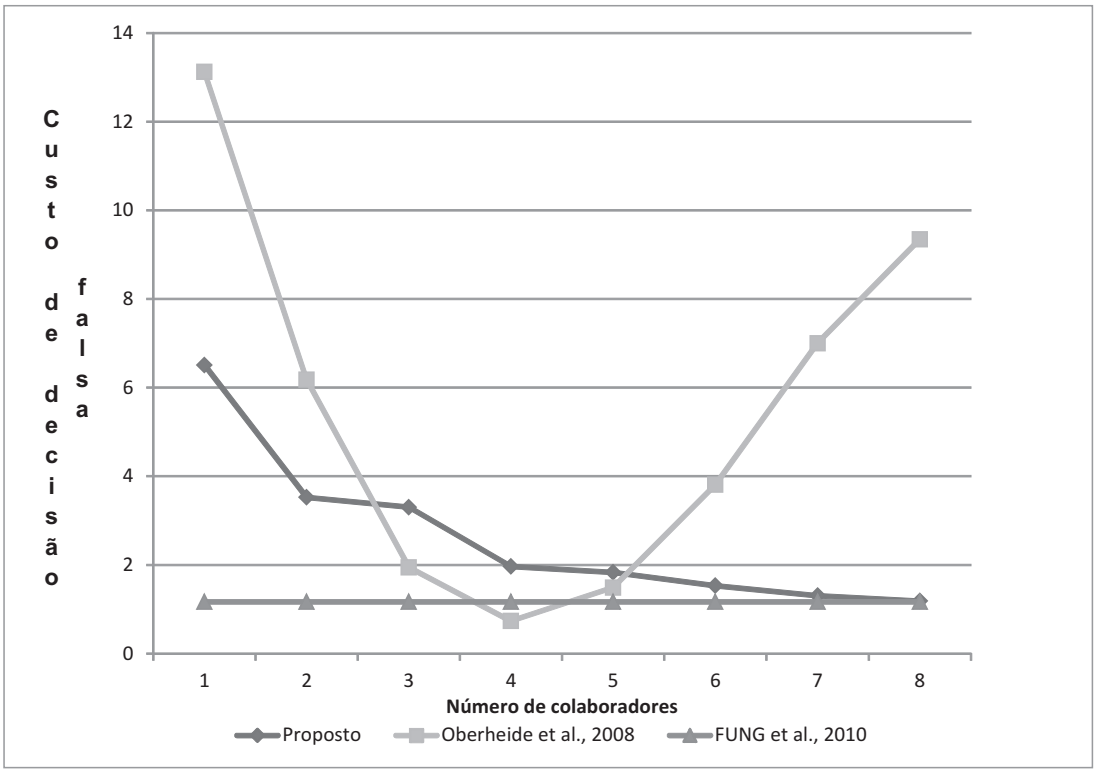

Figura 4.1: Comparação de custo utilizando métodos de decisão.

No próximo experimento foi avaliado o custo da manutenção esperado pelas decisões falsas no impacto do número de colaboradores. Essa métrica diz respeito ao número

ideal de colaboradores em uma rede para detecção de intrusão.

Foi desenvolvido um cenário com quinze nós colaboradores, onde há o interesse em verificar o custo da manutenção associado aos recursos utilizados para manter essa colaboração. Na Figura 4.2 verifica-se que o custo decresce quando há agregação de mais colaboradores. Pode-se observar que o sistema proposto tem o mesmo desempenho que o projeto de Fung et al. (FUNG; ZHANG; BOUTABA, 2010) a partir da entrada de mais nós colaboradores. O custo da manutenção chega ao ponto ótimo com nove colaboradores, isso afirma que com maior número de colaboradores terá um melhor custo de manutenção para identificar a intrusão.

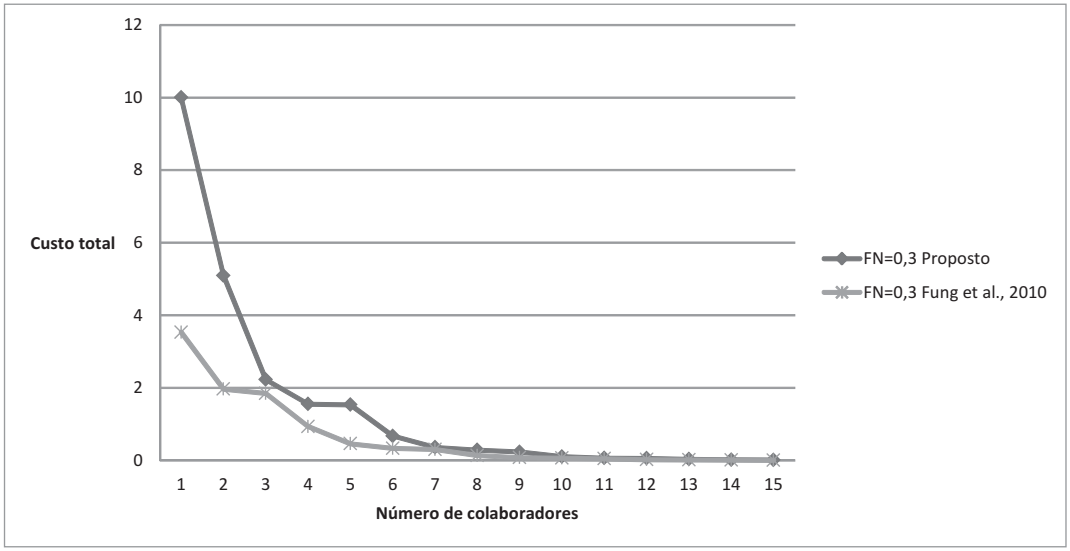

Figura 4.2: Custo médio da colaboração

O próximo experimento avalia o algoritmo de seleção gulosa proposto pelo projeto Fung et al. (FUNG; ZHANG; BOUTABA, 2010), onde compara-se com o sistema proposto. Na Figura 4.3 é possível identificar que o custo do uso do algoritmo guloso é mais eficiente que o sistema proposta e também identifica-se que quando o número de colaboradores é maior que onze nós a proposta equipara-se ao modelo comparado.

No último experimento foi comparado o percentual de intrusos detectados por uma amostragem aleatória de 10.000 registros, onde foram definidos 20% de suspeitos e 10% de intrusos considerando que a probabilidade de identificação de intrusos é de 50% dos nós colaboradores. Foram testados o modelo de Fung et al. (FUNG; ZHANG; BOUTABA, 2010), um modelo de detecção de intrusão centralizado utilizado por Farroukh et al. (FARROUKH et al., 2008) e o sistema proposto. Na Figura 4.4 pode-se identificar que a colaboração centralizada mantém os 50% de detecção, já o projeto de Fung et al. devido a utilização de um componente agregador de confiança começa tem um péssimo inicio, e melhora

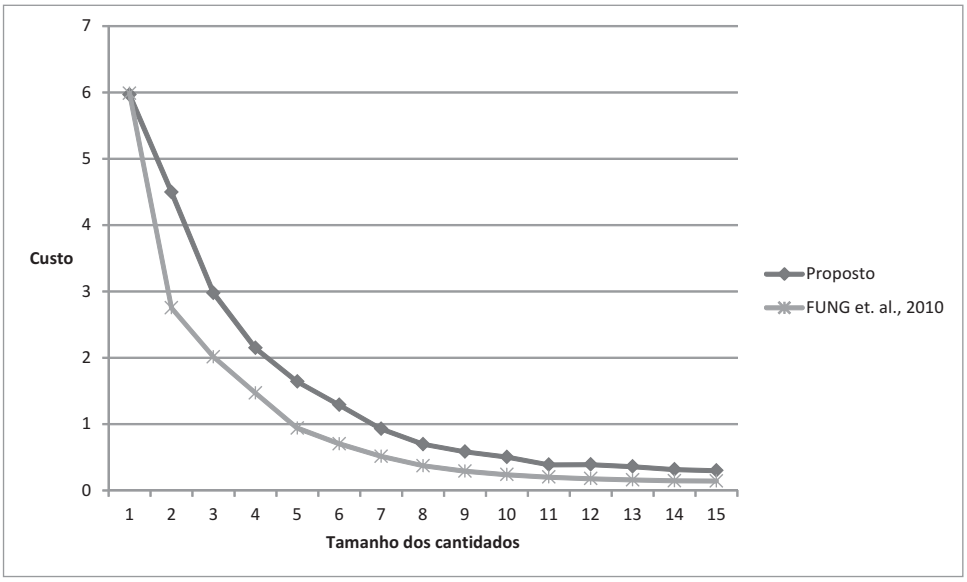

Figura 4.3: Custo usando algoritmo guloso para seleção de conhecimento

a medida que os nós aumentam sua colaboração. O sistema proposto tem um melhor desempenho em relação aos demais desde seu início comparando a Fung et al. ao final do número de nós colaboradores, provando que a utilização de colaboração entre sistemas IDS tem uma boa performance na detecção de intrusão.

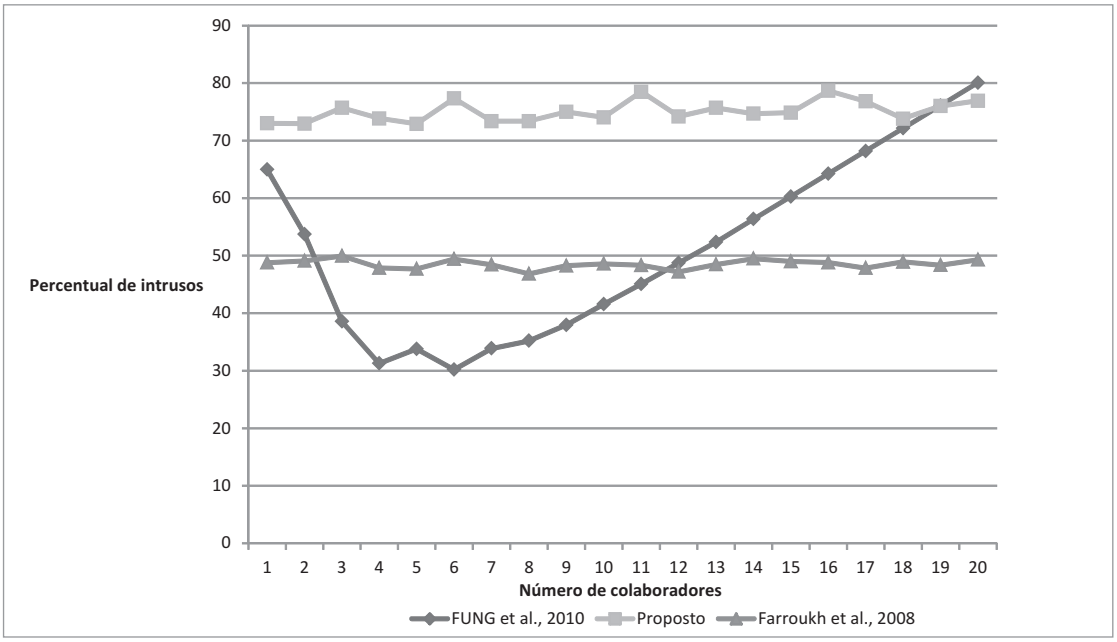

Figura 4.4: Percentual de Intrusos detectados por amostragem aleatória

4.3 Aplicação prática do Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC)

Para provar a eficiência do sistema proposto foram realizados testes em um ambiente real utilizando análise de dados de cinco servidores, usando o software comercial de gerenciamento de e-mail Postfix (VENEMA et al., 2012). Definiu-se um período de testes totalizando 240 horas de atividade dos servidores, na Tabela 4.3 apresenta uma visão de cada servidor analisado, onde é informado a quantidade de contas de e-mails, a quantidade de domínios e sua localização na Internet.

Tabela 4.3: Lista dos servidores usados nos testes

Nomes	**Número de clientes**	**Domínios**	**Localização**
A	87	5	Atlanta/GA/USA
B	226	36	Absecon/NJ/USA
C	21	1	Jaraguá do Sul/SC/BR
D	86	4	Itajaí/SC/BR
E	257	40	Joinville/SC/BR
Total	**677**	**86**	

4.3.1 Avaliação e resultados reais

No experimento realizado foi feita a análise em um grafo G(V,A) não orientado completo. Na Figura 4.5 comparou-se três resultados, sendo:

- A análise por regras de assinatura: usando a probabilidade condicional;
- A análise colaborativa das respostas únicas dos nós da colaboração: usando o modelos proposto para análise;
- A análise centralizada : onde todos os nós consultam um centralizador para identificar a intrusão.

4.4 Conclusão

Esse trabalho descreve o Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC), proposto para o controle eficiente de detecção de intrusão

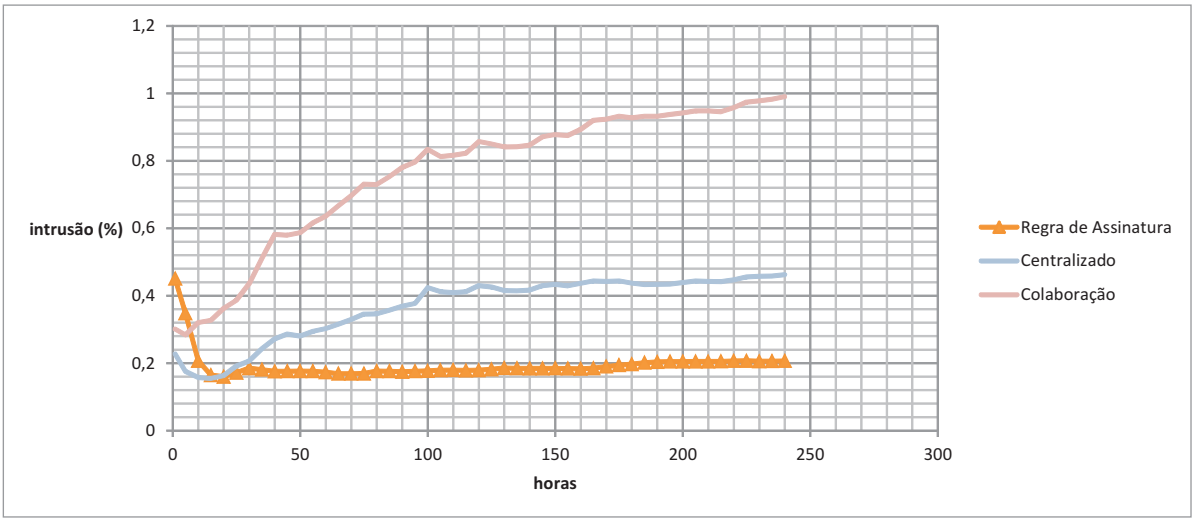

Figura 4.5: Avaliação da eficiência do sistema proposto

através da utilização de modelo de colaboração, apresentando um boa eficiência na detecção de intrusos. A avaliação do sistema foi realizada utilizando experimentos simulados computacionalmente com modelos propostos na literatura com Fung et al. (FUNG; ZHANG; BOUTABA, 2010), Farroukh et al. (FARROUKH et al., 2008) e Oberheide et al. (OBERHEIDE; COOKE; JAHANIAN, 2008). O sistema apresentou um bom desempenho na relação de detecção de intrusão por nós colaboradores, mantendo uma boa performance em relação aos demais, provando que pode ser utilizado para detecção de intrusão em redes colaborativas.

Capítulo 5

Conclusão

Esse trabalho apresentou o Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC), que utiliza o modelo matemático de Dempster-Shafer (CAMPOS; CAVALCANTE, 2003) comparado aos modelos implementados por Fung et al. (FUNG; ZHANG; BOUTABA, 2010) que utiliza o modelo Bayesiana, Farroukh et al. (FARROUKH et al., 2008) do modelo centralizado e Oberheide et al. (OBERHEIDE; COOKE; JAHANIAN, 2008), que utilizado o modelo limiar.

Na avaliação dos experimentos identifica-se que a abordagem Bayesiana apresenta melhores resultados em três experimentos realizados em relação devido ao modelo de decisão implementado por esse. O sistema proposto a medida que os nós colaboradores participam da decisão de identificação de intrusão se aproxima do modelo proposto por Fung et al.

Foi realizado também outro experimento comparando as abordagens de Farroukh et al. e Fung et al., onde o Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC) apresentou o melhor desempenho na identificação de intrusão nos primeiros 20 nós do que os demais.

O trabalho também apresentou uma análise do o Sistema de Detecção de Intrusão com utilização de Abordagem Colaborativa (SIDIAC) em um ambiente real, onde foram utilizados registros de cinco servidores e comparado com soluções comerciais. O sistema proposto apresentou o melhor desempenho na identificação de intrusão que a solução comercial.

5.1 Trabalhos Futuros

Verificou-se na revisão da literatura propostas que utilizam modelos de inteligência artificial para identificação de intrusão, como sugerido pelo projeto de Elshoush e Osaman

(ELSHOUSH; OSMAN, 2010) a utilização do modelo de Fuzzy. Como sugestão para trabalho futuros propõe-se a implementação do modelo colaborativo com utilização de técnicas de inteligência artificial e comparar sua eficiência com os modelos matemáticos Bayesiano e Dempster-Shafer.

Referências Bibliográficas

AZZEDIN, F.; MAHESWARAN, M. Evolving and managing trust in grid computing systems. In: IEEE. *Electrical and Computer Engineering, 2002. IEEE CCECE 2002. Canadian Conference on*. [S.l.], 2002. v. 3, p. 1424–1429.

BRADEN, R. Requirements for internet hosts-communication layers. 1989.

BYE, R.; CAMTEPE, S. A.; ALBAYRAK, S. Collaborative intrusion detection framework: characteristics, adversarial opportunities and countermeasures. In: *Proceedings of CollSec: Usenix Workshop on Collaborative Methods for Security and Privacy*. [S.l.: s.n.], 2010.

CAMPOS, F.; CAVALCANTE, S. An extended approach for dempster-shafer theory. In: IEEE. *Information Reuse and Integration, 2003. IRI 2003. IEEE International Conference on*. [S.l.], 2003. p. 338–344.

CENTER, C. C. Cert/cc statistics 1988-2006. *From Internet: URL http://www. cert. org/stats*, 2003.

CHEUNG, S. Securing collaborative intrusion detection systems. *Security & Privacy, IEEE*, IEEE, v. 9, n. 6, p. 36–42, 2011.

DANTAS, M. A. *Computação distribuída de alto desempenho: redes, clusters e grids computacionais*. [S.l.]: Axcel Books, 2005.

ELSHOUSH, H. T.; OSMAN, I. M. Reducing false positives through fuzzy alert correlation in collaborative intelligent intrusion detection systems?a review. In: IEEE. *Fuzzy Systems (FUZZ), 2010 IEEE International Conference on*. [S.l.], 2010. p. 1–8.

FARROUKH, A. et al. Distributed and collaborative intrusion detection systems. In: IEEE. *Communications Workshop, 2008. LCW 2008. IEEE Lebanon*. [S.l.], 2008. p. 41–45.

FUNG, C. Collaborative intrusion detection networks and insider attacks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, v. 2, n. 1, p. 63–74, 2011.

FUNG, C. *Design and management of collaborative intrusion detection networks*. Tese (Doutorado) — University of Waterloo, 2013.

FUNG, C. et al. Design of a Simulation Framework to Evaluate Trust Models for Collaborative Intrusion Detection. In: *IFIP Network and Service Security Conference (N2S 09)*. [S.l.: s.n.], 2009.

FUNG, C. et al. Trust management and admission control for host-based collaborative intrusion detection. *Journal of Network and Systems Management*, Springer, v. 19, n. 2, p. 257–277, 2011.

FUNG, C.; ZHANG, J.; BOUTABA, R. Effective acquaintance management based on bayesian learning for distributed intrusion detection networks. IEEE, 2012.

FUNG, C. et al. SMURFEN: A Framework of Knowledge Sharing for Collaborative Intrusion Detection. In: *17th International Conference on Network and Service Management (CNSM 2011)*. [S.l.: s.n.], 2011.

FUNG, C. J. et al. Dirichlet-based trust management for effective collaborative intrusion detection networks. *Network and Service Management, IEEE Transactions on*, v. 8, n. 2, p. 79 –91, june 2011. ISSN 1932-4537.

FUNG, C. J.; ZHANG, J.; BOUTABA, R. Effective Acquaintance Management for Collaborative Intrusion Detection Networks. In: *16th International Conference on Network and Service Management (CNSM 2010)*. [S.l.: s.n.], 2010.

GLOBO, J. *Lista de sites do governo afetados por onda de ataques virtuais*. 2013.

HWANG, K.; LIU, H.; CHEN, Y. Cooperative anomaly and intrusion detection for alert correlation in networked computing systems. *IEEE Transaction on Dependable and Secure Computing*, Citeseer, 2004.

INNELLA, P. et al. The evolution of intrusion detection systems. *SecurityFocus–2001*, 2001.

JIA, C.; CHEN, D. Performance evaluation of a collaborative intrusion detection system. In: IEEE. *Natural Computation, 2009. ICNC'09. Fifth International Conference on*. [S.l.], 2009. v. 6, p. 409–413.

KAHN, C. et al. A common intrusion... In: CITESEER. *Journal of Computer Security*. [S.l.], 1998.

LAZAREVIC, A.; KUMAR, V.; SRIVASTAVA, J. Intrusion detection: A survey. In: *Managing Cyber Threats*. [S.l.]: Springer, 2005. p. 19–78.

LEU, F.-Y. et al. Integrating grid with intrusion detection. In: IEEE. *Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on*. [S.l.], 2005. v. 1, p. 304–309.

LIN, W. et al. Collaborative distributed intrusion detection system. In: IEEE. *Future Generation Communication and Networking, 2008. FGCN'08. Second International Conference on*. [S.l.], 2008. v. 1, p. 172–177.

MAGALHAES, R. M. *Host-Based IDS vs Network-Based IDS*. 2006.

MAGAZINE, P. C. *Hacker do PS3 culpa arrogância da Sony por vazamento de dados da PSN*. 2011.

MENASCÉ, D. A.; NGO, P. Understanding cloud computing: Experimentation and capacity planning. In: *Computer Measurement Group Conference*. [S.l.: s.n.], 2009.

MISLOVE, A. et al. Ostra: Leveraging trust to thwart unwanted communication. In: *NSDI*. [S.l.: s.n.], 2008. v. 8, p. 15–30.

OBERHEIDE, J.; COOKE, E.; JAHANIAN, F. Cloudav: N-version antivirus in the network cloud. In: *USENIX Security Symposium*. [S.l.: s.n.], 2008. p. 91–106.

PATEL, A.; JÚNIOR, J. C.; PEDERSEN, J. M. An intelligent collaborative intrusion detection and prevention system for smart grid environments. *Computer Standards & Interfaces*, Elsevier, 2013.

RAN, Z. A model of collaborative intrusion detection system based on multi-agents. In: IEEE. *Computer Science & Service System (CSSS), 2012 International Conference on*. [S.l.], 2012. p. 789–792.

RANA, S.; GUJRAL, R.; SINGH, M. Securing grid using intrusion detection system. 2007.

RICHARDSON, R. Csi computer crime and security survey. *Computer Security Institute*, v. 1, p. 1–30, 2008.

ROESCH, M. et al. Snort: Lightweight intrusion detection for networks. In: *LISA*. [S.l.: s.n.], 1999. v. 99, p. 229–238.

SABAHI, F.; MOVAGHAR, A. Intrusion detection: A survey. In: IEEE. *Systems and Networks Communications, 2008. ICSNC'08. 3rd International Conference on*. [S.l.], 2008. p. 23–26.

SCARFONE, K.; MELL, P. Guide to intrusion detection and prevention systems (idps). *NIST Special Publication*, v. 800, n. 2007, p. 94, 2007.

SHEN, C.; XUE, S. Design and implementation of distributed collaborative intrusion detection system model. In: IEEE. *Fuzzy Systems and Knowledge Discovery (FSKD), 2010 Seventh International Conference on*. [S.l.], 2010. v. 3, p. 1224–1228.

SIRIVIANOS, M.; KIM, K.; YANG, X. Socialfilter: introducing social trust to collaborative spam mitigation. In: IEEE. *INFOCOM, 2011 Proceedings IEEE*. [S.l.], 2011. p. 2300–2308.

SNAPP, S. R. et al. Dids (distributed intrusion detection system)-motivation, architecture, and an early prototype. In: CITESEER. *Proceedings of the 14th national computer security conference*. [S.l.], 1991. p. 167–176.

SOUSA, P. et al. A collaborative approach for spam detection. In: IEEE. *Evolving Internet (INTERNET), 2010 Second International Conference on*. [S.l.], 2010. p. 92–97.

TANENBAUM, A. S.; STEEN, M. V. *Distributed systems*. [S.l.]: Prentice Hall, 2002.

TZI-CKER, C. *Constraints, Style and Focus of Industrial Security Research*. 2007.

VENEMA, W. et al. The postfix home page. *Postfix documentation*, 2012.

VIEIRA, K. et al. Intrusion detection for grid and cloud computing. *It Professional*, IEEE, v. 12, n. 4, p. 38–43, 2010.

WASSERMAN, L. Bayesian model selection and model averaging. *Journal of mathematical psychology*, Elsevier, v. 44, n. 1, p. 92–107, 2000.

WU, Y.-S. et al. Collaborative intrusion detection system (cids): A framework for accurate and efficient ids. In: IEEE. *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*. [S.l.], 2003. p. 234–244.

YEGNESWARAN, V.; BARFORD, P.; JHA, S. Global intrusion detection in the domino overlay system. In: *NDSS*. [S.l.: s.n.], 2004.

YU, J. et al. Trinetr: An architecture for collaborative intrusion detection and knowledge-based alert evaluation. *Advanced Engineering Informatics*, Elsevier, v. 19, n. 2, p. 93–101, 2005.

ZAMAN, S.; KARRAY, F. Collaborative architecture for distributed intrusion detection system. In: IEEE. *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on*. [S.l.], 2009. p. 1–7.

ZARGAR, S. T.; TAKABI, H.; JOSHI, J. B. Dcdidp: A distributed, collaborative, and data-driven intrusion detection and prevention framework for cloud computing environments. In: IEEE. *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2011 7th International Conference on*. [S.l.], 2011. p. 332–341.

ZHONG, Z.; RAMASWAMY, L.; LI, K. Alpacas: A large-scale privacy-aware collaborative anti-spam system. In: IEEE. *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. [S.l.], 2008. p. 556–564.

ZHOU, C. V.; KARUNASEKERA, S.; LECKIE, C. A peer-to-peer collaborative intrusion detection system. In: IEEE. *Networks, 2005. Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication., 2005 13th IEEE International Conference on*. [S.l.], 2005. v. 1, p. 6–pp.

ZHOU, C. V.; KARUNASEKERA, S.; LECKIE, C. Evaluation of a decentralized architecture for large scale collaborative intrusion detection. In: IEEE. *Integrated Network Management, 2007. IM'07. 10th IFIP/IEEE International Symposium on*. [S.l.], 2007. p. 80–89.

ZHOU, C. V.; LECKIE, C.; KARUNASEKERA, S. Decentralized multi-dimensional alert correlation for collaborative intrusion detection. *Journal of Network and Computer Applications*, Elsevier, v. 32, n. 5, p. 1106–1123, 2009.

ZHOU, C. V.; LECKIE, C.; KARUNASEKERA, S. A survey of coordinated attacks and collaborative intrusion detection. *Computers & Security*, Elsevier, v. 29, n. 1, p. 124–140, 2010.

ZHU, Q. et al. A game-theoretic approach to rule sharing mechanism in networked intrusion detection systems: Robustness, incentives and security. In: IEEE. *Decision and Control and European Control Conference (CDC-ECC), 2011 50th IEEE Conference on*. [S.l.], 2011. p. 243–248.

ZHU, Q. et al. A distributed sequential algorithm for collaborative intrusion detection networks. In: IEEE. *Communications (ICC), 2010 IEEE International Conference on.* [S.l.], 2010. p. 1–6.