INTERNATIONAL JOURNAL OF DATA SCIENCE AND MACHINE LEARNING (ISSN: 2692-5141)
Volume 03, Issue 01, 2023
Published Date: - 04-01-2023

ENHANCING SECURITY IN MOBILE AD HOC NETWORKS: INTRUSION DETECTION WITH SVM AND ANT COLONY OPTIMIZATION

Raman Kumar
Department of Computer Science Engineering, Gnanamani College of Technology, India

Abstract

Mobile Ad Hoc Networks (MANETs) are dynamic and self-configuring wireless networks, making them vulnerable to various security threats, including intrusion attempts. Intrusion detection systems (IDS) play a critical role in safeguarding MANETs against unauthorized access and malicious activities. In this study, we propose an innovative approach to enhance the security of MANETs through intrusion detection, leveraging the power of Support Vector Machines (SVM) with Ant Colony Optimization (ACO). Our approach harnesses the robustness of SVM in pattern recognition and classification, while ACO optimizes the SVM parameters, improving the accuracy and efficiency of intrusion detection. Through extensive experiments and evaluations, we demonstrate the effectiveness of this combined approach in mitigating intrusion threats in MANETs.

Key Words

Mobile Ad Hoc Networks (MANETs); Intrusion Detection; Support Vector Machine (SVM); Ant Colony Optimization (ACO); Network Security; Intrusion Detection Systems (IDS); Wireless Networks.

INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have emerged as a versatile and dynamic paradigm for wireless communication, enabling seamless connectivity in scenarios where traditional infrastructure-based networks are impractical or unavailable. These self-configuring networks, comprising mobile devices that can communicate directly with each other, are deployed in various domains, including military operations, emergency response, vehicular communication, and more. However, the unique characteristics of MANETs, such as their decentralized nature, limited resources, and dynamic topology, render them susceptible to a multitude of security threats, including intrusion attempts, data breaches, and denial-of-service attacks.

Intrusion Detection Systems (IDS) serve as the first line of defense against these threats, actively monitoring network traffic and system activities to identify and respond to malicious behavior promptly. In the context of MANETs, the development of effective IDS is of paramount importance to ensure the integrity, confidentiality, and availability of data and services.

In this study, we embark on a journey to enhance the security of MANETs by proposing an innovative approach to intrusion detection. Leveraging the power of Support Vector Machines (SVM) in pattern recognition and classification and combining it with Ant Colony Optimization (ACO) for parameter optimization, our approach aims to bolster the accuracy and efficiency of intrusion detection in MANETs.

SVM has demonstrated exceptional performance in various classification tasks, making it a compelling choice for intrusion detection. However, the effectiveness of SVM hinges on the appropriate selection of hyperparameters. This is where ACO steps in, providing an intelligent optimization technique to fine-tune SVM's parameters, resulting in a more robust and accurate intrusion detection system.

The significance of our approach lies in its potential to mitigate the evolving security threats faced by MANETs while optimizing the use of network resources. As we delve deeper into the intricacies of SVM with ACO for intrusion detection in MANETs, this research aims to contribute to the safeguarding of these networks, ensuring their reliability and secure operation in critical applications.

METHOD

In the realm of wireless communication, Mobile Ad Hoc Networks (MANETs) stand as a beacon of adaptability and connectivity, facilitating communication in environments where traditional infrastructure-based networks may falter. However, the very attributes that make MANETs invaluable—decentralization, dynamic topology, and limited resources—also render them susceptible to security threats. Intrusion Detection Systems (IDS) are the vanguards of defense in this domain, tasked with identifying and thwarting malicious activities. In this context, our study introduces an innovative approach to enhance MANET security through intrusion detection, merging the capabilities of Support Vector Machines (SVM) and Ant Colony Optimization (ACO). SVM, renowned for its pattern recognition and classification prowess, forms the foundation of our approach. ACO complements SVM by optimizing its parameters, culminating in a more robust and efficient intrusion detection system. Our pursuit is driven by the imperative to fortify the security of MANETs, safeguarding data integrity, confidentiality, and availability in these dynamic and vital wireless networks.

Our quest to enhance security in Mobile Ad Hoc Networks (MANETs) through intrusion detection unfolds through a meticulously designed methodology that seamlessly combines the strengths of Support Vector Machines (SVM) and Ant Colony Optimization (ACO).

Data Collection and Preprocessing: We commence by gathering a comprehensive dataset comprising network traffic, system activities, and instances of known intrusions within a simulated MANET environment. This dataset serves as the basis for training and evaluating our intrusion detection system.

Feature Engineering: To facilitate effective intrusion detection, we perform feature engineering to extract relevant attributes from the dataset. These attributes include packet payload data, network traffic patterns, and system resource utilization metrics, among others.

Support Vector Machines (SVM): SVM, renowned for its ability to excel in classification tasks, forms the core of our intrusion detection approach. We configure SVM models to classify network traffic and system activities as either benign or malicious based on the engineered features. However, SVM's performance is highly dependent on the selection of appropriate hyperparameters, which we address through ACO.

Ant Colony Optimization (ACO): ACO, a nature-inspired optimization algorithm, steps in to fine-tune SVM's hyperparameters. This intelligent optimization technique explores parameter configurations and identifies the optimal settings for SVM, enhancing its accuracy and robustness in detecting intrusions.

Evaluation: Rigorous evaluation is a cornerstone of our methodology. We employ a variety of performance metrics, including detection rates, false positive rates, precision, recall, and the F1-score, to assess the effectiveness of our intrusion detection system. Extensive cross-validation ensures the reliability and generalizability of our results.

Comparison: We compare the performance of our SVM-ACO-based intrusion detection system with other established methods, including traditional SVM, neural networks, and rule-based systems, to highlight its efficacy in MANET security enhancement.

Real-World Simulations: To validate the real-world applicability of our approach, we conduct simulations using diverse MANET scenarios and intrusion attack types, considering the dynamic nature of these networks.

Through this comprehensive methodology, we aim to demonstrate the potential of SVM with ACO as a formidable tool in the arsenal of MANET security. Our approach not only bolsters the accuracy of intrusion detection but also optimizes resource utilization, making it a promising frontier in safeguarding the integrity and availability of data and services in MANETs.

RESULTS

Our research into enhancing security in Mobile Ad Hoc Networks (MANETs) through intrusion detection with Support Vector Machines (SVM) and Ant Colony Optimization (ACO) has yielded promising results. The outcomes of our study can be summarized as follows:

Improved Detection Accuracy: The combined approach of SVM with ACO significantly improved the accuracy of intrusion detection in MANETs when compared to traditional SVM and other established methods. The fine-tuning of SVM's hyperparameters through ACO led to more precise classification of network traffic and system activities, reducing false positives and false negatives.

Optimized Resource Utilization: By enhancing the accuracy of intrusion detection, our approach minimizes unnecessary resource consumption, making it more efficient for deployment in resource-constrained MANET environments. This optimization is critical for maintaining network performance while ensuring robust security.

Robustness Across Scenarios: Our methodology demonstrated robustness across a variety of MANET scenarios and intrusion attack types, showcasing its adaptability and effectiveness in dynamic network conditions.

DISCUSSION

The discussion surrounding the results of our research centers on the implications and significance of our findings:

Enhancing MANET Security: The improved accuracy of intrusion detection achieved through SVM with ACO has far-reaching implications for MANET security. The ability to detect and respond to malicious activities more effectively enhances the overall security posture of these self-configuring networks.

Resource-Efficient Security: In MANETs, where resources such as bandwidth and power are limited, resource-efficient security mechanisms are paramount. Our approach strikes a balance between security and resource utilization, ensuring that the network remains operational even in the presence of potential threats.

Adaptability and Generalizability: The robustness of our approach across different MANET scenarios underscores its adaptability and generalizability. This adaptability is crucial, given the dynamic and unpredictable nature of MANETs.

CONCLUSION

In conclusion, our study represents a significant advancement in enhancing the security of Mobile Ad Hoc Networks. By harnessing the power of Support Vector Machines with Ant Colony Optimization, we have achieved a notable improvement in intrusion detection accuracy while optimizing resource utilization. This approach not only bolsters the security of MANETs but also ensures the efficient operation of these networks in various scenarios.

As MANETs continue to gain prominence in applications ranging from military operations to disaster response, our research contributes to the development of more resilient and secure communication infrastructures. The fusion of machine learning and optimization techniques in the realm of intrusion detection holds immense promise for safeguarding the integrity, confidentiality, and availability of data and services in these dynamic and vital wireless networks.

REFERENCES

1. J. Jabez and B. Muthukumar, “Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach”, Procedia Computer Science, Vol. 48, pp. 38- 346, 2015.
2. Gulshan Kumar, Krishan Kumar and Monika Sachdeva, “The Use of Artificial Intelligence Based Techniques for Intrusion Detection: A Review”, Artificial Intelligence Review, Vol. 34, No. 4, pp. 369-387, 2010.
3. Zahra Bazrafshan, Hashem Hashemi, Seyed Mehdi Hazrati Fard and Ali Hamzeh, “A Survey on Heuristic Malware Detection Techniques”, Proceedings of 5th International Conference on Information and Knowledge Technology, pp. 113-120, 2013.
4. N. Ye, S.M. Emran, Q. Chen and S. Vilbert, “Multivariate Statistical Analysis of Audit Trials for Host-Based Intrusion Detection”, IEEE Transactions on Computers, Vol. 51, No. 7, pp. 810-820, 2002.
5. P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia Fernandez and E. Vazquez, “Anomaly based Network Intrusion Detection: Techniques, Systems and Challenges”, Computer and Security, Vol. 28, pp. 18-28, 2009.
6. C. Kruegel, D. Mutz, W. Robertson and F. Valeur, “Bayesian Event Classification for Intrusion Detection”, Proceedings of International Conference on Annual Computer Security Applications, pp. 14-23, 2003.
7. D.Y. Yeung and Y. Ding, “Host-Based Intrusion Detection using Dynamic and Static Behavioral Models”, Pattern Recognition, Vol. 36, No. 1, pp. 229-243, 2003.

8. A.M. Cansian, E. Moreira, A. Carvalho and J.M. Bonifacio, “Network Intrusion Detection using Neural Networks”, Proceedings of International Conference on Computational Intelligence and Multimedia Applications, pp. 276-280, 1997.

9. T.R. Srinivasan, R. Shanmugalakshmi and B. Madhusudhanan, “Dynamic Remote Host Classification in Grid Computing using Clonalg”, Proceedings of International Conference and Workshop on Emerging Trends in Technology, pp. 198-201, 2010.