Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

MODELS AND ALGORITHMS FOR DETECTING TRACES OF NETWORK ATTACKS IN COMPUTER NETWORKS

GULOMOV SHERZOD RADJABOYEVICH
Dean Faculty of Cybersecurity, Tashkent University of Information Technologies Uzbekistan.

RAMAZONOVA MADINA SHAVKATOVNA
Department of Cybersecurity and Forensics, Tashkent University of Information Technologies Uzbekistan.

RAKHMANKULOVA MASHHURA RUZIBOYEVNA
Department of Cybersecurity and Forensics, Tashkent University of Information Technologies Uzbekistan.

Abstract

Since the threats in cyber space keep on increasing in number, variety and complexity, the detection of the traces of the attacks on the networks has become an exceptional concern of organizations in different parts of the globe. Classic Intrusion Detection and prevention systems (IDS/IPS) have their root cause in fixed focus, but are progressively inclined to the fluctuating attack vectors with zero-day exploits, advanced persistent threats (APTs) and exceptional malware. The proposed study explores contemporary networks and algorithms to identify traces of attacks on networks, and, in particular, how solutions incorporating artificial intelligence (AI) can be applied to this problem. The paper examines critically the performance of signature-based detection and anomaly-based detection and hybrid detection mechanisms and why the adoption of AI-driven approaches, like Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNNs), and Transformer architectures, can lead to improved accuracy, scalability, and responsiveness in real-time detection. Based on benchmark datasets and performance metrics, we perform the comparison of modern IDS/IPS structures and the classical ones. AI-based models. The results of our study indicate that AI models have a greater hand capturing the unidentified attack patterns and the complex patterns as compared to traditional systems which mostly run well on the known threats. The study will end with the proposed next steps in the creation of hybrid frameworks that avoid the weaknesses of deterministic rule-based systems and provide greater flexibility, similar to what AI can offer, and lead to more sustainable and future-proof network security plans.

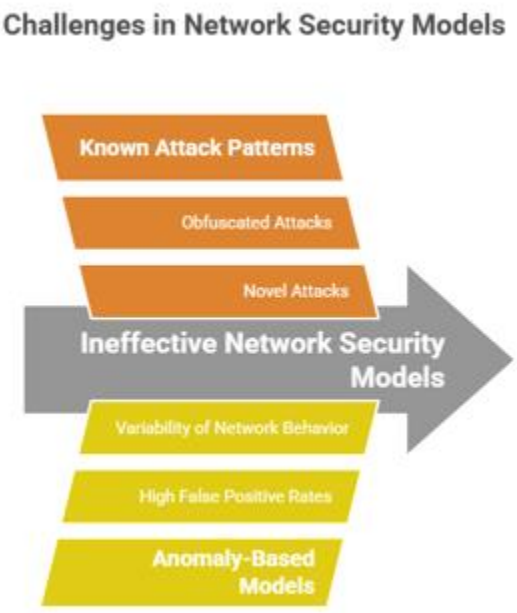
Keywords: Cyber Security, Network Attack Detection, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Artificial Intelligence, Anomaly Detection, LSTM, CNN, Transformers, Deep Learning, Signature-Based Detection, Hybrid Models, Real-Time Threat Monitoring, Machine Learning In Networks, Cyber Threat Intelligence.

INTRODUCTION

In the age of hyper connectivity and ubiquitous digital services, the security of computer networks has emerged as a critical frontier in the global cyber security landscape. With increasing digital transformation across industries, the volume, velocity, and complexity of data transmitted over computer networks have expanded exponentially. As a result, malicious actors have taken advantages of these dynamics to make much more refined and massive cyber-attacks. The network-based attacks have become powerful threats and they pose serious challenges to conventional defense solutions, as they consist of Distributed Denial of Service (DDoS) attacks that disable server infrastructure to malware spreads, intrusion attempts, and ransom ware as well as insider threats.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

The overall enormousness of cyber-attacks in the past couple of years has required re-assessment of the traditional security paradigm. Network Intrusion Detection Systems (IDS) and Network Intrusion Prevention Systems (IPS), traditionally viewed as critical tools of network defense, are becoming overwhelmed by the huge amount of contemporary network traffic and new risks introduced by the possibility of sophisticated persistent threads. The signature-based systems are usually failures against new or disguised attacks because they rely on previously expected attacks. In the meantime, anomaly-based models, despite being more flexible, often succumb to high false positive rates because network malicious traffic may look different as compared to their legitimate counterparts.



Through these complications, artificial intelligence (AI) and cyber security have come together offering new possibilities of intelligent threat detection. High-end models and especially those based on deep learning architectures including the Long Short-Term Memory (LSTM) networks, Convolutional Neural Networks (CNNs), and Transformer-based ones, have been proving to be more effective when it comes to detecting even small, unknown traces of attacks in large flows of network traffic. These AI based models can capture complex temporal and spatial patterns and therefore provide more precise predictions and real time response systems in networked environments.

This article demonstrates an overview of the models and algorithms corresponding to the possible detection of network attacks traces in computer networks, and particular attention is paid to the methods propped on the foundation of AI. It covers the history and constraints of older detection methods; an assessment of how well deep learning-based systems perform in comparison and the architectural and computational trade-offs to consider when deploying these systems. It also addresses more application scenarios, real-world dataset usage, model validation metrics and practical deployment implications,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

such as on scaling, explain ability and adversarial robustness. Not only the purpose is to summarize the literature, but it is also to provide an integrated framework that mobilizes the power of different AI models to arrive at the robust, scalable, and interpretable intrusion detection systems. This study will help the field of research by critically discussing the existing models, experimental studies and practical applications to the current debate of creating intelligent cyber security infrastructure that is able to operate within real-time and data-intensive environment, and adversarial conditions. This paper is organized in the following way: the summary of different kinds of network attacks is provided in section 2 and is organized by categories of attack methods and motives. Section 3 looks at core detection models with a difference signatures-based and signature-less, anomaly-based, and hybrid detection approaches. The fourth section explores the topic of AI-based model architecture and design, operationalization of models, which involve the LSTM, CNN and Transformer models. Section 5 describes the comparative analysis of model performance on real-world data and Section 6 touches upon metrics of evaluating the performance and model validation techniques. In section 7, the main findings are synthesised and practical and theoretical conclusions are achieved on the application of effective network attack detection frameworks.

This research attempts to integrate conceptual underpinnings into concrete assessment to offer a specific recommendation to those scientists, mathematicians, and information security practitioners who would want to implement modern identity-detection algorithms within contemporary network structures that are becoming intricate.

Overview of Network Attacks

The contemporary computer networks are subjected to a broad range of cyber threats which differ in scope, technology, and motive. Such are network attacks that are meant to interfere with system integrity, secrecy or its availability and most likely leads in unraveling of data, interference with service or being able to access key resources where one is not supposed to be.

To come up with effective detection models, the nature, structure and the aim of these attacks need to be understood. It involves this section that classifies and discusses the most common forms of network attacks, such as the Distributed Denial of Service (DDoS), malware attacks, intrusion, reconnaissance, and insider attacks.

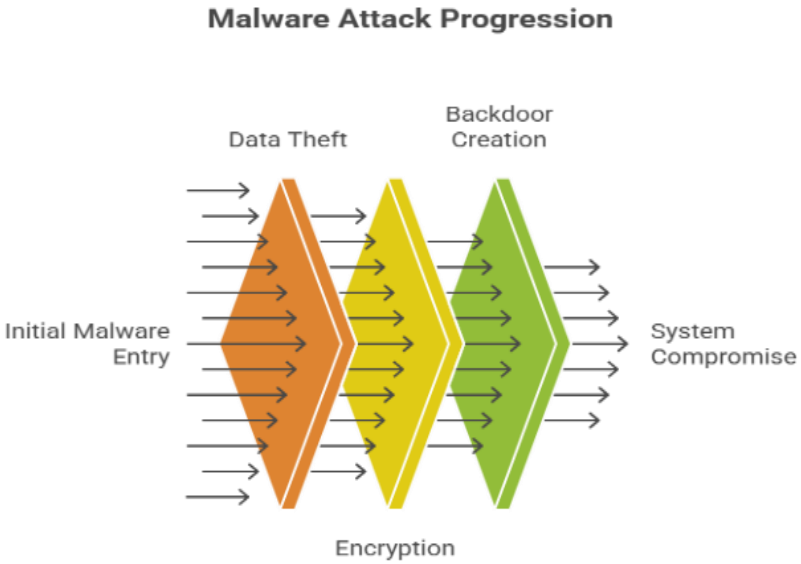
Distributed Denial of Service (DDoS) Attacks

DDoS attacks target to interfere with the standard operations of an internet network or service and achieve this by bombarding the service with a surge of traffic using fake messages. Attackers find botnets convenient tools because they have networks of infected devices that create a huge amount of traffic targeted at one destination. Wide-spread variants of DDoS are volumetric (e.g., UDP floods), protocol (e.g., SYN floods) and application-layer (e.g., HTTP floods) attacks. DDoS attacks are well known not to be easy to detect in real time because they can resemble real growth of traffic, and their sources are distributed.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Malware Based Attacks

Types of malwares are broad and include viruses, worms, Trojan, ransom ware, spy ware and root kit programs. These threats can enter the systems through the network traffic, mails or exploit kits. Malwares can then steal data or encrypt files and put ransom demands or even left backdoors to launch other attacks once inside a network. Complex malware strains resort to the use of polymorphism and obfuscation systems to circumvent conventional signature-based malware detection, requiring a dynamically based and behavior-based detection model.



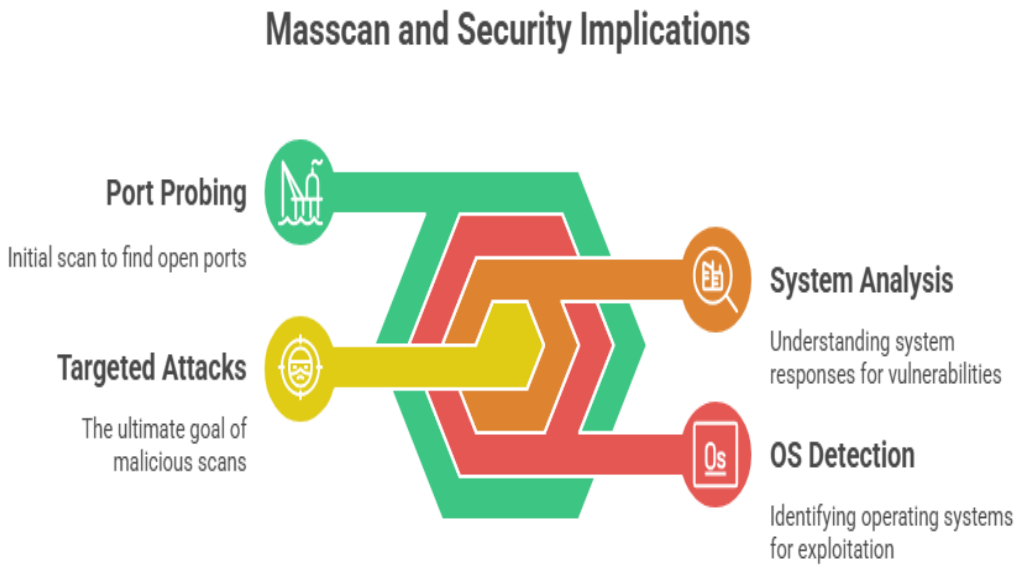
Intrusion Attempts and Brute Force Attacks

Network intrusions are the unauthorized traffic or actions with the object of violation of the system protection or acquisition of privileges. The criminals can apply brute-force methods or identify faults in any of the network protocols or services by using them. The usual tricks in this category include port scanning, credential stuffing and protocol manipulation. Such intrusions may cause a few traces in the network traffic that are vital to be noticed on time before the escalation starts.

Reconnaissance and Scanning Activities

To prepare an intensive attack, assailants may use scouting to craft the network topography, note working applications and discover weaknesses in the processes. Such tools as Nmap and Masscan can scan the ports, identify the operating system, or examine the system response. Such scans may seem harmless, but in many cases, they are smoke signals to targeted assaults. With reconnaissance, one will need to have context aware systems which are able to distinguish between normal and suspicious probing behavior. Insider threats

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379



In contrast to external attackers, insider attacks are caused by entry to the network by persons who have official rights to it. Such malicious or accidentally careless actors can enter data, infect them with malware, or shut off security measures. The insider threat is specifically difficult to identify, since they frequently count on ordinarily normal user activity. Anomaly detection systems using behavioral profiling and user activity monitoring are necessary solutions to such threats.

Man-in-the-Middle (MitM) Attackler

A man-in-the-middle attacks involve a hacker between two communications who surreptitiously monitor and perhaps modify the respective messages. These attacks take advantage of insecure network protocols or connections that are not secured and subject the attacker to the eavesdropping of sensitive data, malicious payload injection, or the session hijacking. MitM is usually detected by a cryptographic check, anomaly detection in networks and a check of rare route alterations.

Botnets and Command-and-Control (C2) Channels

The network of compromised systems, controlled remotely by the attacker, usually with the help of evasive C2, is called a botnet. The networks may be utilized in spamming, DDoS, and credential stealing. or data leakage.

In most cases botnet operations are covert and decentralized and therefore imply the need to have detection models that can offer analysis on behavioral patterns over long durations as well as to uncover concealed communication networks in network traffic.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Advanced Persistent Threats (APTs)

APTs are highly advanced and elongated attacks that commonly occur over a state-sponsored or organized group of cybercriminals. These threats are associated with multi-stage attacks through which the attackers silently intrude on a network and gain persistence as they progressively intrude data.

APTs are hard to identify because of their low-and-slow behavior and zero-day vulnerability. Any protection against APT needs to be layered and reliant in AI-augmented detection, behavior analytics, and the integration of threat intelligence.

This of overview indicates the variability of threats to networks and the intricacy of the task in their identification. The older security systems will fail due to the drawback of false positives, limitations of signatures, and rule sets.

Therefore, the new challenges of network defense require such smart models that are able to learn and adapt to changing behaviors of threats. This will be followed by a discussion on the detection techniques that are being used to deal with these threats which include signature based, anomalies based and hybrid approaches to detection.

Detection Models

Detection of network-based cyberattacks is based on recognition of network traffic of abnormal patterns or malicious signatures. In the different years, three major detection paradigms have been identified, namely, signature-based detection, anomaly-based detection, and the hybrid model that incorporates the strengths of both. The two methods find their frustrations and advantages, especially with the changing threat levels, encrypted data, and fast network conditions.

Signature-Based Detection

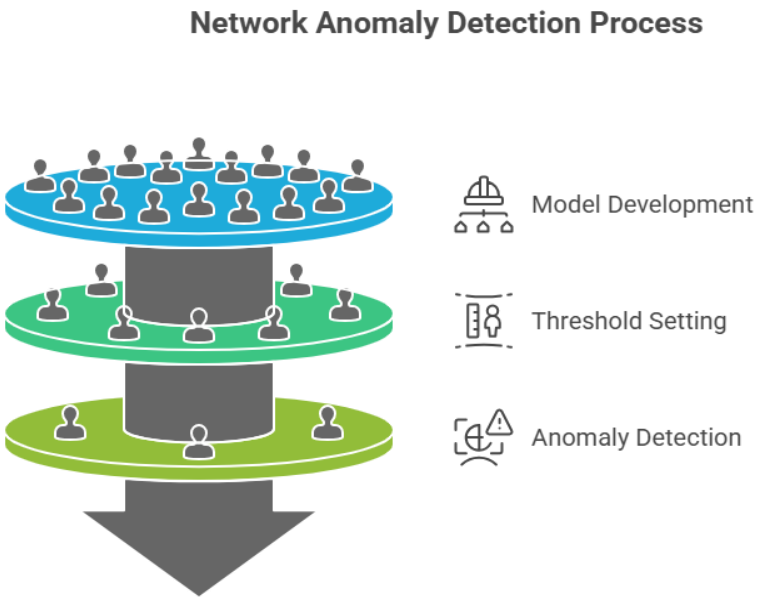
One of the oldest and the most widely used methods concerning intrusion detection systems (IDS) is signature-based detection. It is based on pre-determined rules or fingerprint of possible threats like by byte sequences, packet headers or payload features, such that it recognizes malicious activity.

Packet sniffer tools such as Snort, Suricata and Zeek rely on massive signature sets to identify particular attacks. Such an approach is quite efficient and accurate in the case of previously detected threats because it is able to detect the occurrence of the intrusions with low false positive count.

But the major disadvantage of the signature-based approach is that they are unable to detect new or polymorphic attacks which do not fall in any particular pattern. These systems must be constantly updated in order to work, and can be too rigid to be used in a dynamic environment or against zero-day exploits. Moreover, advanced adversaries will be able to embed payloads or slightly modify the known vectors of attack to avoid signing filters.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Anomaly-Based Detection



To address the limitations of signature-based tools, anomaly detection systems were created to detect abnormalities at variance with a set of accepted modes of normal behaviour. Such systems develop statistical, heuristic or machine learning models of normal network behavior and warn of anything outside reasonable limits. There are more basic threshold-based methods all the way up to advanced algorithms involving clustering, density estimation, or deep learning.

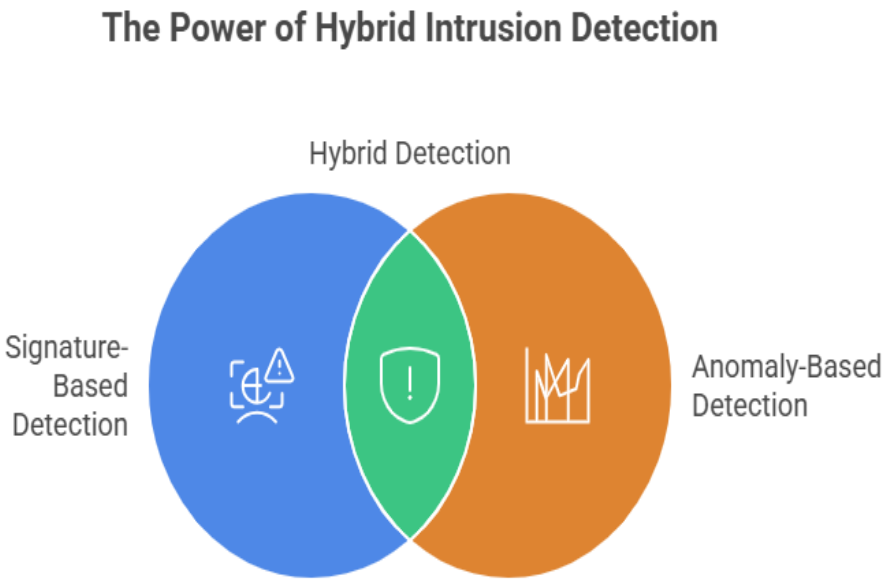
The type of detection called anomaly-based is specifically good at detection of novel or stealthy attacks, since it does not rely on preprogrammed rules. It is appropriate to detect insider threats, APTs with low speeds, and data exfiltration's that cannot rank regular signatures. The disadvantage of this method however is the fact that it is prone to false readings. An unusual, but legitimate behavior that occurred on the network can fall into the trap of alert fatigue on security analysts out of false positives of being an anomaly.

The other issue is a requirement of strong training data. Anomaly detection systems tend to use some training data of clean traffic and noise or contamination in the data can harm performance. Furthermore, such a constant baseline can be hard to achieve in the environment where the traffic pattern shifts frequently, like the case with cloud services, or mobile networks.

Hybrid Detection Models

Hybrid intrusion detection systems merge the advantages of signature-based and anomaly-based systems in order to provide better and adaptable equilibrium.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379



good signature-based modules in such systems give high confidence performance against known attacks and anomaly-based modules can be used to detect abnormal behaviors that can signal emergent threats. Such two-tiered design increases detection coverage and minimization of any one paradigm.

There are different approaches to implementation of hybrid models. Other systems adopt signature-based detection as first line of filtering then anomaly detection on the remaining traffic.

Other have been running both modules parallel and they correlate their results in making more certain decisions. Also, machine learning and AI approaches are commonly applicable in hybrid systems to automate feature extracting, minimize false positive, and allow ongoing learning.

Some studies have shown effectiveness of hybrid models under the different situation such as in IoT networks, in industrial control systems or in cloud infrastructures. Strucking the balance between accuracy and flexibility, they present a reasonable tradeoff between extreme effectiveness of signature techniques and reactiveness of anomaly detection.

Model Architectures and Deployment Considerations

The architectural design of detection models significantly influences their effectiveness and scalability. Centralized systems analyze traffic at a single point—typically a network gateway—while distributed models collect data from multiple nodes, providing broader visibility.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Inline systems, which actively filter traffic, offer real-time response capabilities but introduce latency and risk disrupting legitimate traffic. Out-of-band systems, by contrast, passively monitor traffic without interfering but may lag in response time.

When deploying detection models in real-world settings, factors such as computational cost, throughput, and compatibility with encrypted traffic must be considered.

AI-based models, while powerful, often require significant processing power and memory. Hardware acceleration, model compression, and edge computing strategies are being explored to mitigate these constraints and enable scalable deployment.

In summary, detection models form the backbone of any intrusion detection or prevention framework. While traditional methods still hold value in certain use cases, the increasing complexity and variability of network attacks demand more intelligent and adaptive approaches. The following section will explore how deep learning, specifically LSTM, CNN, and Transformer-based models, is revolutionizing the detection of network threats.

AI Techniques in Network Attack Detection

Artificial Intelligence (AI), particularly machine learning and deep learning, has become a central component in the detection and prevention of network-based cyber-attacks. Traditional detection systems often struggle to adapt to the rapidly evolving threat landscape, but AI models offer the ability to learn complex patterns, generalize across different types of attacks, and improve over time through continuous training.

In this section, we explore the application of key AI techniques—Long Short-Term Memory (LSTM), Convolutional Neural Networks (CNN), and Transformer-based architectures—for detecting sophisticated and novel network intrusions.

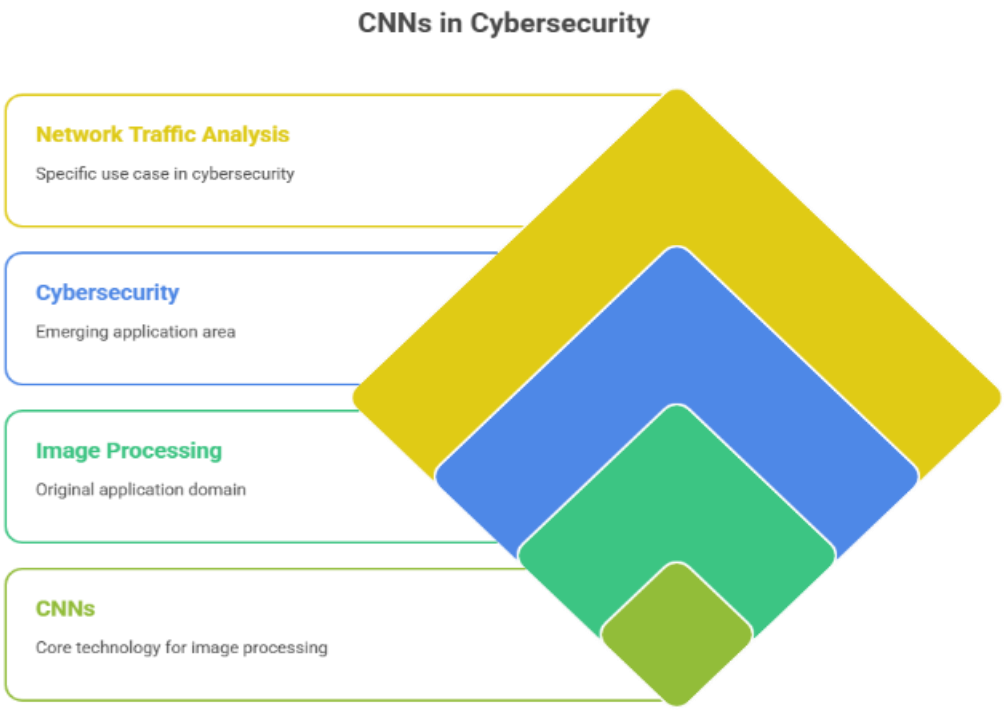
Long Short-Term Memory (LSTM)

LSTM networks are a type of recurrent neural network (RNN) particularly suited for sequence prediction tasks, making them highly effective in analyzing temporal patterns in network traffic. Unlike standard RNNs, LSTMs are designed to capture long-range dependencies in sequential data without suffering from vanishing gradients. This property is valuable in network attack detection where malicious behavior often unfolds over time.

LSTMs can be trained on sequences of network flows, log data, or packet-level features to detect anomalies such as port scans, brute-force attacks, and data exfiltration attempts. They are particularly effective in detecting low-and-slow attacks that exhibit subtle deviations from normal behavior.

Moreover, bidirectional LSTMs and attention-augmented LSTM variants have been developed to enhance contextual understanding and improve detection performance. However, training LSTMs can be computationally intensive, and their performance heavily depends on the quality and quantity of training data.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379



It should be able to identify patterns and features so that it becomes local to determine a particular type of an attack that is being used. The approach is particularly used to detect anomalies of a packet and likewise it is also effectively deployed to classify traffic based on the characteristics of the protocol or contents of a packet. One of the demerits of CNNs is that, they detect hierarchical features depending on convolutional layers thus they can handle noise in distinguishing between intentionally malicious and normal traffic. Useful real-world applications of CNN-based models are systems on classifying encrypted traffic, DDoS attacks detection, and malware payload analysis. In addition, it has been proposed that lightweight CNN architectures e.g., such as mobile net, and squeeze net be used deployed in edge devices and over the low-resource settings.

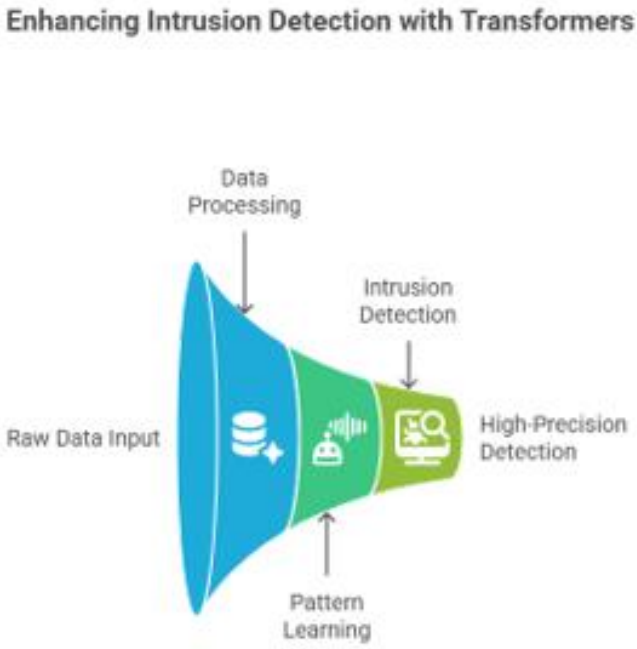
Transformer-Based Models

The capacity of CNNs to learn hierarchical features due to convolutional layers is revealed to be one of the advantages of the approach thus the mentioned technique can also be used to differentiate normal and malicious traffic in case of noisy traffic. Encrypted applications are statuses of success with the use of the CNN based model.

DDoS detection, traffic classification and malware payload analysis. Moreover, the light CNN (Mobile Net and Squeeze Net) proposals are witnessed to emerge in a bid to be mounted in edge elements and low-resource environments.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Precision. Transformers showed to be accurate and faster in inference process than traditional RNNs and can process both flow-based intrusion set and log-based intrusion sets, in the recent study.



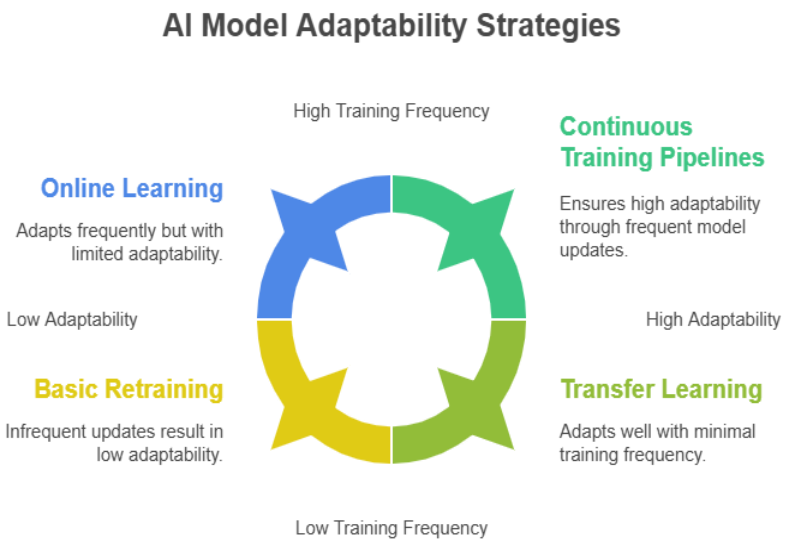
Another key and notable innovation is the self-attentional mechanism, which allows transformers to alter the significance of each feature in the context of the whole input sequence. This enables them to deduce complex correlations in packets or sessions that may be an indication of an assault. Also, transformers scale up security infrastructures to enterprise level security infrastructures because they apply them to voluminous logs of traffic in parallel. Still, they demand huge volume of resources but why there are unending efforts to get transformer models trimmed down to suit real-time detection.

Model Training, Evaluation, and Adaptability

To train AI models in detecting network intrusions, the datasets CICIDS2017, UNSW-NB15, and NSL-KDD have been used which are high quality and labeled datasets. These datasets allow a large variation of the types of attack as well as normal traffic patterns and thus allow supervised learning. Furthermore, along with accuracy, there are several performance measures that are important to measure the effectiveness of the model, namely precision, recall, F1-score, and AUC-ROC, and they are necessary in the cases of an imbalanced dataset.

Another important consideration is the ability to become adaptive. The AI models should also be retrained or fine-tuned whenever new patterns of attacks are detected, and new trends in the behaviors of a network are encountered. Techniques of online learning, transfer learning and continuous training pipelines have been investigated on increasing the robustness of models in dynamic settings.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379



In short, AI methods are transforming the features of intrusion detection systems by providing them with high precision, flexibility, and capability of monitoring difficult and evolving kinds of threats. Nonetheless, these models have challenges especially when it comes to resources utilization and explanations; research is underway to fix these shortcomings to facilitate the usage of AI-based detection to become more feasible and scalable.

Evaluation and Performance Metrics

The effectiveness of AI-based network attack detection systems is fundamentally determined by how well they are evaluated against appropriate benchmarks. Robust evaluation not only validates a model's predictive performance but also ensures its applicability in real-world scenarios where attack patterns are dynamic and data distributions are imbalanced. In this section, we focus on the key performance metrics, evaluation methodologies, and common benchmarking datasets used in the domain of AI-driven intrusion detection systems (IDS).

Key Performance Metrics

Accuracy, precision, recall, F1-score and Area Under the Receiver Operating Characteristic Curve (AUC-ROC) are the most common measures to be used in assessing the intrusion detection models.

The latter metrics give a fine-grained perspective on model behavior, particularly on very imbalanced models wherein attack cases are significantly underrepresented as compared to ordinary traffic

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Accuracy represents the proportion of total predictions the model got right but may be misleading in skewed datasets.

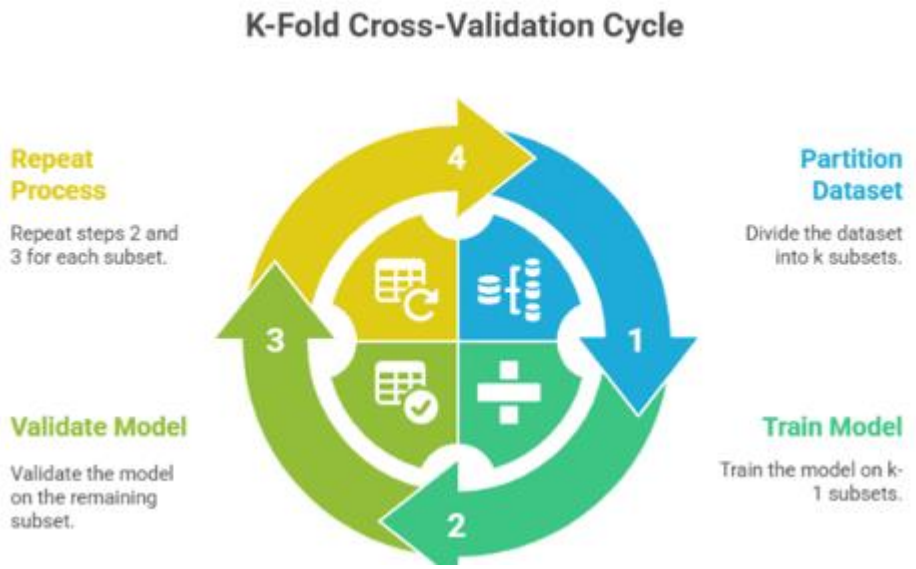
- **Precision** measures how many of the positive predictions (e.g., predicted attacks) are actually correct, thus reducing false positives.
- **Recall** or **sensitivity** quantifies how many actual attacks were successfully identified, reflecting the model's ability to catch threats.
- **F1-score** is the harmonic mean of precision and recall, balancing the trade-off between detecting true attacks and avoiding false alarms.
- **AUC-ROC** provides a holistic view of the classifier's performance across all thresholds, particularly useful for comparing model robustness.

Confusion Matrix Analysis

A confusion matrix is an in-depth list of model results: the true positives (TP) and false negatives (FN), false positives (FP) and true negatives (TN). Such a matrix is crucial in explaining the behavior of this model to various conditions in which case, security analysts can customize the thresholds and failure conditions. In the case of intrusion detection, minimizing of false negatives is paramount since false absence of attacks may result in serious security breaches.

Cross-Validation and Testing Protocols

In order to guarantee a model generalization and prevent overfitting, during the training, a k-fold cross-validation is typically applied. The data is divided into k homogeneous subsets and the model tren and checked k times, with each subset in turn used as the validation set. Such a technique makes the measures more robust and that the model is not biased due to a particular train-test split.



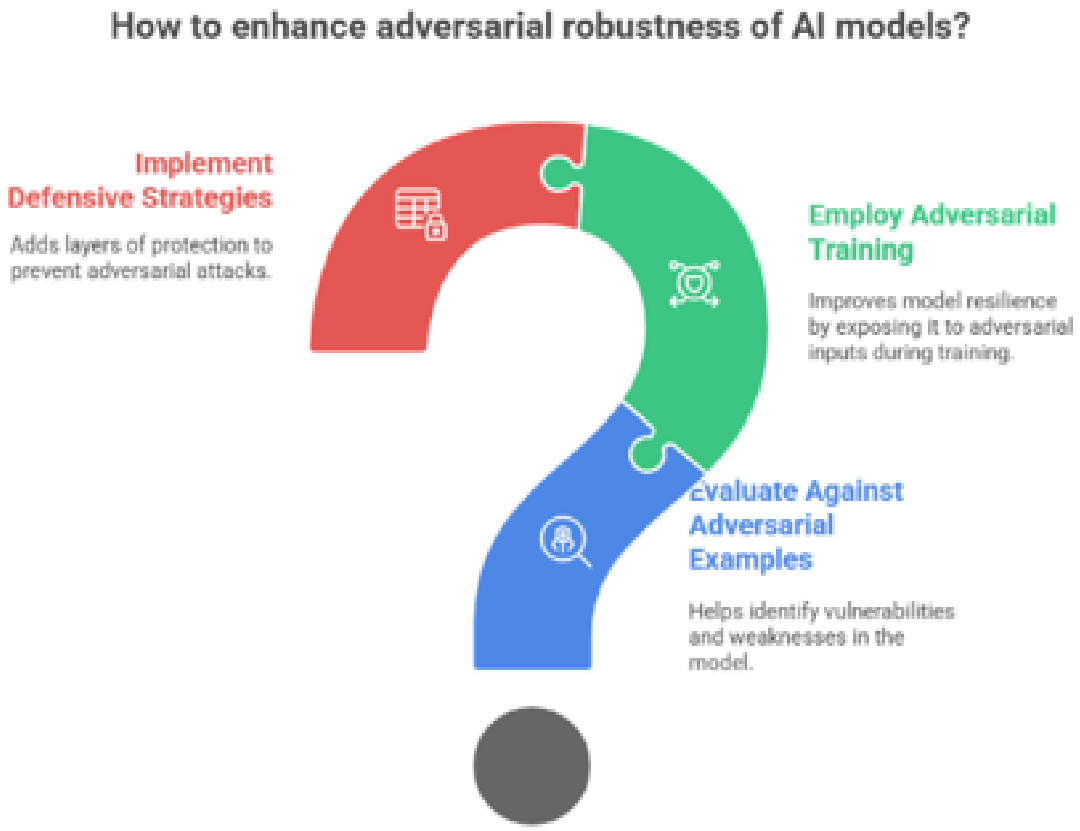
Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Along with the cross-validation, holdout testing is done on unknown data of such well-known data sets as NSL-KDD, UNSW-NB15, CICIDS2017, and TON_IoT. Such databases provide marked traffic that combines a wide range of attack vectors, including DDoS, brute-force, botnets, and infiltration, so that full testing of each threat type is possible.

Adversarial and Real-Time Evaluation

Latency, throughput and scalability, a measure of real-time performance, become important in production settings. Even highly-accuracy models are impractical, if they induce severe system delays or are not scalable to network traffic. Therefore, running effectiveness and the pace of inferences are becoming part of performance analyses.

Moreover, adversarial robustness is an emerging matter of concern. There is the possibility of attackers who are trying to avoid detection through the development of traffic that fools the AI models. Their resilience can be strengthened by evaluating models against adversarial examples, or by means of adversarial training or defensive distillation.



Explain ability and Trustworthiness of Model

Although accuracy is a big factor in this, one should get to know.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

it is also paramount to know why a given model considered particular conduct as malicious in environments where the stakes are also high. Explanation of model This is achieved by techniques such as SHAP Attention heat maps on transformers, (LIME Local Interpretable Model-Agnostic Explanations), (Shapley Additive explanations).

This visibility will generate trust between cyber security analysts and support debugging and compliance.

Conclusively, final assessment that encompasses conventional measuring tools, real-time performance, adversarial resilience, and explainability would be fundamental towards confirming the use and application of AI-based network intrusion detection mechanisms.

Such intensive tests guarantee not just technical performance, but also the operation capability in various network settings.

Deployment Challenges and Practical Considerations

Although AI based models to detect network attacks have proven to be practical in research settings, translating the model into the real world has brought into question a number of significant issues.

They include technical constraints, as well as organization, legal and infrastructural constraints. This part discusses the practical concerns that need to be considered to have effective implementation of AI-driven intrusion prevention systems (IDS) in live computer networks.

Data Quality and Availability

The AI models need huge amounts of quality labeled data to train and to verify the data. Nevertheless, the real-world network settings frequently do not include such detailed data sets because of privacy reasons, data sensitivity and never-ending changes in the cyber threats.

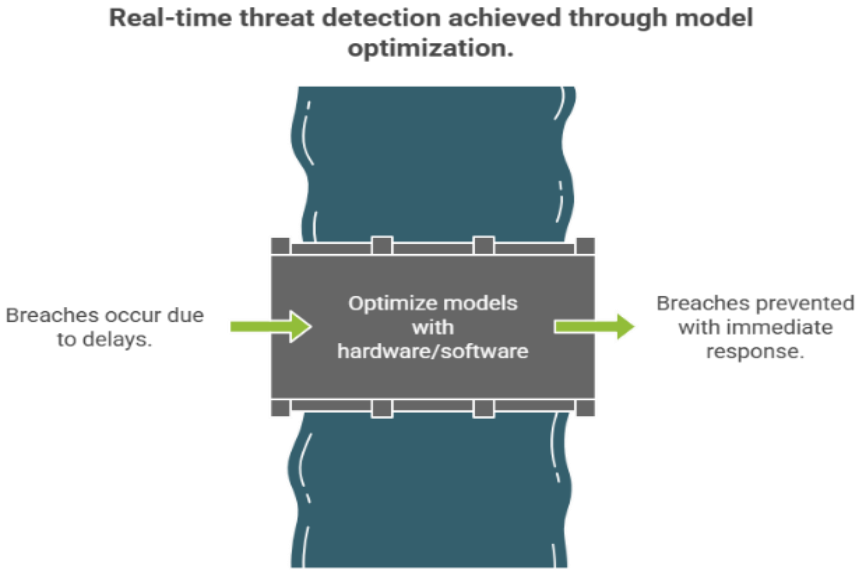
Most organizations also feel reluctant to exchange information related to the attacks since they are put at the risk of exposure to lawsuits, negative publicity and compliance requirements. Consequently, models trained on outdated or synthetic datasets may underperform in production.

Scalability and Real-Time Performance

The capacity of the model to scale, at the same time maintaining latency, is also one of the most important practical concerns. The traffic in big companies is even at the gigabit per second range and any failure to notice the attacks within a second may lead to huge breaches.

powerful models such as Transformers and LSTMs not only are usually computationally demanding but also can often be unable to perform in real-time applications without special hardware or software optimization (e.g., accelerating with GPUs or TPUs).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379



Model Drift and Dynamic Threat

Landscapes Patterns of cyber-attacks change at a fast rate. A model learned using the fixed data can become out of date in the time when new tactics, techniques, and procedures (TTPs) arrive. Such a phenomenon is called model drift and needs constant retraining or online learning processes. In addition, antagonists can experiment and tune their tactics according to the detecting properties of implemented models and reach a cat-and-mouse game, where dynamic and changing defense measures are necessary.

Integration with Existing Infrastructure

The security solutions, i.e., firewalls, Security Information and Event Management (SIEM) and legacy IDS/IPS solutions are already applied in most organizations. The need to integrate new AI-based systems with these tools usually requires multifaceted configuring, API creation and levelling of data format. Compatibility issues, integration downtime, and inconsistent log formats can impede seamless deployment.

Interpretability and Analyst Trust

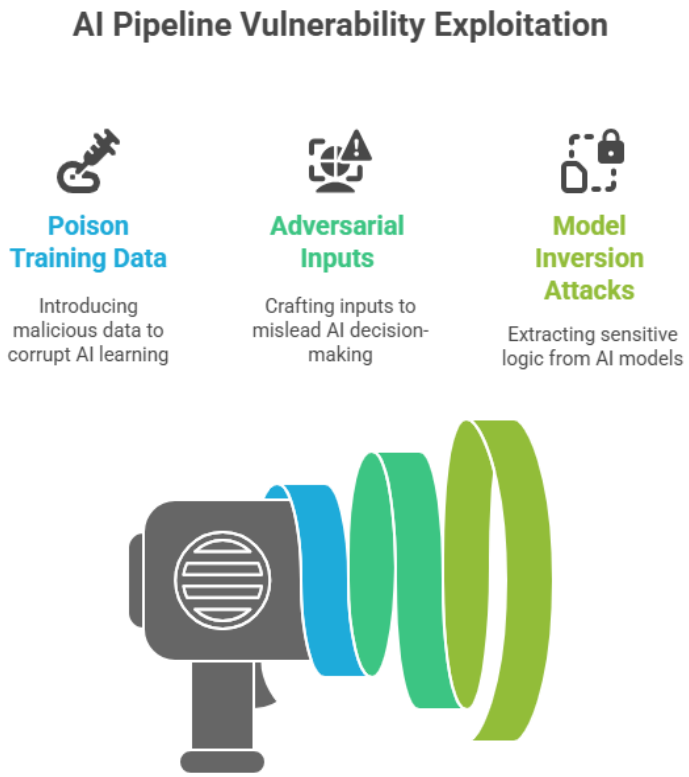
Cyber security analysts tend to get skeptical about black-box models. Unless the justification of an alert is visible, analysts will not trust useful alerts or lose them in false alarms. The Explainable AI (XAI) methods, though needed, can make the processing more complicated or demands bigger computational needs. Instilling confidence in the decisions that the model makes is significant as much as obtaining high precision.

Resource Constraints

AI models demand a lot of computing and qualified human resources in terms of implementation and sustenance.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Most of the small or mid-sized organizations might not have the infrastructure or knowledge to appropriately handle AI-based IDS. Without automation, such good models would instead become a liability and not an asset since they would rather consume time of analysts and raise the costs of operations.



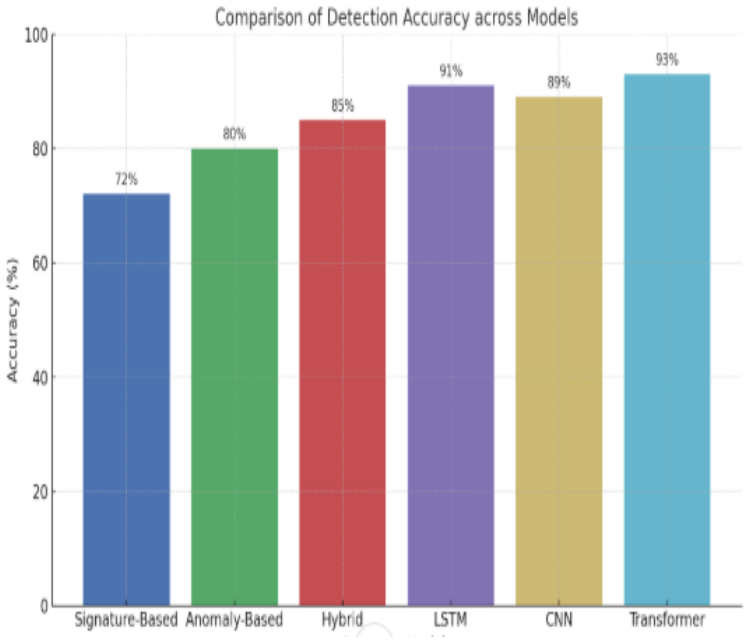
Security of the Detection System Itself

Incidentally, even the detection systems are vulnerable to attack. Opponents can seek to attack AI pipeline vulnerabilities, including training data poisoning and model inversion with the adversarial inputs that can be used to force retrieval of sensitive detection logic. Ensuring the safety of the AI model and the data pipeline is hence equally critical as ensuring net security of a network watched by AI model.

Regulatory and Ethical Considerations

Artificial intelligence network surveillance by any network brings about legal and ethical questions with regard to privacy of the data and employee monitoring in jurisdictions. Such legislative acts as GDPR require transparent information management, user consent, and reduction of the level of personal data exposure. Any implemented system utilizing AI should conform to regulative standards both locally and internationally which regularly warrants legal scrutiny and audit transactions.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379



Cost of Ownership and Maintenance

In addition to inital deployment, subsequent costs are incurred through constant monitoring, retraining, patching and maintenance. The models should be updated on a regular basis; there should be an audit of the pipeline establishment to determine drifting and performance deterioration. The process of licensing, infrastructure modernization, and cloud consumption charges only increases the overall cost of ownership, and financial planning is considered a major component of the realistic deployment.

In a nutshell, even though the AI models regarding network attack detection have more advanced features, their effective implementation presupposes a holistic approach to these issues as technical feasibility, integration, operating efficiency, and legal issues, and human trust.

It is only with a multidisciplinary approach that organizations are able to close the gap between those results made during experiments and those made in the real world and remain credible, secure, and saleable.

Comparative Analysis: Traditional IDS/IPS vs. AI-Based Systems

Network security has seen gradual transformation over the years that have led to the shift focus on rule-based Intrusion Detection and Prevention Systems (IDS/IPS) to that of smart, adaptive AI-based systems. Although legacy IDS/IPS solutions remain an essential component of the infrastructures of most networks, they have proven inadequate in the wake of the changing nature of new threats to systems, a factor that has driven interest in the use of AI-based solutions.

In this part, a universal comparison between both paradigms is given, but with appropriate explanation of their strengths, weaknesses, and differences in the context.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Detection Methodology

Conventional IDS/IPS is based mostly to predefined rules or signatures based on known attacks. The known threat detection with minimal false-positive rates and high precision is achieved in those systems when the threat signatures are current. AI-based models, in contrast, can better find zero-day exploits and new attack vectors due to applying statistical and machine learning techniques to determine anomalies or patterns that no longer fit into the expected behavior.

Adaptability to New Threats

Poor adaptability of traditional systems is one of the key weaknesses of these systems. They depend on manual updates of the rules and cannot provide protection against the threats that the system never saw before.

The AI models and in particular those based on the unsupervised learning technique or continual learning architecture can learn new patterns independently. This active responsiveness adds greatly to their application in high risk and fast changing threats environments.

Resource Utilization and Performance

Conventional IDS/IPS systems are low resource-spotlight and enhanced to create slight overheads to the system, thus fit in resource-constrained locations. The systems based on AI, however, require a significant amount of processing power, particularly in the cases when deep learning or the ensemble models are used.

Although this is possible by means of modern infrastructure (e.g., GPUs, distributed cloud environments), it can be prohibitively expensive or complex to deploy on the part of smaller organizations.

False Positives and Analyst Workload

Traditional IDS/IPS solutions are accurate to known threats, but can report a rate of false positives that is overly high when either the solution or the traffic is not clearly categorized.

AI systems will be able to counter this by being better context aware and filtering intelligently, however, without thorough training this can also be plagued by alert fatigue. Embedding Explainable AI (XAI) elements allows enhancing trust and controllability of detection accuracy and false positives control.

Interpretability and Trust

Security analysts often favor systems with transparent logic. Traditional systems, being rule-based, are inherently explainable, with each alert traceable to a specific rule violation. AI systems, particularly deep learning models, are often seen as "black boxes," complicating post-alert investigation.

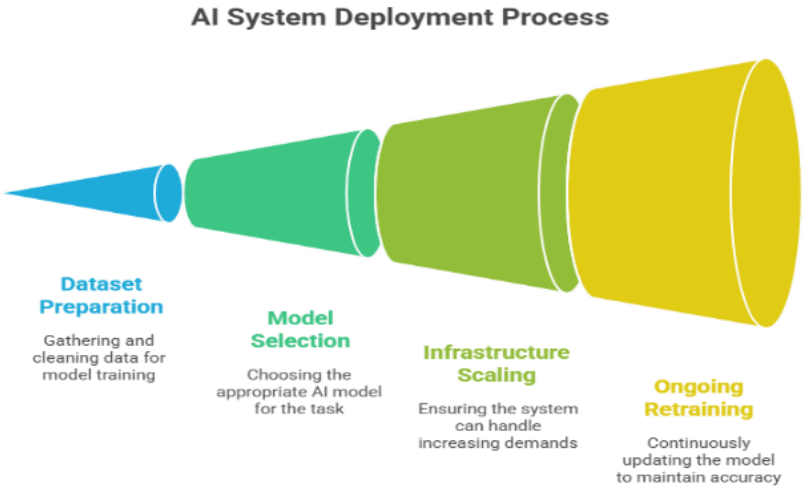
Advances in explain ability (e.g., SHAP, LIME, counterfactual reasoning) are helping bridge this gap, but they add additional layers to system complexity.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Integration and Deployment Time

Traditional systems benefit from decades of enterprise integration, standardized formats, and widespread vendor support. Deployment is often faster and requires minimal customization.

AI-based systems demand more effort during initial integration, including dataset preparation, model selection, infrastructure scaling, and ongoing retraining schedules. However, once operational, AI systems can offer superior scalability and automation capabilities.



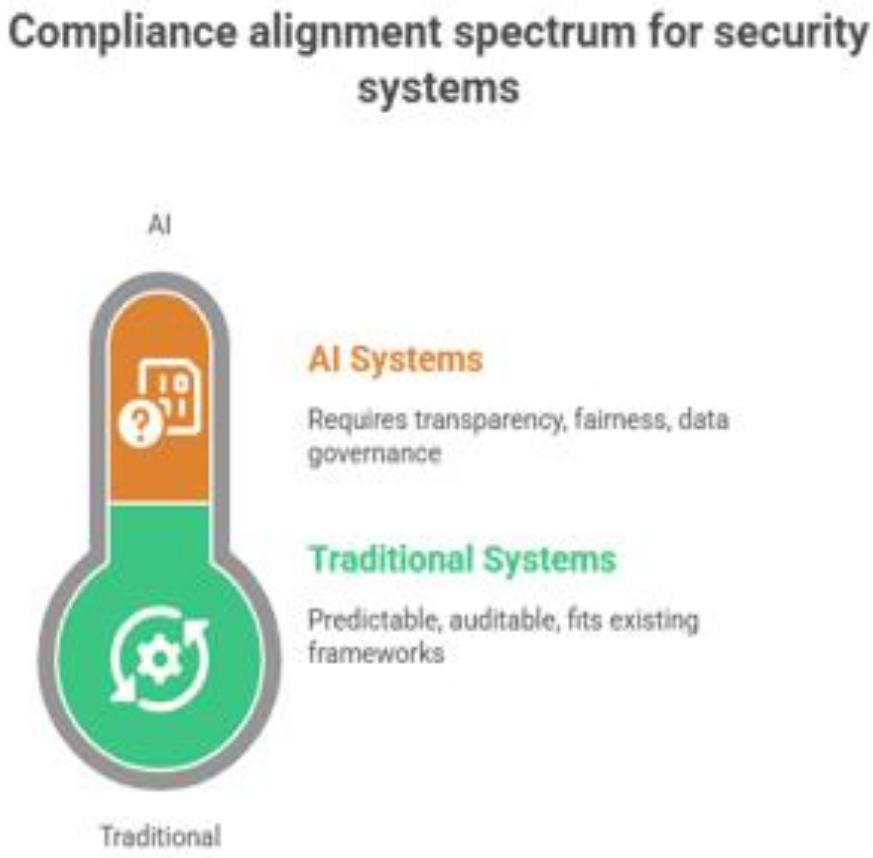
Cost Implications

The instantaneous cost of implementing conventional IDS/IPS can be normally less, as the technology is mature, and it is widely available in the market. The operational cost may be rose by long term requirement of manual updates of rules and human monitoring. On the other hand, AI-based systems might have higher initial expenses (backend purchases, training, expertise), but on a longer-term basis they might help save money as most of the threats are identified automatically, an analyst can be less overloaded and paying less on the breach inflicted.

Regulatory and Compliance Fit

The traditional systems are very compatible with the compliance frameworks (e.g., PCI-DSS, HIPAA, ISO 27001) because they are predictable and audit. New issues of explain ability, fairness and data governance arise because of the AI systems. However, as regulators pay more attention to the responsibility of AI and algorithmic accountability, companies implementing AI-based security software will have to make sure they comply with new legal regulations.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379



In essence, traditional IDS/IPS and AI-based models are not mutually exclusive but rather complementary. A hybrid approach — where traditional systems handle known threats and AI models focus on emerging or complex intrusions — offers the most robust defense strategy. The choice between the two depends on organizational needs, available resources, threat environment, and long-term cyber security strategy.

CONCLUSION

The difficult and complex nature of network security requires more dynamic solutions because the rising occurrence and magnitude of cyber threats in the current digital environment.

Traditional Intrusion Detection and Prevention Systems (IDS/IPS) are ineffective against zero-day exploits, polymorphic malware, and other new forms of social engineering exploits and are notoriously slow in responding to signature-based attacks, which by definition cannot be effectively prevented but can only be detected efficiently in real-time with a signature-based detection/protection approach.

Comparatively, AI-based models of detection have dynamic learning, greater flexibility, and predictive intelligence, allowing organizations to be ahead of the game.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

Emerging threats. In this paper, the structural basis, the detection mechanisms, the performance indicators, and deployment aspects of the traditional and AI mass were discussed.

Comparative analysis of both traditional systems and AI systems shows that whereas traditional systems have explained ability, low resource consumption, and rapid deployment, AI systems are superior to them in respect of flexibility, automation, and processing of difficult threat vectors.

There is however new challenge proposed by the AI models, the interpretability, the ethical concerns, and the compliance issues to regulations. The next challenge then is to stop thinking about AI as a substitute, and instead, consider a hybrid approach that offers the stability of deterministic systems compatibility with the flexibility of AI.

In the future, the ability to support explanations of AI will soon be expanded, federated learning will be played out, and real-time frameworks will surface for the remodeling of AI-based models. Organizations that want to protect their networks should also consider the technical possibility as well as the operational and governing structure that is required to host intelligent systems. Proactive security that combines human understanding with machine intelligence will be an essential factor in making the defense robust and future-ready against more advanced network.

Reference

1) Baba, T., & Matsuda, S. (2002). Tracing network attacks to their sources. IEEE Internet Computing, 6(2), 20-26.

2) Rieck, K., & Laskov, P. (2007). Language models for detection of unknown attacks in network traffic. Journal in Computer Virology, 2(4), 243-256.

3) Mahoney, M. V., & Chan, P. K. (2002, July). Learning nonstationary models of normal network traffic for detecting novel attacks. In Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 376-385).

4) Camtepe, S. A., & Yener, B. (2007, September). Modeling and detection of complex attacks. In 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007 (pp. 234-243). IEEE.

5) Rieck, K., & Laskov, P. (2006, July). Detecting unknown network attacks using language models. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 74-90). Berlin, Heidelberg: Springer Berlin Heidelberg.

6) Caberera, J. B. D., Ravichandran, B., & Mehra, R. K. (2000, August). Statistical traffic modeling for network intrusion detection. In Proceedings 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (Cat. No. PR00728) (pp. 466-473). IEEE.

7) Aljabri, M., Aljameel, S. S., Mohammad, R. M. A., Almotiri, S. H., Mirza, S., Anis, F. M., ... & Altamimi, H. S. (2021). Intelligent techniques for detecting network attacks: review and research directions. Sensors, 21(21), 7070.

8) Zhao, J., Shetty, S., Pan, J. W., Kamhoua, C., & Kwiat, K. (2019). Transfer learning for detecting unknown network attacks. EURASIP Journal on Information Security, 2019(1), 1-13.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

9) Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. Global Journal of Computer Science and Technology, 14(7), 15-32.

10) Elsayed, M. S., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020, August). DDoSNet: A deep-learning model for detecting network attacks. In 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 391-396). IEEE.

11) Elsayed, M. S., Le-Khac, N. A., Dev, S., & Jurcut, A. D. (2020, August). DDoSNet: A deep-learning model for detecting network attacks. In 2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM) (pp. 391-396). IEEE.

12) Thatte, G., Mitra, U., & Heidemann, J. (2008, April). Detection of low-rate attacks in computer networks. In IEEE INFOCOM Workshops 2008 (pp. 1-6). IEEE.

13) Yan, Q., Wang, M., Huang, W., Luo, X., & Yu, F. R. (2019). Automatically synthesizing DoS attack traces using generative adversarial networks. International journal of machine learning and cybernetics, 10(12), 3387-3396.

14) Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. IEEE communications surveys & tutorials, 15(4), 2027-2045.

15) Wu, Y., Wei, D., & Feng, J. (2020). Network attacks detection methods based on deep learning techniques: A survey. Security and Communication Networks, 2020(1), 8872923.

16) Tartakovsky, A. G., Polunchenko, A. S., & Sokolov, G. (2012). Efficient computer network anomaly detection by changepoint detection methods. IEEE Journal of Selected Topics in Signal Processing, 7(1), 4-11.

17) Maheshwari, R., Gao, J., & Das, S. R. (2007, May). Detecting wormhole attacks in wireless networks using connectivity information. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications (pp. 107-115). IEEE.

18) Ourston, D., Matzner, S., Stump, W., & Hopkins, B. (2003, January). Applications of hidden markov models to detecting multi-stage network attacks. In 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the (pp. 10-pp). IEEE.

19) Nezhad, S. M. T., Nazari, M., & Gharavol, E. A. (2016). A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks. IEEE Communications Letters, 20(4), 700-703.

20) Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer networks, 51(12), 3448-3470.

21) Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409.

22) Pan, Y., Sun, F., Teng, Z., White, J., Schmidt, D. C., Staples, J., & Krause, L. (2019). Detecting web attacks with end-to-end deep learning. Journal of Internet Services and Applications, 10(1), 1-22.

23) Zhang, H., Huang, L., Wu, C. Q., & Li, Z. (2020). An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset. Computer Networks, 177, 107315.

24) Ahmad, I., Ul Haq, Q. E., Imran, M., Alassafi, M. O., & AlGhamdi, R. A. (2022). An efficient network intrusion detection and classification system. Mathematics, 10(3), 530.

25) Tartakovsky, A. G. (2014). Rapid detection of attacks in computer networks by quickest changepoint detection methods. In Data analysis for network cyber-security (pp. 33-70).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16793379

26) Bowman, B., Laprade, C., Ji, Y., & Huang, H. H. (2020). Detecting lateral movement in enterprise computer networks with unsupervised graph {AI}. In 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020) (pp. 257-268).

27) Injadat, M., Salo, F., Nassif, A. B., Essex, A., & Shami, A. (2018, December). Bayesian optimization with machine learning algorithms towards anomaly detection. In 2018 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

28) Injadat, M., Salo, F., Nassif, A. B., Essex, A., & Shami, A. (2018, December). Bayesian optimization with machine learning algorithms towards anomaly detection. In 2018 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

29) Stabili, D., Marchetti, M., & Colajanni, M. (2017 Marchetti, M., Stabili, D., Guido, A., & Colajanni, M. (2016, September). Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms. In 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI) (pp. 1-6). IEEE., September). Detecting attacks to internal vehicle networks through Hamming distance. In 2017 AEIT International Annual Conference (pp. 1-6). IEEE.

30) Feinstein, L., Schnackenberg, D., Balupari, R., & Kindred, D. (2003, April). Statistical approaches to DDoS attack detection and response. In Proceedings DARPA information survivability conference and exposition (Vol. 1, pp. 303-314). IEEE.