The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2023

Volume 23, Pages 262-268

ICRETS 2023: International Conference on Research in Engineering, Technology and Science

Enhancing Cybersecurity with Trust-Based Machine Learning: A Defense against DDoS and Packet Suppression Attacks

Adnan Ahmed
Quaid-e-Awam University of Engineering, Science and Technology

Muhammad Awais
Quaid-e-Awam University of Engineering, Science and Technology

Mohammad Siraj
King Saud University

Muhammad Umar
Quaid-e-Awam University of Engineering, Science and Technology

Abstract: As technology becomes more intertwined with our daily lives, it is increasingly important to protect our data from attackers. Cyber security has become a top priority for individuals, businesses, and governments, as the threat of cybercrime is constantly evolving and becoming more sophisticated. With the rapid increase in cyberattacks, it has become tricky and cumbersome for cybersecurity experts to react to them all, predict new attacks and analyze the impact of damage being done to business. Traditional security measures such as firewalls, anti-virus software, and intrusion detections are no longer adequate in protecting against new vulnerabilities, especially insider and misbehavior attacks. Recently, Artificial Intelligence based techniques have brought tremendous improvements in cybersecurity with the integration of machine learning (ML) algorithms. ML methods have been built upon large volumes of real-time network data to deploy automated security and threat detection systems. Nonetheless, various cyber-attacks still circumvent traditional security mechanisms deployed to detect those attacks. To address the challenge, in this paper, we propose a machine learning-enabled trust-based routing protocol (TrustML-RP) that identifies the attacking nodes responsible for Distributed Denial of Service (DDoS) and packet suppression attacks. The proposed TrustML-RP scheme first adopts a distributed trust model for establishing trust factor among the participating nodes and later employs an effective combination of ML algorithms e.g., Artificial Neural Network (ANN) and Support Vector Machine (SVM) to find an optimal and secure route and identify attacker nodes. A comprehensive performance evaluation of the proposed scheme is carried out to demonstrate the efficiency on a reasonably sized network containing mixed nodes. The results demonstrate the effectiveness of the proposed scheme in building a trusted network environment and improving network security. The research findings suggest that the integration of a trust-based model and ML techniques can improve traditional cybersecurity methods thereby enabling cybersecurity professionals to design more effective cybersecurity systems.

Keywords: Cyber security, Machine learning, Trust-based routing, Cyber-attacks, DDoS, Packet suppression attack

Introduction

The advancement in the internet, information and communication technologies have demonstrated significant progress in various fields such as internet-of-things, cloud computing, e-government, e-commerce, e-banking, cloud computing and smart cities. Such advancement and improved networking technologies also facilitated the

evolution of more sophisticated hacking techniques and tools, thereby allowing cyber-criminals to carry out more complex and advanced cyber-attacks (Awais Rajput et al., 2022; Malaivongs et al., 2022). Due to ever-increasing data breaches, it has become tricky and cumbersome for cybersecurity experts to react to them all, predict new attacks and analyze the impact of damage being done to business. Despite the effectiveness of traditional security methods, they often exhibit vulnerabilities to mitigate attacks such as Distributed Denial of Service (DDoS), flooding, insider threats, node misbehavior and packet suppression attacks, which can cripple an organization's network infrastructure (Cheema et al., 2022). Trust-based schemes have demonstrated significant advantages while mitigating such attacks by monitoring the traffic flows and developing the degree of trustworthiness between network devices (Shafi et al., 2023; Zeng et al., 2022). However, the existing trust-based schemes lack the ability to handle the volume and complexity of network traffic data generated by distributed devices. This has created a pressing need for AI and machine learning (ML) techniques to detect attacks and provide robust cybersecurity defense systems (Hasan et al., 2023). AI and ML techniques have been paramount in building automated security systems, automatically learning from the network traffic data, adapting to new attack patterns and threat detection by examining the huge amount of data in real-time (Zhang et al., 2022).

In this paper, we have proposed an enhanced cybersecurity scheme, TrustML-RP, that integrates the trust-based method with ML techniques in routing decisions to counter node misbehavior and Distributed Denial of Service (DDoS) cyber-attacks. The DDoS attack overwhelms a targeted network or computer by flooding a huge amount of traffic (might be fake traffic) from multiple sources. TrustML-RP aims to counter TCP SYN flooding, UDP flooding and ICMP flooding attacks. Moreover, the proposed scheme also mitigates the node misbehavior attack in which a normal participating node switches its behavior to a malicious node. A brief description of these attacks is provided below:

TCP SYN attack: An attacker sends a large number of TCP SYN packets to a target machine that doesn't allow a three-way handshake, leaving the target machine to wait for a response that never comes. Consequently, system resources are tied up and become unavailable to authorized users.

UDP flood attack: Unlike the TCP SYN attack, the UDP flood attack doesn't require a three-way handshake, and overwhelms the target machine with the massive amount of UDP traffic.

ICMP flood attack: An attacker sends a storm of ICMP packets, called *Pings*, to the victim machine, and causes the system to be overloaded with ICMP packets, which results in denial of service or degraded performance.

Packet Suppression attack: It's a type of routing attack in which an attacker node sends the fake route response packet to the source node and announces them as the most suitable candidate to forward packets to the destination device. However, after receiving the packets, either it drops selective packets or all received packets to create transmission disruption and denial of service (Grover et al., 2011).

To counter these attacks, the TrustML-RP scheme employs a trust-based machine learning methodology that can help in building trust in machine learning-based cybersecurity systems. This methodology involves identifying the types of DDoS and packet suppression attacks, defining trust-based metrics, collecting training data, training the machine learning model, integrating the model into the system, and evaluating the performance of the system.

The main contribution of this paper is twofold: (i) trust-based routing scheme to establish trustworthiness among the participating devices (nodes). The proposed TrustML-RP scheme incorporates the trust factor and route discovery mechanisms from our previous work (Ahmed et al., 2015). (ii) integration of ML techniques such as ANN and SVM to detect the attacker nodes. Based on the detection, attacker nodes are isolated from the active routes for packet transmission.

The rest of the paper is organized as follows: Section 2 provides a literature review of the existing research. Section 3 describes the methodology of the proposed TrustML-RP scheme. Section 4 presents the results and finally, Section 5 summarizes the research findings.

Related Work

The authors in (Zahra et al.2022) proposed a machine learning based schemes called, multiclass machine-learning-based model leveraging the light gradient boosting machines (MC-MLGBM), for detecting Rank and

wormhole attacks in the network. The dataset is generate using the Cooja network simulator which models the both static and mobile networks. The performance of proposed scheme in validated using multiclass-specific metrics such as cross-entropy, Cohn's kappa, and Matthews Correlation Coefficient (MCC). A distributed IDS scheme is presented (Ercan et al., 2022) for vehicular area networks to detect position falsification attack. the features used to detect position falsification attacks are estimated distance between sender and receiver, the difference between the declared and estimated distance between sender and receiver and estimated angle of arrival. The distance between sender and receiver is measured using Received Signal Strength (RSS) method. The posed scheme is implemented using KNN, RF and ensemble learning based ML methods. The OMNET++ and SUMO simulators have been used for simulating the vehicular network and generating VeReMi dataset that consist of 5 different attacks and 3 attacker rates 10%, 20% and 30% for various traffic densities (van der Heijden et al., 2018). A machine learning based routing scheme is proposed by (Luong et al., 2019) to detect and prevent flooding attacks. The proposed scheme Flooding Attack Prevention Routing Protocol (FAPRP) scheme is based n kNN ML method which uses route discovery frequency vector for feature selection such as route discovery time and inter-route discovery time. The NS2 simulator has been use to build and train the dataset. The kNN classifier is used to organize the nodes into two class vector Normal Vector Class (NVC) and Malicious Vector Class (MVC).

Proposed Scheme

In this section, the working mechanism of the proposed TrustML-RP scheme is presented to counter DDoS and node misbehavior attacks. The methodology is comprised of two phases. The first phase is responsible for establishing trust among the nodes in an ad-hoc network using distributed trust model. TrustML-RP incorporates the trust model from our previous work (Ahmed et al., 2015), however, a brief description of trust estimation is provided in the subsequent subsection. Whereas, the second phase is responsible for using ML techniques ANN and SVM to find possible routes and detect attacker nodes in the network based on the provided dataset.

Trust Estimation

The trust estimation factor is based on the packet forwarding behavior of a node. To estimate the trustworthiness of nodes, a methodology can be followed that involves collecting evidence, calculating trust values, setting a threshold, identifying trusted and misbehaving nodes, taking appropriate action, and updating trust values. The evidence is collected based on observing the packet forwarding behavior of a node by monitoring the traffic patterns that indicate potential attacks. Based on the collected evidence, the trust level of a node is calculated. If a node correctly forwards the packets to the intended destination, its trust rating is increased. Conversely, if it behaves abnormally and drops the packets instead of forwarding them to the destination its trust rating is decreased. The trust values fall within the range of [0,1] and a threshold value of 0.5 is used to differentiate between the normal (trusted) and attacker (misbehaving) nodes. The nods whose trust value fall below the threshold is considered malicious node while the nodes having trust values above the threshold are considered normal nodes. Appropriate action can then be taken against misbehaving nodes, such as isolating or blocking them, or deploying additional security measures to prevent further attacks. It is important to continue monitoring and updating trust values based on node behavior to maintain an accurate and up-to-date assessment of node trustworthiness.

Machine Learning Model

Following the trust estimation, the labelled data is prepared for training of the ML models. This involves checking and removing any null values, removing redundancy, and fixing structural errors. Relevant features from the dataset are selected based on the attack type. A feature mapping step then captures the input ranges in a suitable space for training purpose. The dataset is divided into train and test data by a ration of 70:30 to get around overfitting. The workflow of proposed scheme is shown in Figure 1.

An artificial neural network (ANN) and a support vector machine (SVM) model are fit to the train data. The ML model's parameters are provided in Table 1. The trained models are exported and integrated into the system by deploying it at the network edge to process incoming traffic in real-time. The model should generate a trust score for each incoming packet and use it to make decisions about forwarding or dropping the packet. The

performance of the trust-based machine learning scheme is evaluated by measuring its accuracy, F1-score, and processing time.

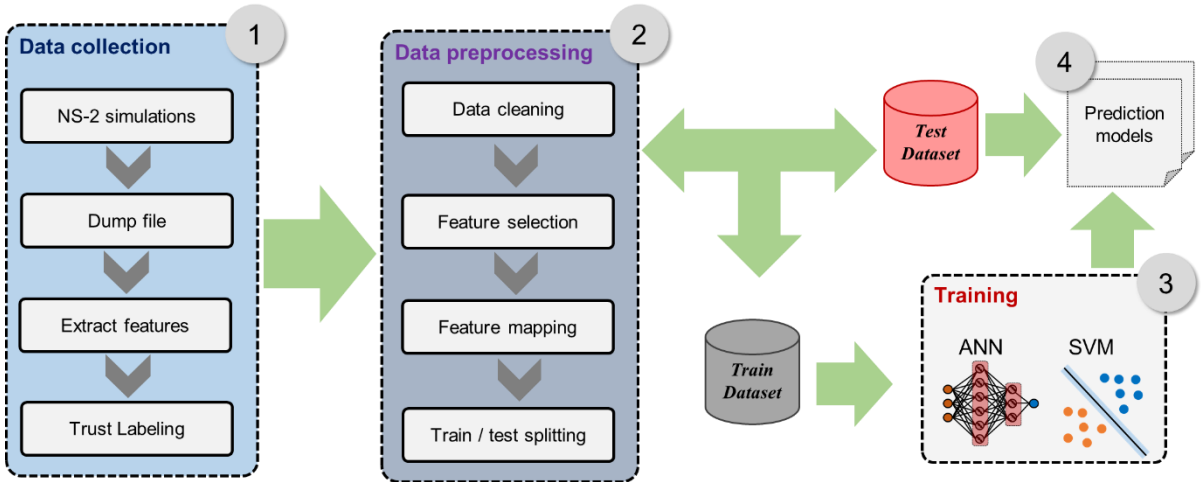

Figure 1. Trust-ML workflow

Table 1. Parameters of Ml Models

Algorithm	Parameter configuration
ANN	epochs=100 batch_size=64 activation=relu optimizer=adam
SVM	Gamma=0.1 C=1000

Results and Discussion

The proposed scheme is evaluated on the test dataset and the results are presented in this section mainly for accuracy and training time. The NS-2 simulator has ben used to simulate the network of 300 nodes, where the nodes are randomly deployed in an area of 100m x 100m. The attacker nodes are also randomly deployed which model the behavior of packet suppression and DDoS attacks (TCP-SYN, UDP and ICMP flood).

Figure 2 visualizes the accuracy score of the trained models i.e., the SVM and ANN classifiers on the test data for the three attack types (TCP-SYN attack, UDP and ICMP flood attacks). Overall, the SVM classifier outperforms the ANN by reaching up to 91% accuracy (in case of UDP attack). ANN's maximum accuracy score remained 71% for TCP_SYN attack types. We believe that this might be caused by mainly two factors: size of the dataset and the architecture of the ANN which was kept simple for the sake of training complexity. However, when sufficient training data and time is available, ANN's performance could be greatly improved.

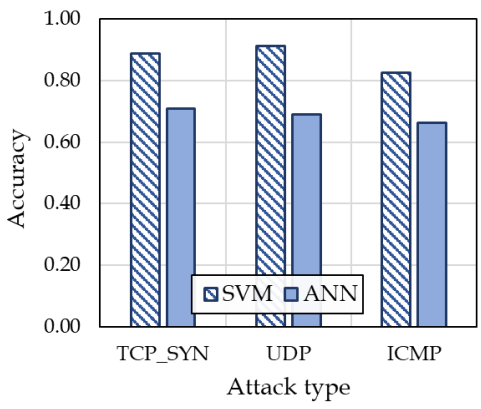

Figure 2. Accuracy of ML methods

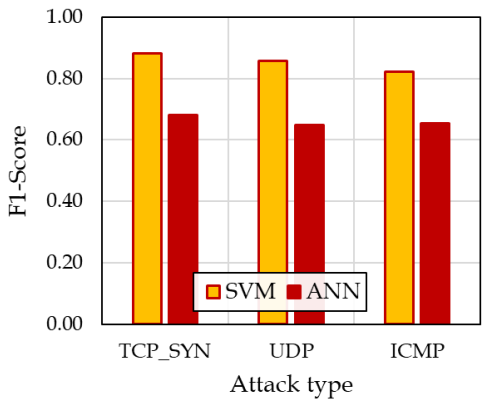

Figure 3. F1-score of ML methods

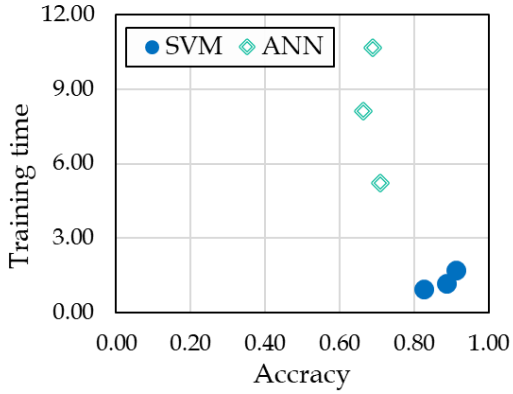

Figure 4. Accuracy vs. Training time for TCP_SYN attack

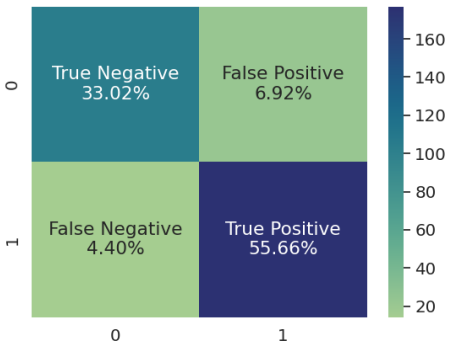

Figure 5. Confusion matrix for the SVM classifier for TCP_SYN attack

In Figure 3, we show the F1-socre of the ML methods. Here, again a similar trend is to be observed and SMV classifier obtains way better F1-scores as compared to the ANN. In our case, we plot a comparison showing a tradeoff curve for training times and accuracy in Figure 4. In this case it is clearly seen that the ANN classifier tends to occupy the center part of the graph whereas the points on the lower right corner are more favorable points which represent higher accuracy and lower training times. The training times of both classifiers are detailed in Table 2. Finally, in Figure 5 a confusion matrix for the TCP_SYN attack is shown for the SVM classifier showing a distribution of predictions made by the classifier.

Table 2. Training time for ML algorithms

Algorithm	Training time (s)	
	SVM	ANN
TCP_SYN	1.19	5.21
UDP	1.72	10.64
ICMP	0.96	8.12

Overall, the experimental results demonstrated that the ML methods are greatly capable of capturing the behavior of the malicious nodes in a real-time network environment. Particularly, we evaluated SVM and ANN classifier to differentiate normal and malicious nodes. The SVM classifier in this case showed superior performance for the test dataset. This enables the proposed TrustML-RP scheme to make more informed decision regarding the trusted and malicious nodes and isolate them from the active routes thereby leads to the selection of trusted routes. Consequently, results in the improved network performance as compared to existing schemes, in terms of the throughput and end-to-end delay as shown in the Figures 6 and 7. The various number of malicious nodes are randomly deployed in the network of 300 nodes. The design of TrustML-RP centered upon integration of trust and AI methods, thereby significantly minimizes the impact of misbehaving nodes and outperform their counterpart schemes.

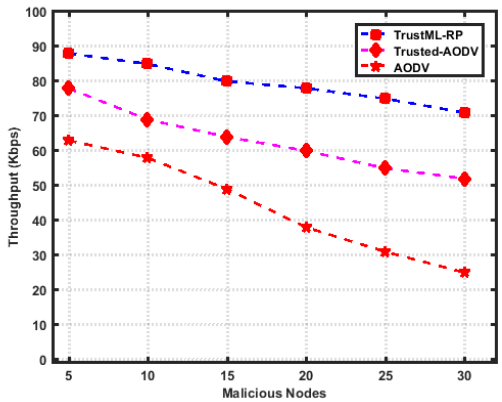

Figure 6. Throughput performance

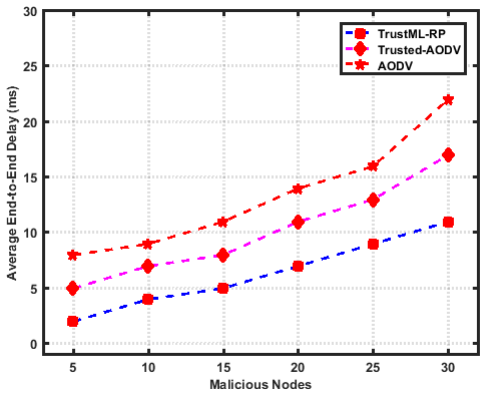

Figure 7. End-to-End delay performance

Conclusion

This paper presented a TrustML-RP scheme to counter packet suppression and DDoS attacks such as TCP-SYN attack, UDP and ICMP flooding attacks. The TrustML-RP scheme integrates the concept of trust and ML methods (ANN and SVM) to improve the attack resilience capability of cybersecurity scheme. The presented results depicted that the proposed TrustML-RP scheme efficiently detected the malicious nodes with better accuracy, isolated them from the active routes, paved the way for trusted network environment and improved the level of network security. Furthermore, the result finding also suggested that traditional cybersecurity mechanism can become more effective with the integration of AI-based machine learning techniques thereby enables cybersecurity professional to deploy automated security and threat detection system.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors

Acknowledgement

* This article was presented as an oral presentation at the International Conference on Research in Engineering, Technology and Science (www.icrets.net) held in Budapest/Hungary on July 06-09, 2023.

*This work was supported by Pakistan Science Foundation (PSF) via grant number PSF/P&D/TG-ND (882)/2023.

References

Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A trust and energy aware routing protocol for wireless sensor network. *IEEE Sensors Journal*, *15*(12), 6962–6972.

Awais Rajput, M., Umar, M., Ahmed, A., Raza Bhangwar, A., Suhail Memon, K., & Misbah, A. (2022). Evaluation of machine learning based network attack detection. *Sukkur IBA Journal of Emerging Technologies*, *5*(2), 58–66.

Cheema, A., Tariq, M., Hafiz, A., Khan, M. M., Ahmad, F., & Anwar, M. (2022). Prevention techniques against distributed denial of service attacks in heterogeneous networks: A systematic review. *Hindawi Security and Communication Networks*.

Ercan, S., Ayaida, M., & Messai, N. (2022). Misbehavior detection for position falsification attacks in VANETs using machine learning. *IEEE Access*, *10*, 1893–1904.

Grover, J., Prajapati, N. K., Laxmi, V., & Gaur, M. S. (2011). Machine learning approach for multiple misbehavior detection in VANET (pp.644-653). *International Conference on Advances in Computing and Communications.* Springer.

Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of Network and Computer Applications*,*209.*

Luong, N. T., Vo, T. T., & Hoang, D. (2019). FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks. *Wireless Communications and Mobile Computing*.

Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber trust index: A framework for rating and improving cybersecurity performance. *Applied Sciences*, *12*(21).

Shafi, S., Mounika, S., & Velliangiri, S. (2023). Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. *Procedia Computer Science*, *218*, 2309–2318.

van der Heijden, R. W., Lukaseder, T., & Kargl, F. (2018). VeReMi: A dataset for comparable evaluation of misbehavior detection in VANETs. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *254*, 318–337.

Zahra, F., Jhanjhi, N. Z., Brohi, S. N., Khan, N. A., Masud, M., & AlZain, M. A. (2022). Rank and wormhole attack detection model for RPL-based internet of things using machine learning. *Sensors*, *22*(18), 6765. https://doi.org/10.3390/s22186765

Zeng, P., Liu, A., Zhu, C., Wang, T., & Zhang, S. (2022). Trust-based multi-agent imitation learning for green edge computing in smart cities. *IEEE Transactions on Green Communications and Networking*, *6*(3), 1635–1648.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, *55*(2), 1029–1053.

Author Information

Adnan Ahmed
Quaid-e-Awam University of Engineering, Science and Technology,
Nawabshah, Pakistan.
Contact e-mail: adnan.ahmed03@quest.edu.pk

Mohammad Siraj
King Saud University
Riyadh, Saudi Arabia

Muhammad Awais
Quaid-e-Awam University of Engineering, Science and Technology
Nawabshah,, Pakistan

Muhammad Umar
Quaid-e-Awam University of Engineering, Science and Technology,
Nawabshah, Pakistan.

To cite this article:

Ahmed, A., Awais, M., Siraj, M., & Umar, M. (2023). Enhancing cybersecurity with trust-based machine learning: A defense against DDoS and packet suppression attacks. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 23*, 262-268.