Information Horizons: AMERICAN Journal of Library And Information Science Innovation
Volume 2, Issue 12, 2024 ISSN (E): 2993-2777

Network Attack Detection Systems (Intrusion Detection Systems, IDS) and their Capabilities

Mallayev Oybek Usmankulovich
Alfraganus University, PhD, Dotsent
Mukhamedaminov Aziz Odiljon O‘g‘li
Engineer UNICON.UZ

Abstract. *This article presents the opinions of domestic and foreign scientists on modern methods for developing network attack detection systems. "Network attack detection systems" refers to systems designed to identify, monitor, and respond to unauthorized or malicious activities within a computer network. These systems aim to protect the network from potential security breaches or attacks. Common examples include Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The article presents a comparative analysis of network access detection systems.*

Keywords: *Network Intrusion Detection Systems (NIDS), Intrusion Prevention Systems (IPS), Statistical anomaly detection, Locations of Deployment, Demilitarised zones, Training a model using labelled datasets of network traffic, support vector machines.*

Introduction.

Security systems called Network Intrusion Detection Systems (NIDS) keep an eye on network traffic for malicious activities and send out alerts when they spot questionable trends. They serve as an essential line of defence in an all-encompassing cybersecurity plan. Instead of actively blocking or preventing attacks, NIDS mainly detect them, in contrast to Intrusion Prevention Systems (IPS). They are responsible for spotting dangers and alerting administrators so that manual action or the activation of additional security measures may take place.[1]

This is an explanation of NIDS:

How NIDS Operate:

NIDS analyse packets on a network segment to passively monitor network activity. They accomplish this in a number of ways:

Detection by signature: This is the most used method. Network traffic is compared by NIDS to a database of known attack signatures, or harmful traffic patterns. An alert is set off if a match is discovered. This approach can overlook new or zero-day attacks, but it works well against established threats.[2]

Using anomaly-based detection, a baseline of "normal" network traffic is established. An alarm is triggered by any notable departure from this baseline. Although this technique can identify undiscovered assaults, it is prone to false positives in the event that network behaviour changes in a

[1] **Stallings, W.** (2020). *Network Security Essentials: Applications and Standards.* Pearson Education.
[2] **Scarfone, K., & Mell, P.** (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).* National Institute of Standards and Technology (NIST).

legal way or if the baseline is not precisely set.

Materials.

Statistical anomaly detection: This technique finds abnormalities by statistically analysing network traffic.

Machine learning-based detection: Even if the patterns are previously unknown, advanced NIDS use machine learning algorithms to examine network data and find patterns suggestive of malicious activity. This provides more precision and flexibility in response to changing dangers.[3]

NIDS types include:

Network traffic passing via a particular network segment, such as a switch port, router interface, or network tap, is monitored by network-based intrusion detection systems (NIDS). It looks for malicious behaviour in the payloads and packet headers.

Although not quite an NIDS, host-based intrusion detection systems (HIDS) should be distinguished. Instead of keeping an eye on the entire network, HIDS keeps an eye on activities on a particular host, such as a computer or server. It looks for unusual behaviour in process activity, file system modifications, and system logs.[4]

Locations of Deployment: To optimise their efficacy, NIDS are usually placed in key areas of the network:

Network perimeter: keeping an eye on all incoming and outgoing traffic.

Internal network segments: keeping an eye on traffic in certain network segments to identify potential internal dangers.

Demilitarised zones, or DMZs, are used to safeguard servers that are accessible via the internet.

Benefits of NIDS:

Full network visibility: Able to keep an eye on every bit of traffic moving across a particular network segment.[5]

Unknown attack detection (with anomaly-based systems): Able to detect assaults that signature-based systems are not yet aware of.

Network traffic is not impeded by passive monitoring.

Scalability: Able to grow to fit big networks.

Research and methods.

NIDS drawbacks include:

High alert volume: May result in a large number of false positives, necessitating thorough investigation of each alarm by administrators.

Impact on performance: Although often passive, performance may be impacted by unusually large traffic levels.

Limited context: The source and target of assaults may not be fully understood.

Vulnerable to evasion tactics: Skilled attackers may use strategies to avoid discovery.

Modern techniques for creating network attack detection systems take advantage of developments in big data analytics, artificial intelligence, and machine learning to get beyond the drawbacks of conventional signature-based methods. Below is a summary of various techniques:

---

[3] **Bace, R. G., & Mell, P.** (2001). *Intrusion Detection Systems.* NIST Special Publication 800-31.

[4] **Northcutt, S., & Novak, J.** (2002). *Network Intrusion Detection.* Sams Publishing.

[5] **Davis, J., & Magrath, S.** (2013). *A Survey of Network-Based Intrusion Detection Data Sets.*

1. Based on machine learning (ML) Methods:

Training a model using labelled datasets of network traffic—where each data point is classified as either benign or malicious—is known as supervised learning. Typical algorithms that are employed include:

SVMs, or support vector machines: It can manage non-linear connections and works well with high-dimensional data.[6]

Random Forests: An ensemble learning technique that enhances accuracy and resilience by combining many decision trees.

Neural networks, particularly deep learning, are highly accurate in extracting intricate patterns and characteristics from unprocessed network data. For the analysis of sequential data, such as network packets, Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are very useful.[7]

Unsupervised Learning: This method finds abnormalities and departures from typical behaviour by analysing network traffic without labelled data. Beneficial for identifying new threats and zero-day attacks:

Results.

Clustering methods (like DBSCAN and k-means) reveal outliers as possible threats by grouping together similar network traffic patterns.

Neural networks that can learn to recreate input data are called autoencoders. When the reconstruction error is large, anomalies are found.

One-class SVM: recognises deviations as anomalies by training a model on typical traffic data.

Reinforcement Learning: By interacting with the network environment and rewarding accurate classifications, this technique may be utilised to create adaptive intrusion detection systems that learn and get better over time.

2. Based on Deep Learning (DL) Methods:

A kind of machine learning called deep learning is particularly good at processing high-dimensional, complicated data. Among the particular architectures utilised are:

Recurrent neural networks (RNNs) are good at collecting context and temporal relationships in sequential input, such as network packets. Two common RNN variations are Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU).[8]

Autoencoders: Used for anomaly detection by reconstructing typical network traffic and identifying deviations as possible attacks. Convolutional Neural Networks (CNNs): Effective for extracting spatial features from network traffic data, such as image representations of packet headers or network flows.

Synthetic network traffic data may be produced by Generative Adversarial Networks (GANs), which can enhance training datasets and increase model resilience.

3. Hybrid Approaches: The best systems frequently incorporate a variety of strategies:

Combining techniques based on ML and signatures: Whereas machine learning manages unknown threats, signature-based detection effectively manages known threats.

---

[6] **Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E.** (2009). *Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges.* Computers & Security, 28(1-2), 18-28.

[7] **Sommer, R., & Paxson, V.** (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.* IEEE Symposium on Security and Privacy.

[8] **Mitchell, R., & Chen, I. R.** (2014). *A Survey of Intrusion Detection Techniques for Cyber-Physical Systems.* ACM Computing Surveys, 46(4), 1-29.

Ensemble approaches: Combining many machine learning models to increase overall accuracy and lessen the effect of individual model flaws.[9]

Discussion.

Techniques for Big Data Analytics:

In order to manage the enormous amount of network traffic data, effective data processing and analysis methods are needed:

Two distributed computing frameworks for handling big datasets are Hadoop and Spark.

NoSQL databases are made to manage semi-structured and unstructured data.

Processing data as it comes in real time is known as data stream processing.

Feature Engineering and Selection: The effectiveness of ML/DL models depends on effective feature engineering. This entails choosing pertinent criteria that accurately depict the characteristics of network traffic and can assist in differentiating between malicious and benign activity. Features might consist of:

Packet headers include protocols, ports, and source and destination IP addresses.

Content of the payload: (With strict privacy considerations)

Packet sequences between two hosts are known as network flows.

Features of time series: volume, frequency, and duration of traffic.

Metrics for Evaluation:

Comparing various approaches and guaranteeing system efficacy require accurate evaluation. Important metrics consist of:

Accuracy: The proportion of cases that are accurately categorised.

Precision: The percentage of assaults that were accurately detected out of all the instances that were reported as attacks.

Recall: The percentage of attacks that were accurately detected out of all real attacks.

The F1-score is the accuracy and recall harmonic mean.

The proportion of benign cases that are mistakenly labelled as assaults is known as the false positive rate.

The advantages and disadvantages of network access detection systems are given in the table below:

№	Name of IDS	Advantages	Disadvantages
1	SolarWinds Security Event Manager	Centralized logging and correlation of security events.	Can be resource-intensive and impact system performance.
		Real-time threat detection and response.	May require additional tuning for optimal use.
		Wide range of integration with other SolarWinds tools.	The free trial version may have limitations compared to the full product.
2	CrowdStrike Falcon Intelligence	Uses advanced AI to detect and respond to threats.	Costly, especially for large enterprises.
		Offers endpoint protection, threat intelligence, and incident response.	Limited visibility into network traffic compared to traditional IDS solutions.
		Lightweight agent with minimal impact on system performance.	Dependence on vendor-provided threat intelligence could be a drawback.

[9] **Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R.** (2017). *Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System.* IEEE International Symposium on Networks, Computers and Communications (ISNCC).

3	Snort	Open-source and highly customizable.	Performance can degrade with large traffic volumes.
		Wide community support and frequent updates.	Complex configuration and tuning required for optimal use.
		Effective at detecting known attack patterns and anomalies.	Lacks behavioral analysis capabilities.
4	Zeek (formerly Bro)	ocuses on analyzing network traffic to detect suspicious activity.	Steeper learning curve due to its scripting nature.
		Real-time event correlation and alerting.	Not as well-suited for traditional signature-based detection.
		Modular and extensible, allowing for custom scripts and plugins.	Limited integration with third-party security tools.
5	Suricata	High-performance, open-source IDS/IPS.	Complexity in tuning for optimal performance.
		Real-time packet processing and threat detection.	Resource-intensive, which can affect system performance.
		Active development community and frequent updates.	Limited detailed analysis for complex threats.
6	IBM QRadar	Comprehensive security information and event management (SIEM) platform.	Expensive, with high implementation costs.
		Good for large enterprise environments with extensive integration capabilities.	Performance can be affected by large data volumes.
		User-friendly interface and extensive reporting options.	Some users report difficulties with scalability and high false positive rates.
7	Security Onion	Free, open-source security monitoring and threat detection platform.	Can be complex to set up and configure.
		Includes IDS/IPS, network monitoring, and more.	Performance may not match commercial alternatives in high-traffic environments.
		Active community for support and contributions.	Lacks some advanced features available in paid solutions.
8	Open WIPS-NG	Open-source wireless intrusion detection system (WIDS).	Limited capabilities compared to commercial WIDS solutions.
		Monitors and analyzes wireless networks for anomalies and threats.	May require manual tuning for optimal performance.
		Relatively lightweight and easy to deploy.	Smaller community and less frequent updates compared to other IDS tools.
9	Sagan	Open-source, flexible and lightweight log monitoring tool.	Limited detailed analysis capabilities.
		Simple setup and configuration.	Not as mature as other log analysis tools like Splunk.
		Allows custom alerts and real-time event monitoring.	Limited integration with third-party security tools.
10	Splunk	Powerful data indexing and search capabilities.	Expensive, especially at scale.
		Real-time analytics and visualization.	Can require significant hardware resources.
		Strong integration with a wide range of data sources.	Steep learning curve for users without prior experience.

They can be classified depending on when and where they are used. The following table presents the results of the classification:

№	Name of IDS	When	Where
1	SolarWinds Security Event Manager	You manage multiple servers and services on a network and need centralized event monitoring.	Small to mid-sized organizations, especially if you already use the SolarWinds ecosystem.
2	CrowdStrike Falcon Intelligence	When you need to detect emerging threats, protect endpoints, and respond quickly.	In large enterprises, government organizations, and organizations that manage a large number of endpoints.
3	Snort	When you need to track attack signatures that require close detection.	In small networks or where inexpensive but effective network security monitoring is required.
4	Zeek (formerly Bro)	When you need to observe specific and deep network anomalies and analyze logs.	**Where** : Large network infrastructures, academic institutions, or wherever analytics-driven security strategies are needed.
5	Suricata	When you need to analyze high-speed network streams in real time.	In organizations that handle large volumes of traffic or where increased IDS/IPS performance is needed.
6	IBM QRadar	When comprehensive security monitoring is needed, a centralized SIEM system is required.	In large corporations, financial institutions, and organizations with complex security requirements.
7	Security Onion	When you need a free tool that combines comprehensive security monitoring, IDS, and log analysis.	Organizations with small budgets, testing environments, or professionals learning security analysis.
8	Open WIPS-NG	When you need to monitor the security of your wireless network and track errors.	In organizations with existing wireless infrastructure, such as educational institutions or cafes.
9	Sagan	When real-time monitoring and correlation of logs is required.	Where a lightweight and affordable tool is needed, especially in small and medium-sized organizations that perform log-based analysis.
10	Splunk	When you need to perform advanced analytics, log indexing, and real-time analysis.	Large organizations, financial services, and businesses that manage many types of data.
11	Machine Learning-based Detection	When you need to identify emerging threats, perform behavioral analysis, and automate security.	Large network infrastructures, organizations in the financial sector, companies working with IoT devices, or places where real-time analysis of large amounts of data is required.

The choice of which of these tools to choose depends on the size of the organization, security goals, infrastructure complexity, and budget. For example, larger enterprises can turn to tools like Splunk, IBM QRadar, or CrowdStrike, while smaller organizations can use free or open source tools like Snort, Security Onion, or Sagan. Machine learning- based solutions are used to detect and automate complex threats.

Conclusion.

These cutting-edge methods are becoming more and more important to modern network attack detection systems in order to increase their precision, flexibility, and capacity to identify complex and dynamic threats. Proactive and intelligent systems that can absorb information from previous attacks and adjust to novel attack tactics are becoming more and more important.[10]

To sum up, NIDS are essential to network security. They work best, though, when combined with

[10] **Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y.** (2013). *Intrusion Detection System: A Comprehensive Review.* Journal of Network and Computer Applications, 36(1), 16-24.

other security techniques and technologies in a layered security strategy. The particular requirements and features of the network should be taken into account while selecting an NIDS.

List of used literatures:

1. **Stallings, W.** (2020). *Network Security Essentials: Applications and Standards.* Pearson Education.
2. **Scarfone, K., & Mell, P.** (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).* National Institute of Standards and Technology (NIST).
3. **Zaynidinov H., Mallayev O.** *Parallel Algorithm for Calculating the Learning Processes of an Artificial Neural Network.* AIP Conference, 2022, 2647, 050006.
4. **Bace, R. G., & Mell, P.** (2001). *Intrusion Detection Systems.* NIST Special Publication 800-31.
5. **Northcutt, S., & Novak, J.** (2002). *Network Intrusion Detection.* Sams Publishing.
6. **Davis, J., & Magrath, S.** (2013). *A Survey of Network-Based Intrusion Detection Data Sets.*
7. **Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E.** (2009). *Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges.* Computers & Security, 28(1-2), 18-28.
8. **Sommer, R., & Paxson, V.** (2010). *Outside the Closed World: On Using Machine Learning for Network Intrusion Detection.* IEEE Symposium on Security and Privacy.
9. **Mitchell, R., & Chen, I. R.** (2014). *A Survey of Intrusion Detection Techniques for Cyber-Physical Systems.* ACM Computing Surveys, 46(4), 1-29.
10. **Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P. L., Iorkyase, E., Tachtatzis, C., & Atkinson, R.** (2017). *Threat Analysis of IoT Networks Using Artificial Neural Network Intrusion Detection System.* IEEE International Symposium on Networks, Computers and Communications (ISNCC).
11. **Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y.** (2013). *Intrusion Detection System: A Comprehensive Review.* Journal of Network and Computer Applications, 36(1), 16-24.