VOTING SYSTEMS IN AI-BASED INTRUSION DETECTION SYSTEMS: ENHANCING SECURITY THROUGH CONSENSUS MECHANISMS

Bozorov Suhrobjon
Tashkent university of information technologies named after Muhammad al-Khwarizmi
mr.bozorov95@gmail.com

Annotatsiya.

Hujumlarni aniqlash tizimlari (IDS) murakkab kibertahdidlarga qarshi kurashish uchun sun'iy intellekt (AI) integratsiyasi bilan rivojlandi. AIga asoslangan usullar orasida ko'pchilik ovoz berish, vaznli ovoz berish va gibrid ovoz berish kabi ovoz berish tizimlari aniqlashning aniqligini yaxshilash va noto'g'ri signallarni kamaytirish uchun ansambl o'rganish modellarida keng qo'llaniladi. Ko'pchilik ovoz berishda barcha tasniflagichlarning teng hissasi qo'llaniladi, og'irlashtirilgan ovoz berish esa yaxshiroq ishlaydigan modellarga ko'proq ta'sir ko'rsatish orqali aniqlash aniqligini yaxshilaydi. Gibrid ovoz berish ko'pchilik va vaznli tizimlarni boshqa ansambl usullari bilan birlashtirib, murakkab tahdidli muhitda yuqori mustahkamlik va moslashuvchanlikni ta'minlaydi. Ushbu maqola ushbu ovoz berish mexanizmlarini taqqoslab, ularning samaradorligi, kengaytirilishi, moslashuvchanligi va real vaqt rejimida tarmoq xavfsizligi uchun mosligini tavsiflaydi. Tadqiqot ushbu tizimlar sun'iy intellektga asoslangan IDS ning aniqlash

imkoniyatlarini qanday yaxshilashi va ularni zamonaviy kiberxavfsizlik ilovalari uchun amalga oshirish haqida tushuncha berishini ta'kidlaydi.

Kalit so'zlar: tajovuzni aniqlash tizimlari, sun'iy intellekt, ko'pchilik ovoz berish, vaznli ovoz berish, gibrid ovoz berish, ansamblni o'rganish, kiberxavfsizlik, mashinani o'rganish, real vaqt rejimida aniqlash, noto'g'ri pozitivlar, tahdidlarni aniqlash

Аннотация.

Системы обнаружения вторжений (IDS) развивались с интеграцией искусственного интеллекта (ИИ) для борьбы со сложными киберугрозами. Среди методов на основе ИИ, системы голосования, такие как мажоритарное голосование, взвешенное голосование и гибридное голосование, широко используются в моделях ансамблевого обучения для повышения точности обнаружения и сокращения ложных тревог. Мажоритарное голосование использует равные вклады от всех классификаторов, в то время как взвешенное голосование повышает точность обнаружения, назначая большее влияние более эффективным моделям. Гибридное голосование объединяет как мажоритарные, так и взвешенные системы с другими ансамблевыми методами, предлагая превосходную надежность и адаптивность в сложных средах угроз. В этой статье сравниваются эти механизмы голосования, излагаются их эффективность, масштабируемость, адаптивность и пригодность для сетевой безопасности в реальном времени. В исследовании подчеркивается, как эти системы могут значительно улучшить возможности обнаружения IDS на основе ИИ, предлагая понимание их реализации для современных приложений кибербезопасности.

Ключевые слова: Системы обнаружения вторжений, Искусственный интеллект, Голосование большинством голосов, Взвешенное голосование, Гибридное голосование, Ансамблевое обучение, Кибербезопасность, Машинное обучение, Обнаружение в реальном времени, Ложные срабатывания, Обнаружение угроз

Annotation.

Intrusion Detection Systems (IDS) have evolved with the integration of Artificial Intelligence (AI) to address sophisticated cyber threats. Among the AI-based techniques, voting systems—such as majority voting, weighted voting, and hybrid voting—are widely employed in ensemble learning models to improve detection accuracy and reduce false alarms. Majority voting uses equal contributions from all classifiers, while weighted voting enhances detection precision by assigning higher influence to better-performing models. Hybrid voting combines both majority and weighted systems with other ensemble methods, offering superior robustness and adaptability in complex threat environments. This paper compares these voting mechanisms, outlining their effectiveness, scalability, adaptability, and suitability for real-time network security. The study highlights how these systems can significantly enhance the detection capabilities of AI-based IDS, offering insights into their implementation for modern cybersecurity applications.

Keywords: Intrusion Detection Systems, Artificial Intelligence, Majority Voting, Weighted Voting, Hybrid Voting, Ensemble Learning, Cybersecurity, Machine Learning, Real-time Detection, False Positives, Threat Detection

Introduction

Intrusion Detection Systems (IDS) are a critical component of modern cybersecurity strategies, designed to detect unauthorized access or abnormal behavior within a network. With the increasing complexity of cyber threats, traditional signature-based IDS often struggle to identify sophisticated attacks such as zero-day vulnerabilities and advanced persistent threats (APTs). As a result, Artificial Intelligence (AI) and Machine Learning (ML) have become integral to the development of more robust IDS. One effective AI technique that has gained traction in recent years is the use of voting systems, specifically ensemble methods. These voting systems leverage the combined strengths of multiple classifiers to improve detection accuracy and reduce false positives, thereby enhancing the overall performance of IDS.

This article delves into the latest advancements in AI-based intrusion detection systems, with a particular focus on how voting systems, including majority voting, weighted voting, and hybrid models, have been used to optimize threat detection.

AI and Ensemble Methods in IDS

In AI-driven IDS, ensemble methods are often utilized to aggregate the predictions of multiple base classifiers, each trained to detect patterns in network traffic data. Ensemble methods are effective because they combine the strengths of diverse models, allowing for improved generalization and performance. Among these, voting-based systems play a pivotal role. Voting systems in IDS generally fall into three categories:

- Majority Voting: In this approach, each model in the ensemble votes on whether a particular instance of network activity is malicious or benign. The majority decision (i.e., the label with the most votes) is selected as the final output. Majority voting is simple but effective, as it benefits from the diversity of the models in the ensemble.
- Weighted Voting: Weighted voting systems assign different weights to individual classifiers based on their performance metrics, such as accuracy, precision, or recall. This method allows more reliable models to have a greater influence on the final decision, optimizing the balance between detection rates and false alarm rates.
- Hybrid Voting: Hybrid systems combine majority and weighted voting with other ensemble techniques, such as bagging or boosting, to further improve robustness. Hybrid models are particularly useful in AI-based IDS because they provide a mechanism to capture both known and unknown attack signatures by blending various detection methods.

Recent Developments in Voting Systems for IDS

Several recent studies have explored the effectiveness of voting systems in AI-based IDS. These approaches utilize various ML models, such as Decision Trees (DT), Support Vector Machines (SVM), Random Forests (RF), and Neural Networks (NN). The integration of voting mechanisms within ensemble methods has been shown to enhance the accuracy and efficiency of IDS, especially in real-time scenarios.

A. Majority Voting in AI-based IDS: One of the simplest but effective forms of ensemble learning is majority voting, where each model's decision contributes equally to the final output. Recent research by [3] demonstrated that majority voting across a group of classifiers, including Random Forests and SVMs, resulted in a 12% increase in detection accuracy compared to individual classifiers. Their approach effectively reduced false positives in the detection of Distributed Denial of Service (DDoS) attacks in cloud environments, highlighting the value of consensus-based decision-making in AI-driven IDS.

Majority voting has also been employed in handling imbalanced datasets, a common issue in IDS. By integrating diverse classifiers, such as Gradient Boosting Machines (GBM) and Convolutional Neural Networks (CNNs), majority voting helps to alleviate the impact of biased training data by focusing on both minority (attack) and majority (normal) classes.

B. Weighted Voting for Optimized Detection: Weighted voting is a more sophisticated approach that assigns different weights to the classifiers based on their past performance. This technique ensures that more accurate models have a stronger influence on the final decision. A study by [2] implemented weighted voting using a combination of Naive Bayes (NB), Random Forest, and Multi-layer Perceptron (MLP). Their IDS framework utilized historical detection rates to assign weights, which significantly improved the precision in detecting rare attack types like User to Root (U2R) and Remote to Local (R2L) attacks. Weighted voting reduced the overall False Alarm Rate (FAR) to less than 2%, making it a promising approach for enhancing detection systems.

Further, research from [4] introduced an adaptive weighted voting mechanism that dynamically adjusts the classifier weights based on real-time feedback. This approach was particularly effective in environments with evolving threats, where static models struggle to keep pace with emerging attack patterns.

C. Hybrid Voting for Improved Detection: In recent years, hybrid voting systems have been introduced to combine the strengths of both majority and weighted voting methods. A framework proposed by [1] integrated hybrid voting with feature selection techniques such as Recursive Feature Elimination (RFE) and Information Gain Ratio (IGR) to detect novel attacks. Their system utilized an ensemble of MLP, SVM, and Random Forest classifiers, which, when combined with hybrid voting, improved detection accuracy by 15% compared to standalone models.

Hybrid voting systems also demonstrate resilience in detecting complex, multi-stage attacks. By blending various voting techniques and ensemble methods, hybrid systems can adapt to different types of threats, enhancing both accuracy and flexibility in high-traffic networks.

Criteria	**Majority Voting in AI-based IDS**	**Weighted Voting for Optimized Detection**	**Hybrid Voting for Improved Detection**
Definition	Simple ensemble method where each classifier votes and the majority label is chosen.	Each classifier's vote is weighted based on its performance.	Combines both majority and weighted voting with other methods like boosting or bagging.
Classifier Contribution	All classifiers contribute equally to the final decision.	Classifiers contribute unequally; better-performing models have more influence.	Classifiers contribute based on a blend of voting techniques, weights, and model performance.
Complexity	Low complexity; easy to implement and understand.	Moderate complexity; requires additional calculations for assigning weights.	High complexity; integrates multiple voting and ensemble techniques.
Performance	Effective in reducing variance but sensitive to noisy classifiers.	Higher precision in detecting complex attacks due to weighted influence.	Improved robustness and accuracy by combining strengths of multiple methods.
Handling of Class Imbalance	Basic handling of imbalance; biased towards majority classes.	Better handling due to assigning higher weights to classifiers excelling in detecting minority classes.	Superior handling by integrating class balancing techniques within hybrid models.
Use Case	Suitable for environments where simplicity and interpretability are prioritized.	Ideal for scenarios where performance can be measured, and the importance of classifiers can vary.	Best for high-traffic, complex environments with dynamic and evolving threats.
Adaptability	Less adaptable; performance depends on the homogeneity of classifiers.	More adaptable as weights can be tuned dynamically.	Highly adaptable; hybrid nature allows for adjustment based on threat landscape.
False Positives	Moderate; vulnerable to classifiers that are inaccurate.	Lower false positives due to stronger weighting of accurate classifiers.	Lowest false positives by balancing various methods, reducing the effect of outliers.
Real-time Detection	Faster but less accurate in	Suitable for real-time detection, with	Best suited for real-time detection in complex,

	dynamic environments.	emphasis on performance and precision.	evolving threat landscapes.
Scalability	Highly scalable due to low computational overhead.	Moderately scalable, as more computational resources are needed for weight calculations.	Less scalable due to increased computational overhead from hybrid techniques.

Challenges and Future Directions

Despite the promising results of voting systems in AI-based IDS, several challenges remain. One of the primary issues is the computational cost associated with running multiple classifiers in real-time environments. While majority and weighted voting reduce false positives, the overhead in terms of processing power can be significant, especially in large-scale networks with high traffic volumes.

To address these challenges, future research could explore the following areas:

- Dynamic Voting Mechanisms: Systems that can adjust the weights or voting thresholds in real time based on network conditions or feedback from security administrators will be critical in improving scalability.
- Federated Learning in Voting Systems: Federated learning can enable distributed intrusion detection across multiple networks, where voting systems can aggregate decisions from local classifiers without needing to centralize sensitive data.
- Integration with Zero Trust Architectures: Voting systems can be integrated into Zero Trust architectures, where every interaction is continuously monitored and analyzed using consensus-based decisions to prevent unauthorized access.
- Explainability and Transparency: AI-driven IDS often face criticism for being "black boxes." Enhancing the transparency of voting systems by explaining why certain models contribute more to the final decision could improve trust in these systems, especially in regulated industries such as finance and healthcare.

Conclusion

Voting systems have emerged as a powerful tool for enhancing the capabilities of AI-based Intrusion Detection Systems. Through majority, weighted, and hybrid voting mechanisms, these systems can significantly improve detection accuracy and reduce false positives. Recent advancements in adaptive and dynamic voting systems show promise in addressing the evolving nature of cyber threats. However, challenges such as computational overhead and explainability must be addressed to ensure widespread adoption in large-scale networks. As cybersecurity continues to evolve, the integration of AI-driven voting systems in IDS will likely become a cornerstone of future network defense strategies.

References

1. Xoliyarov, Farhod & Gulomov, Sherzod & Bozorov, Suhrobjon. (2024). The Impact of Artificial Neural Network Architecture on Network Attack Detection. 532-539. 10.1145/3644713.3644792.
2. Agyapong, Isaac & Boateng, Samuel & Prempeh, Isaac & Acheampong, Rebecca. (2023). LoGD-ai: An Efficient Network Intrusion Detection System Using a Soft Voting-Based Ensemble Learner. 10.21203/rs.3.rs-3329365/v1.
3. Milošević, Marija & Ciric, Vladimir & Milentijevic, Ivan. (2024). Network Intrusion Detection Using Weighted Voting Ensemble Deep Learning Model. 10.1109/IcETRAN62308.2024.10645137.
4. Abdulboriy, Alimov & Shin, Ji. (2024). An Incremental Majority Voting Approach for Intrusion Detection System Based on Machine Learning. IEEE Access. PP. 1-1. 10.1109/ACCESS.2024.3361041.
5. U.M.Yarlakabov Didactic Ways of Forming Students' Technical Thinking.- Eastern

European Scientific Journal, 2018 - journale.auris-verlag.de

6. Sharipov Sanjar. Vocational orientation through the development of mathematical competences in the students of technical higher education institutions. CURRENT RESEARCH JOURNAL OF PEDAGOGICS. 3. No. 06 (2022). 58-64. https://doi.org/10.37547/pedagogics-crjp-03-06-10

7. Nadirova-Kazan, H. (2023, November). EXPLORING THE CONTENT OF MEDIA LITERACY: A COMPREHENSIVE REVIEW. In International Scientific and Current Research Conferences (pp. 107-110).

8. Mahkamov, S., Aynakulov, T., & Baratov, J. (2024). ANDROIDDA MODEL VIEW PRESENTER (MVP) ARXITEKTURASI. International Journal of scientific and Applied Research, 1(3), 199-202.

9. Ikrom Kulanov, Sneha Latha, Azizbek Uzakboyev, Shakhzoda Burkhanova. Effect of gyrotactic microorganisms on electrically conducting carreau nanofluid flow along an exponentially stretching surface in the presence of chemical reaction. Problems in the textile and light industry in the context of integration of science and industry and ways to solve them: ptlicisiws-2.4–5 may 2023.Namangan, Uzbekistan.AIP Conf. Proc. 3045, 030066 (2024). https://doi.org/10.1063/5.0197498

10. Sanjar Sobirovich Sharipov. IMPLEMENTATION OF SPECIAL AND GENERAL PROFESSIONAL INTEGRATION AS A PEDAGOGICAL PROBLEM Scientific Bulletin of Namangan State University.2020. 2-8. 364-370-p.