Estado da Arte
Intrusion Detection System

1st Guilherme de Oliveira Kfouri
Departamento de Engenharia Elétrica (ENE)
Faculdade de Tecnologia (FT)
Brasília, Brasil
guiokfouri@gmail.com

2nd Daniel Gomes V. Gonçalves
Departamento de Engenharia Elétrica (ENE)
Faculdade de Tecnologia (FT)
Brasília, Brasil
gomesvenzi@gmail.com

3rd Bruno V. Dutra
Departamento de Engenharia Elétrica (ENE)
Faculdade de Tecnologia (FT)
Brasília, Brasil
brunodutr@gmail.com

4th João Fiuza de Alencastro
Departamento de Engenharia Elétrica (ENE)
Faculdade de Tecnologia (FT)
Brasília, Brasil
joao.alencastro@gmail.com

***Abstract*—Artigo de estado da arte no campo das tecnologias de sistemas de detecção/prevenção de intrusão. Nesse artigo fazemos uma análise do funcionamento padrão de soluções IDS, as metodologias utilizadas e o contexto em que as mesmas se aplicam.**

***Index Terms*—IDS, IPS, Estado da arte IDS, Características de um IDS, zero-day, defence in depth.**

I. Introdução

Intrusion detection systems, ou IDS's, são ferramentas de segurança que vêm se tornando cada vez mais necessárias à medida que firewall's e outras instâncias de segurança não são suficientes para garantir a integridade da rede [1]. Diante dos diversos ataques de redes, por exemplo os ataques DDoS contra grandes empresas: Amazon.com e E-bay nos anos 2000, GitHub(2018) utilizando o Malware Mirai BotNet, a mensagem de que é necessário investir em segurança ficou clara. Estudos mostram que quase todas as grandes corporações e grande parte das médias organizações já possuem algum sistema de detecção de intrusão [2].

Os IDS's foram introduzidos no mundo da segurança de comunicações com a função de monitorar, identificar e notificar a ocorrência de atividades maliciosas ou não autorizadas, se tornando assim uma camada de segurança cada vez mais essencial, uma vez que a complexidade e grau de automação dos ataques de rede tem aumentado exponencialmente.

Atualmente, no mundo globalizado e interconectado que vivemos, se tornou uma necessidade a oferta de serviços através da internet pública, e-commerce, por parte de empresas, sejam elas de pequeno, médio ou grande porte. Porém, deixar suas redes e serviços abertas dessa maneira expõe os mesmos para ataques e uso indevido, tornando assim a necessidade de implementações e pesquisa na área de segurança um pilar para a manutenção da integridade das comunicações em rede. Com o passar dos anos novas tecnologias de segurança foram surgindo, cada uma contendo suas respectivas forças e fraquezas, porém, nenhuma delas se destacou como a resposta para todos os problemas, visto que os ataques tem um espectro de atuação bem diverso. Para mitigar tal espectro foi desenvolvido o conceito de: "Defence in Depth" [3], onde a segurança não é implementada a partir de um único ponto, mas em uma série de camadas que respectivamente aplicam suas forças e vantagens naquilo que outras camadas tem como fraqueza, visando abrangir o máximo possível de ataques e anomalias.

De acordo com a abordagem de segurança "Defence in Depth", a segurança de organizações é dividida nas seguintes camadas [1]:

1. Política de Varredura e Segurança de Vulnerabilidades.
2. Segurança do sistema host.
3. Segurança do roteador.
4. Segurança de Firewall.
5. Detecção de intrusos.
6. Prevenção de intrusos.
7. Plano de Resposta a Incidentes.

Podemos ver que os IDS's apesar de possuírem alguns obstáculos para que a implementação seja eficiente tem evoluído e emergido como uma das soluções mais importantes da atualidade [1]. Além da realização de detecção de intrusos, possui como benefícios o arquivamento de incidentes, envio de relatórios para entidades responsáveis e a capacidade em alguns casos de defender a rede a ataques zero-day sem a necessidade de patches de segurança da comunidade ou de fabricantes.

Das várias possibilidades de IDS's iremos discutir sobre os tipos existentes na Seção 2. Na Seção 3, apresentamos as principais técnicas de detecção utilizadas atualmente e, na Seção 4, os Métodos empregados por IDSs. Terminamos na Seção 5, com uma breve conclusão.

II. Tipos de IDS's

A maneira mais comum de classificar IDS's é agrupá-los pela localização da informação fonte que eles utilizam para operar. As fontes primárias são: pacotes de rede capturados do backbone da rede ou de segmentos LAN, arquivos críticos de sistema e etc. Portanto IDS's podem ser classificados primariamente por:

A. Host Based IDS (HIDS)

Sistemas baseados em Host foram o primeiro tipo de IDS a ser desenvolvido e implementado. Eles ficam situados em apenas um Host, com a função de monitorar e analisar as informações coletadas neste e portanto, não observa o tráfego não endereçado ao seu hospedeiro. Seu uso está ligado ao rastreamento e verificação de informações relativas aos eventos e registros de logs e sistemas de arquivos, como arquivos de configuração, permissão entre outros. Os dados podem ser analizados localmente ou enviados para uma máquina de análise diferente.

HIDS's são extremamente úteis em detectar ameaças internas. Se um usuário tentar atividades não autorizadas, ou modificar arquivos não permitidos, um bom HIDS deve ser capaz de detectar e coletar informações pertinentes sobre a tentativa da maneira mais rápida possível.

Em uma dimensão muito grande o HIDS se torna problemático. Diante de uma grande rede com centenas de endpoints coletar e separar informações específicas para cada máquina individual se prova ineficiente e ineficaz. Outra desvantagem de HIDS's é a possibilidade de durante um ataque o próprio ser desativado [1, 4].

B. Network Based IDS (NIDS)

A forma comercial mais utilizada de Intrusion Detection System é a Network-Based [1]. Esses sistemas realizam detecção de ataques por meio da captura e processamento de pacotes advindos da rede em que se encontram. A detecção de ataque em geral é feita por comparação com uma base de dados que contém as assinaturas (características) de ataques e seus variantes, análise de anomalia por meio de comportamento padrão, decodificação de protocolos e etc [5]. Falaremos mais sobre os métodos de detecção na seção 3.

Para que a análise situacional de um IDS esteja de acordo com a situação real em que a rede se encontra é necessário um bom posicionamento do mesmo na rede. Em geral IDS's são executados de maneira "promíscua", ou seja, de maneira que consigam analisar todos tráfego da rede, até aquele que não é endereçado para ele. Mas a capacidade de analisar qualquer tráfego de nada importa se o mesmo não consegue chegar ao IDS, para isso o bom posicionamento é essencial para garantir a eficácia, um bom exemplo disso é a conexão de um NIDS com um switch central, de maneira que o switch faça o SPAN do tráfego da rede LAN para a interface do IDS.

Os fatos de NIDS's em geral analisarem a rede em modo "promíscuo" e em posicionamento privilegiado proporcionam a vantagem de dificultar a observação dele rede, tornando assim o ciclo de um ataque mais suscetível a detecção e falha, por simplesmente não saber que não está sendo observado.

A inserção de um NIDS resulta em pouco impacto na rede. NIDS's como dito anteriormente são sistemas passivos que analisam o que vem da rede sem interferir com o funcionamento padrão da mesma.

Alguns NIDS's possuem problemas em lidar com fragmentação de pacotes, causando instabilidade no funcionamento e possivelmente um fim na execução.

Um dos principais pontos negativos na utilização de NIDS's é o fato de que eles não conseguem fazer análise de tráfego criptografado [1], uma vez que por analisarem o tráfego de maneira promíscua não são os dispositivos finais cujo túnel de cifragem foi fechado com, impossibilitando assim uma análise mais profunda, ainda mais em redes modernas que cada vez mais tendem a adotar a criptografia como técnica essencial de comunicação [6].

C. IDS Híbrido

Os dois tipos de IDS diferem um do outro, porém, se complementam muito bem. A possibilidade de um IDS possuir tanto uma parte HIDS como uma parte NIDS é chamado de IDS Híbrido.Um IDS ideal deve ser híbrido, tendo em cada host um HIDS, cobrindo a capacidade de monitorar e analisar a informação local, e um NIDS examinando os pacotes que trafegam através da rede [7].

Na imagem 1 abaixo, é representado uma árvore que deriva diferentes tipos de IDS's.

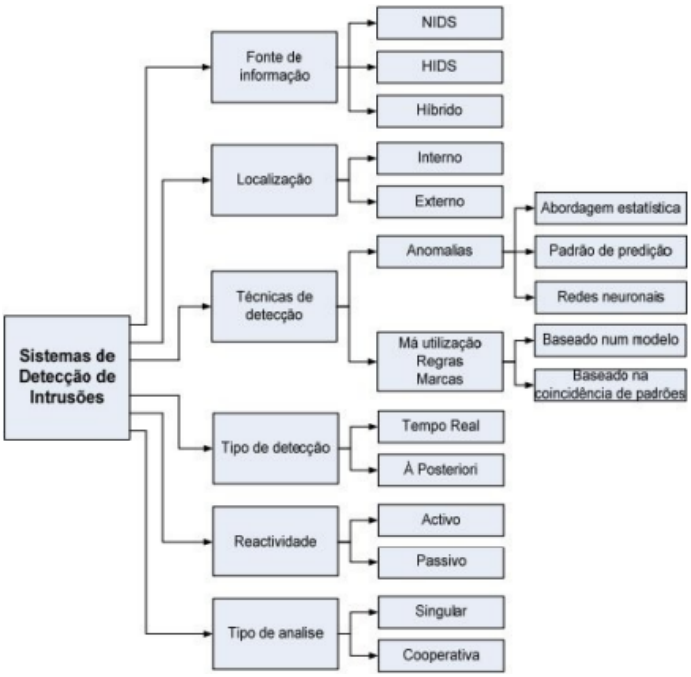

Fig. 1. Árvore de diferentes tipos de IDS's.

III. Técnicas de Detecção

Técnicas de Detecção ou Mecanismos de Detecção [5] são o núcleo do funcionamento de um IDS, eles são os responsáveis

por analisar o contexto de um rede/host para determinar se em certo momento um ataque está em execução ou não.

Existem várias abordagens utilizadas para detecção de intrusos, cada uma delas possuindo suas forças, fraquezas e desafios a serem superados.

A. Detecção por Assinatura

A Detecção baseada em assinatura, também chamada de Correspondência de padrões. Nessa metodologia um conjunto de regras que abordam as características de um ataque e seus variantes são cadastrados na solução, a partir do momento que o IDS está em execução todos os pacotes serão comparados com as informações cadastradas na regra a afim de se encontrar um padrão. Quando tal padrão é identificado um ataque pode ter sido avistado.

A funcionalidade de métodos de detecção baseados em assinatura se assemelham à Scanner de Vírus [8], uma vez que eles podem detectar todos os padrões conhecidos de ataques.

Para que esse método de detecção se torne efetivo é necessário uma base de dados [1][5] compreensiva e extensa de todos os ataques conhecidos e seus variantes, para que assim os mesmos consigam ser identificados, uma vez que detecção por assinatura é completamente ineficaz quando encontra os chamados ataques zero-day, ataques cujo comportamento e informações ainda não conhecidos, o que faz com que passem, em geral, completamente despercebidos por um IDS que tem como mecanismo de detecção assinaturas de ataques.

Como dito anteriormente, o grau de complexidade de ataques de rede vem crescendo com o tempo, e com isso o comportamento e as características dos ataques sejam modificadas. Para que um IDS que realiza análise por assinatura consiga se manter a par dos ataques recentes e por consequência seja capaz de proteger a rege de intrusos é necessário uma constante atualização da base de dados de comparação, afim de que ela ande lado a lado com as informações descobertas sobre novos ataques [1].

Pegar um dado e o comparar com uma base de dados pode ser um problema, uma vez que tanto a frequência com que novos dados vão chegando quanto o tamanho da base de dados podem ser enormes, tornando-se necessário um alto poder computacional, podendo em casos extremos comprometer a funcionalidade correta da IDS [1].

B. Detecção por Anomalia

A Detecção baseada em Anomalia parte do princípio que ataques são ações diferentes de atividades pré-estabelecidas como normais [4]. Inicialmente, é necessário definir um perfil de comportamento do que seria o uso rotineiro do usuário/Host ou grupo de usuários. Esse padrão deve ser feito empiricamente analisando, por exemplo, um período de uma semana de atividades e constatando quais são as atividades que ocorrem e que não ocorrem naturalmente.

O IDS então monitora a rede e utiliza diversas métricas para determinar se os dados estão dentro ou fora do perfil pré-estabelecido [10]. Como é natural e até esperado que haja mudanças e desvios do padrão feitos pelo próprio usuário sem intenção maliciosa gerando possíveis falsos positivos, há um grande desafio em utilizar técnicas para definir o padrão e para decidir se uma ação está dentro ou não do padrão.

Para se determinar o que é considerado um comportamento ”normal” há duas principais maneiras, descritas em [11], que são usadas para o objetivo de self-learning ou programmed anomaly detection.

No processo de self-learning, a IDS por Anomalia vai monitorar automaticamente eventos como tráfego de rede, no ambiente que ela foi implementada e tentar construir o que é considerado comportamento normal[11, 12]. No processo de programmed anomaly detection, o IDS deve manualmente aprender o que é considerado um comportamento normal tendo um usuário com uma função de ”professor”

Na segunda parte do processo de Detecção por Anomalia, o IDS deve classificar ações como dentro ou fora do padrão estabelecido por uma das 2 técnicas citadas acima. Para realizar isso afim de ter o menor número de falsos positivos possíveis são utilizadas diversas técnicas de computação e estatística.

Entre elas temos, TCM-KNN (Transductive Confidence Machines for K-Nearest Neighbors) usando machine learning [13], Redes neurais [14]

Uma das grandes vantagens da Detecção por Anomalia é que ela pode detectar ataques zero-day e assim produzindo novas assinaturas de ataques. Isso pode ser observado detectando ataques de novos worms automatizados. Se o sistema estiver infetado por um desses worms, este irá começar a scanear por outras vulnerabilidades no sistema em um passo acelerado, enchendo a rede de tráfego maléfico, causando uma anomalia na conexão TCP ou na largura de banda [12].

A Detecção por Anomalia pode apresentar o melhor resultado para ataques zero-day, porém, também possui suas desvantagens, que são:

1. Grande quantidade de Falsos positivos, baixa precisão;
2. Precisa de um período de treinamento;
3. Exige grande capacidade computacional para aplicar técnicas como machine learning, redes neurais entre outras.
4. Pode precisar de constante retreinamento devido a dados insuficientes de treinamento [15]

C. Detecção por Protocolo

A medida com que os ataques vão evoluindo torna-se necessário a exploração de novas superfícies de ataque em uma rede, uma delas se da por meio de tentativas de ataque por meio de falhas no funcionamento de protocolos de rede.

Interpretar um pacote de acordo com o protocolo e o analisar em buscar de tentativas de intrusão é chamado de Detecção por protocolo [1].

Em geral, o comportamento correto de um pacote de determinado protocolo [5] é baseado nas regras pré-estabelecidas para o protocolo pela RFC.

Tal metodologia de detecção tem a vantagem de ser mais rápida quando comparado por exemplo com Detecção por

Assinatura, uma vez que a quantidade de regras configuradas para se abordar todos os tipos de ataques e seus variantes é muito maior do que as especificações da RFC para o funcionamento correto de um protocolo. Assim os elementos a serem analisados estão em menor quantidade.

A Detecção por protocolo tem como fraqueza estar estritamente amarrada as determinações da RFC, se um ataque ocorrer sem a necissade de abusar de uma falha do protocolo será necessário a configuração de uma nova regra.

D. Detecção por Estado

Detecção por Estado [1] aborda a noção de que Detecção por Assinatura é incapaz de realizar detecções de ataques que ocorrem em vários passos, ao longo de uma conexão TCP por exemplo.

Com Detecção de Estado o IDS consegue realizar a remontagem de pacotes TCP na ordem correta sem overlapping. O rastreamento de conexões também é realizado, afim de determinar se um host talvez possa estar sofrendo de um DDoS por meio de um TCP handshake, ou seja, por meio da exaustão do número de conexões.

Os pontos fortes desse método de detecção são a visualização de ataques que outros tipos de IDS não conseguiriam, ataques em vários passos ao longo de uma conexão TCP e a capacidade de detectar ataques de pacotes longos.

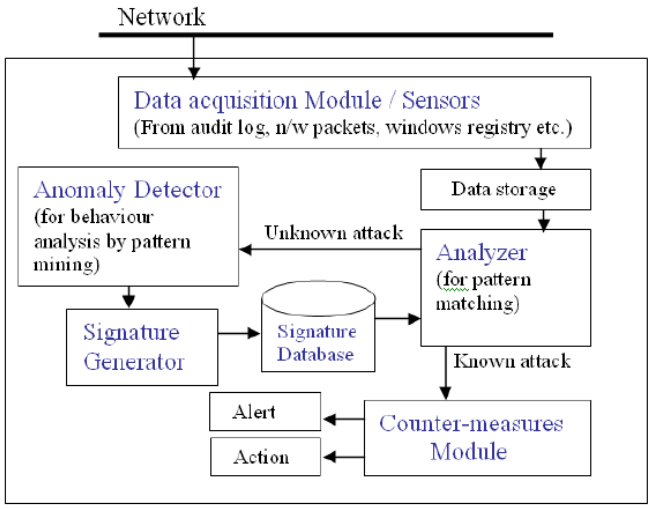

Fig. 2. Diagrama esquemático de um IDS híbrido. Fonte: [12]

IV. Temporização

Os IDS necessitam analisar as informações adquirida nos métodos de detecção mencionados acima, tanto para a geração de logs quanto para iniciar alguma ação de resposta. Para isso, um aspecto que determina com qual frequência a informação capturada será analisada é definido como Temporização [1]. Assim, duas maneiras de analisar os dados podem ser propostas: Análise em tempo real e Análise em blocos.

A. Análise em tempo real

Consiste em analisar os dados adquiridos imediatamente depois de sua captura pela interface de rede do IDS. A análise pode ocorrer de diferentes formas e diferentes níveis de profundidade. As observações feitas em [16] mostram o processo de implementação e o grau de detalhamento de uma análise em tempo real feita em um IDS rodando em ambiente real (Snort).

B. Análise em blocos

Consiste em analisar os dados adquiridos depois de armazenados e processados assim sua análise pode ser feita depois de algum tempo transcorrido da captura dos dados. Nesse tipo de análise um ataque pode ocorrer sem detecão mesmo com um IDS em funcionamento pois a análise dos dados só será feita posteriormente.

V. Métodos de Resposta

Existem dois métodos de resposta à detecção de atividades consideradas intrusivas em IDS convencionais.

A. Resposta Ativa

Conforme [1] a importância da resposta ativa nos IDS reside no no fato de parar a execução de um ataque durante sua ocorrência. Nessa abordagem a ação é feita imediatamente depois da análise considerar um determinado conjunto de dados suspeito. Um IDS ideal deve responder com uma ação imediatamente. Porém, existem inúmeras opições de ações que podem ser tomadas, dentre as principais citadas em [1] temos: reconfiguração de roteadores e firewalls, sequestro de sessão, bloqueio de endereço IP, término da sessão, etc.

B. Resposta Passiva

Ainda baseando-se em [1], quando se trata de resposta passiva, cabe diretamente ao administrador atuar em sequência à descoberta do ataque. Esse processo ocorreria após a coleta e correção dos eventuais dados. Normalmente a resposta passiva acontece em forma de notificação, seja via e-mail, SMS ou alerta 'popup'. Além disso, podem depender de 'armadilhas' SNMP que alertam os sistemas de gerenciamento da rede.

VI. Trabalhos relacionados

A. IDS's em redes de sensores wireless

Em [17] é introduzido uma detecção baseada em um esquema de segurança em redes de sensores wireless. Onde, apesar de sensores móveis possuírem baixa capacidade computacional e de comunicação, eles têm propriedades específicas como a sua estável informação da vizinhança que permite detectar anomalias na rede.

O sistema de detecção apresentado se baseia em ataques em que atacantes disfarçam seus dispositivos de sensores legítimos da rede, podendo injetar informações maliciosas, e, assim, manipular sistemas.

As soluçõe concluída por [17] engloba métodos de detecção em que os sensores baseiam-se em informações esperadas de

suas vizinhanças, podendo assim, detectar e reportar anomalias. E também, utilizam protocolos de compartilhamento de estado ou comportamento esperado para nós vizinhos.

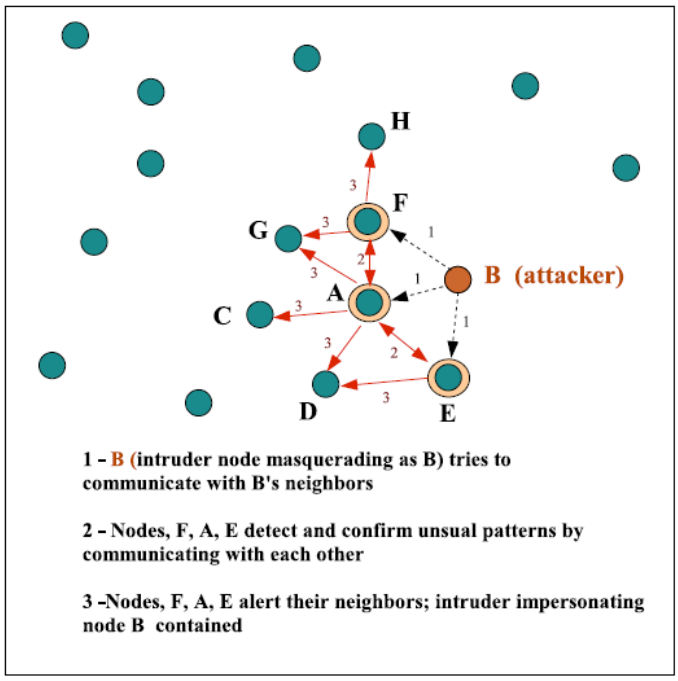

Fig. 3. Representação de um ataque ocorrendo na rede. Fonte: [17]

B. IDS's cooperativos para sistemas ad hoc

Este trabalho [18], a abordagem é feita de maneira mais centralizada. Apesar, de o trabalho em [17] também utilizar o conceito de 'Mobile ad hoc networking' (MANET), em [18] a resposta é proveniente de um algoritmo que elege um nó periodicamente a virar o agente DI (Detector de Intrusão) para simular um ambiente 'clusterizado'. Essa topologia pode trazer grande eficiência enquanto mantém o mesmo nível de efetividade.

Outra diferença percebida nos trabalhos foi a quantidade de ataques ou 'exploits' citados e estudados. São abortados ataques como:

1) 'Black Hole': Buraco negro é quando todo o tráfego é direcionado para um nó específico, que pode não repassar tráfego algum.

2) 'Routing Loop': O ciclo de roteamento acontece quando um ciclo é introduzido em uma rota.

3) 'Network Partition': Particionamento de rede ocorre quando uma rede conectada é particionada em k ($k \geq 2$) sub-redes, onde nós em diferentes sub-redes não podem se comunicar, mesmo que haja uma rota entre eles.

4) 'Selfishness': O ataque de egoísmo acontece quando um nó não está servindo como repetidor para outros nós.

5) 'Sleep Deprivation': Privação de sono é forçar um nó a exaurir/esgotar sua energia da bateria.

6) 'Denial-of-Service': E o mais famoso de todos, negação de serviço, onde um nó é privado de receber e enviar pacotes de dados para seus destinos.

VII. Conclusão

Como foi apresentado na primeira seção, um modelo é melhor estruturado quando a segurança dos sistemas não dependem somente de um método de detecção, apresentando maior complexidade para ser invadido. Um bom modelo de segurança envolve componentes como políticas de acesso, firewalls, IDS's, plano de respostas à incidentes.

A construção de uma taxonomia de princípios de detecção de intrusão prova ser um exercício proveitoso que fornece muitas percepções diferentes para pesquisas futuras.[11]

Os métodos citados possuem suas respectivas vantagens e desvantagens. Uma abordagem heterogênea, utilizando parcelas dos métodos de detecção, varia de acordo com a aplicação e deve ser pensada cautelosamente, já que alguns desses métodos requerem altas taxas de processamento.

References

[1] Peddisetty Naga Raju, Prof. Viiveke Fåk State-of-the-art Intrusion Detection Technologies, Challenges, and Evaluation", Information theory Division, Dept of Electrical Engineering, Linköping University, 2005.

[2] SANS Institute staff - "Intrusion Detection and Vulnerability Testing Tools: What Works?" 101 Security Solutions E-Alert Newsletters, 2001.

[3] Michael Coole, Jeff Corkill, Andrew Woodward - Defence in Depth, Protection in Depth and Security in Depth - A Comparative Analysis Towards a Common Usage Language", Australian Security and Intelligence Conference, 2012.

[4] Paul Innella and Oba McMillan, Tetrad Digital Integrity, LLC Introduction to Intrusion Detection Systems, December 6, 2001

[5] Matin Roesch - "Snort - Lightweight intrusion detection for networks", 1999.

[6] WIRED - "Half of the web is now encrypted. That makes everyone safer", https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer, 2017.

[7] Simranjeet Singh - "A HYBRID INTRUSION DETECTION SYSTEM DESIGN FOR COMPUTER NETWORK SECURITY", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES AND RESEARCH TECHNOLOGY, 2018.

[8] Peter Szor - "The Art of Computer Virus Research and Defense", Symantec press, 2005.

[9] Gong, F. (2003). Deciphering Detection Techniques: Part II Anomaly Based Intrusion Detection White Paper, McAfee Security, McAfee Security White Paper, 2003, Retrieved October 10, 2012.

[10] Stillerman, M., Morceau, C., andStillman, M. (1999). —Intrusion Detection for Distributed Applications‖, Communications of the ACM, 42(7), July, 1999, 62-69

[11] Axelsson, S. (2000). Intrusion-detection systems: A taxonomy and survey. Tech. Rep. 99-15, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 200.

[12] Kanubhai K. Patel, Bharata V. Buddhadev - An Architecture of Hybrid Intrusion Detecion System, Departmente of Computer Engineering, LDCE, G T University (2003).

[13] Yang Li, Li Guo - "An active learning based TCM-KNN algorithm for supervised network intrusion detection", Computers and Society (2007).

[14] Adrian P. Lauf, Richard A. Peters, and William H. Robinson, (2007), Embedded Intelligent Intrusion Detection: A Behavior-Based Approach,Department of Electrical Engineering and Computer Science Vanderbilt University School of Engineering, 2301 Vanderbilt Place.

[15] Botha, M., andvon Solms, R., (2003). — Utilizing fuzzy logic and trend analysis for effective intrusion detection, In Computers and Security, volume 22, 2003, pp 423–434

[16] Mukesh Sharma, Akhil Kaushik, Amit Sangwan, Assistant.Professor, Mtech Scholor, (2012). Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort, 2012, pp 3–4

[17] Onat, I., & Miri, A. (n.d.). An intrusion detection system for wireless sensor networks. WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.

[18] Yi-an Huang, Wenke Lee. A cooperative intrusion detection system for ad hoc networks - Proceedings of the 1st ACM workshop on Security of . . . , 2003 - dl.acm.org