The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 2, April 2025
https://doi.org/10.33022/ijcs.v14i2.4723

A Robust Bayesian Dynamic Stackelberg Game Theory Detection Scheme for Man-in-the-Middle Attack in Mobile Edge Computing Networks

Ramahlapane Lerato Moila[1], Mthulisi Velempini[2]
lerato.moila@ul.ac.za[1], mthulisi.velempini@ul.ac.za[2]
[1,2] Department of Computer Science, University of Limpopo, Polokwane, 0727, South Africa

Article Information

Received : 11 Feb 2025
Revised : 7 Mar 2025
Accepted : 30 Apr 2025

Keywords

Bayesian Dynamic Stackelberg Game Theory, Cybersecurity, Intrusion Detection, Man-in-the-Middle attacks, Mobile Edge Computing

Abstract

Mobile Edge Computing (MEC) networks are emerging technologies transforming how data is processed, stored, and delivered at the edge network, enhancing performance and reducing latency. However, the technology introduces significant cybersecurity challenges, specifically Man-in-the-Middle (MitM) attacks. These attacks compromise sensitive data and can disrupt normal services. This study proposes a robust detection scheme based on Bayesian Dynamic Stackelberg Game Theory to address these vulnerabilities. By incorporating Bayesian inference, the scheme considers uncertainties in the attacker's behaviour and the network environment, enabling the defender to update its strategies dynamically based on observed actions. The simulation results show that the proposed scheme significantly improves the detection scheme for MitM attacks in MEC networks, outperforming other schemes considered in the study. The findings show that integrating Game Theory with Bayesian analysis provides a promising approach for developing adaptive and resilient cybersecurity strategies in the evolving landscape of edge computing.

A. Introduction

The advancement of technology has brought about many challenges. Cloud computing has been considered the future as it provides advantages such as cost efficiency, scalability, flexibility, and security assurance [1]. However, due to the dynamic and broad nature of the services provided by the cloud, it faces challenges that concern consumers, relating to integrity, availability, and confidentiality of data. Despite the benefits, it is also susceptible to challenges such as downtime due to Internet connectivity issues, data privacy, security breaches, limited control, compliance issues, and management costs [2].

To address these challenges, Mobile Edge Computing (MEC) emerged as a promising solution to offload the load of the centralized cloud by bringing data closer to the source for efficient data processing, storage, lower connectivity costs, and reliable and uninterrupted connection [3]. MEC is broadly classified into public and private MEC, as shown in Fig. 1. The public MEC applies across deployments with broad geographic coverage and time-sensitive applications with a need for ultra-low latency, such as public safety, healthcare, and autonomous vehicles. Private MEC, on the other hand, is tailored for localized use cases in conjunction with edge infrastructure and Radio Access Network (RAN) technologies, enabling secure, high-performance solutions for specific industries or enterprises [4].

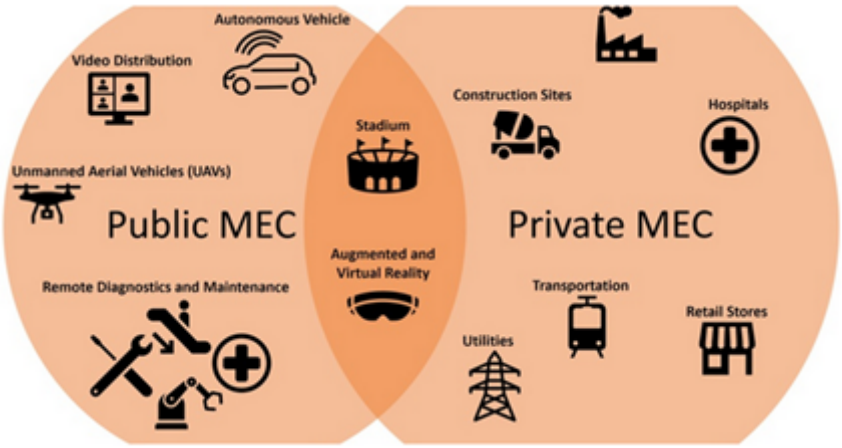

Figure 1. Mobile Edge Computing [4]

MEC technology has revolutionalized how digital data is handled and processed. However, MEC systems are susceptible to complex security challenges that require new approaches to adapt to the advancement of technology. This study aims to develop a robust Manin-the-Middle (MitM) adaptive detection scheme that minimizes high false positives. MitM attacks are common and continue to evolve and become more sophisticated. The literature shows that limitations related to false positives dissipate time and consume resources, causing unnecessary disruptions when attacks remain undetected [5]. However, false negatives allow attackers to compromise a network and sensitive data or disrupt the system. This study employs the Stackelberg Game Theory to model 2 the proposed MitM detection scheme by modeling the defender-attacker interaction. Heinrich Freiherr von Stackelberg, a German economist, introduced the Stackelberg game theory in 1934 [6]. Using this framework, the study contributes to the body of knowledge by developing an

effective detection scheme that can adapt to evolving attacker strategies and improve detection capabilities over time.

1. Related Work

The study in [4] focused on distributed fog computing to minimize the reliance on the cloud for resource-intensive tasks, thereby improving performance and minimize latency. However, fog computing faces significant security challenges. Specifically, the study addresses MitM attacks on the fog layer and proposes an Anomaly-based Intrusion Detection and Prevention System (IDPS) to counter MitM attacks. The study used the exponentially weighted moving average (EWMA), and the simulation results show that the scheme can achieve an accuracy between 80% and 95% percent. However, the proposed scheme highlighted the challenges of increased latency; hence, new approaches are required to address the latency problem. Latency significantly impacts network performance, increases energy consumption, and has security implications.

The study in [7] examined the MEC, which enables offloading latency-sensitive applications. It proposed a SecEdge-Learn Architecture that uses deep learning and blockchain to store data from MEC clusters. This allows deep learning to handle attack scenarios differently. This is done to address the limitations of the machine learning model's limited accuracy and the scalability for real-time attack detection across distributed edge nodes. A more systematic and theoretical analysis is required to explore lightweight models that can execute efficiently with limited resources. Such a model should be flexible and adaptable to cyberattacks and evolving threat landscapes.

The study in [8] addresses the security challenges of the Industrial Internet of Things (IIoT) that use pervasive edge computing for data processing at the edge, minimal response time, and resource limitations. The study proposed a secure and intelligent communication scheme using a parallel Artificial Bee Colony (ABC) (an optimization technique that can explore and exploit large search spaces) algorithm. A more systematic and theoretical analysis may be required; furthermore, it needs to be clarified whether the scheme's scalability in large-scale IoT networks and the overhead of job migration and load balancing have an impact on the network performance. Our study aims to improve the Sybil attack detection and explore alternative optimization algorithms.

MEC decentralizes computational data sources, providing minimized latency while maximizing the throughput. The study in [9] proposed a Resource Allocation and Pricing (RAP)-MEC innovative technique to improve software quality using a session key for encryption purposes and the simulation results show that the scheme minimizes the communication costs by at least 24.85% to 72.73% and its run time from 34.66% 3 to 76.64%. However, the complexity of the proposed scheme may lead to implementation challenges and its dependence on physical unclonable functions, which might be vulnerable to security attacks. Further investigation may be required to explore security techniques to complement the RAP-MEC's existing measures.

The study in [10] focused on the vulnerability of the Internet of Medical Things (IoMT), which is susceptible to MitM attacks. Such attacks can compromise the health and safety of patients. They cause issues in identifying healthcare

emergencies and disrupt the remote healthcare monitoring system operations. The proposed Framework is designed to prevent MitM attacks and ensure secure data transmission in the IoMT devices. The experimental results prove that the scheme achieved a higher detection accuracy for emergency detection and could minimize the false alarm rate by at least 3%. The study is based on Received Signal Strength Indicator (RSSI)-based key derivation, which might be vulnerable to attacks. To address this challenge, other methods for key derivation may be explored to improve the security of the network.

2. Theoretical Foundation

MitM attacks pose a significant threat to the security of the networks. Attackers can intercept and manipulate sensitive data. The traditional schemes often rely on signature-based approaches, which must be optimized for the evolving nature of MitM attacks. The Game theory framework was used to model the interactions between attackers and defenders (detection scheme). The model enables the development of more proactive and adaptive defense detection schemes. This study focuses on the Stackelberg game theory, named after the German economist in 1934. The model has been applied in various anomaly detection studies, especially in areas with high-dimensional big data [11].

The application of the Stackelberg game theory aims to optimize the developed detection scheme by dynamically adjusting to the adversary's actions. The framework enhances the development of a more robust anomaly detection scheme that can adapt to potential threats such as MitM attacks, advanced persistent threats, and zero-day attacks. Bayesian Stackelberg is a powerful tool for designing robust anomaly detection focusing on network scenarios with uncertainty about the attacker's behaviour. In the Bayesian Stackelberg, a defender and an attacker have private data about types or states. The defender first commits to a strategy while considering the possible types of the attacker. The attacker then responds optimally based on the defender's state and the attacker's observed state. In the dynamic Stackelberg, the strategic interaction between the defender and the attacker takes over multiple periods. The dynamic Stackelberg reflects various benefits, such as being realistic for modeling situations where decisions are made over time. It has a strategic adaptation to the evolving state of the game.

3. Bayesian Dynamic Stackelberg Game Theory

Integrating the Bayesian and Dynamic Stackelberg Game Theory is a promising solution to model the uncertainty of an evolving environment. In cyber security, especially the MitM attack, the integrated approach proves to be viable where the defender starts with initial beliefs about potential threats of the MitM attack. The defender monitors the network traffic and updates their beliefs based on the observed anomalies, such as unusual flow data patterns and the changes occurring in routing [12].

3.1 State variables and dynamics

Let $x(t)$ determine the system's state at time t in a dynamic setting. The dynamics govern the evolution of this state:

$$\dot{x}(t) = f(x(t), uL(t), uF(t), \theta) \quad (1)$$

Where:
- $uL(t)$ is the defender's control at time t,
- $uF(t)$ is the attacker's control at time t,
- θ is the defender's type, which is not directly observed by the leader, and
- $f(\cdot)$ describes how the state $x(t)$ changes over time.

3.2 Bayesian beliefs

The defender does not know the exact type θ of the attacker but has a belief represented by a probability distribution $p(\theta)$. As the game progresses, the defender observes the attacker's actions $uF(t)$ and updates its belief function using Bayesian updating. Given the prior belief $p(\theta)$ and the observation of the follower's action $uF(t)$, the posterior belief is updated using Bayes' theorem as follows:

$$P(\theta|uF(t)) = \frac{p(uF(t)|\theta)\ p(\theta)}{p(uF(t))} \quad (2)$$

where:
- $P(uF(t)|\theta)$ is the likelihood of observing the follower's action $uF(t)$ given type θ,
- $p(\theta)$ is the prior belief about the attacker's type θ,
- $P(uF(t))$ is the marginal probability of observing the action $uF(t)$, computed as:

$$P\,(u_F\,(t)) = \sum_{\theta'} P\,(u_F\,(t)/\theta')\cdot p(\theta') \quad (3)$$

This ensures that the posterior belief $P(\theta|uF(t))$ is properly normalized as a probability distribution over the types θ.

3.3 Defender's objective function

The defender aims to maximize its expected payoff over the entire period, considering the system's dynamic evolution and updated beliefs about the attacker's type. Hence, the defender's objective function in a Bayesian Dynamic Stackelberg game can be expressed as:

$$uL(t) maxE\theta[JL] = \left[\int_0^T gL(x(t), uL(t), u * F(t), \theta)\mathrm{dt} + \mathrm{hL(x(T)}, \theta)\right] \quad (4)$$

- $gL(x(t), uL(t), u * (t), \theta)$ is the running payoff of the defender at time t,
- $hL(x(T), \theta)$ is the terminal payoff at the final time T ,
- $E\theta[\cdot]$ denotes the expectation concerning the defender's belief about the attacker's type θ,
- $U * F(t)$ is the attacker's best response at time t, given their type θ and the defender's strategy.

3.4 Defender's optimization problem

The attacker observes the defender's strategy $uL(t)$ and optimizes its payoff given its type θ. The attacker's optimal strategy $u * F(t)$ is given by:

$$U * F(t) = arg\ max(uF(t)) \left[\int_0^T gF(x(t), uL(t), uF(t), \theta)\ \mathrm{dt} + \mathrm{hF(x(T), \theta)} \right] \quad (5)$$

Where:

- $gF\ (x(t), uL(t), uF\ (t), \theta)$ is the running payoff of the attacker (follower) at time t,
- $hF\ (x(T), \theta)$ is the terminal payoff of the attacker at the final time T,
- $uL(t)$ is the defender's control strategy observed by the attacker,
- θ represents the attacker's type, influencing its payoffs.

The attacker's strategy $u\ *\ F\ (t)$ maximizes its total expected payoff over the time interval $[0, T]$, based on the current state $x(t)$, the observed defender's strategy $uL(t)$, and its type θ.

4. Bayesian Dynamic Stackelberg Game Theory

Table 1 is the structure of the Bayesian dynamic Stackelberg theory approach for detecting and responding to anomalies. The algorithm begins with data collection, preprocessing the data to check imbalance data, errors, and missing values, and is used to train the anomaly detection model. All the detected anomalies will trigger an alert, allowing necessary actions to be taken. The algorithm incorporated the Bayesian Framework to update beliefs about the attacker's behaviour over time. The algorithm observes the attacker's actions in every epoch using the Bayesian inference and thus optimizes the defender's strategy accordingly. The system's state will be dynamically updated based on the defender's optimized strategy and the attacker's response, thereby continually refining the defense mechanism. All the generated alerts will be displayed, providing real-time feedback about the potential threats.

Algorithm 1 Proposed Algorithm

1: **data** = collect_data()
2: **preprocessed_data** = preprocess_data(data)
3: **anomaly_model** = train_anomaly_model(preprocessed_data)
4: **anomalies** = detect_anomalies(anomaly_model, preprocessed_data)
5: **alerts** = generate_alerts(anomalies)
6: **prior_p_theta** = initial_belief()
7: **for** t = 1 to T **do**
8: **uf_t** = observed_attacker_action()
9: **p_uf_ given_theta** = likelihood_of_action_ given type(uf_t, prior_p_theta)
10: **posterior_p_theta** = bayesian_update(prior_p_theta, uf_t, p_uf given_theta)
11: **uL_t** = optimize defender strategy(x_t, posterior_p_theta)
12: **uF_star_t** = attacker response(x_t, uL_t, posterior_p_theta)
13: **x_t** = state dynamics(x_t, uL_t, uF_start, posterior_p_theta)

14: **end for**
15: **for** alert **in** alerts **do**
16: print(alert)
17: **end for**

5. Simulation Results

5.1 ARP-SDN dataset

The Address Resolution Protocol—Software Defined Network (ARP-SDN) dataset used in this study is publicly available and downloaded from the Kaggle database. The dataset classifies network traffic with features that include normal and malicious behaviour. Fig. 2 shows the traffic classification. The data has about 15 thousand normal traffic and 13 thousand malicious traffic, as depicted in Figure 2.

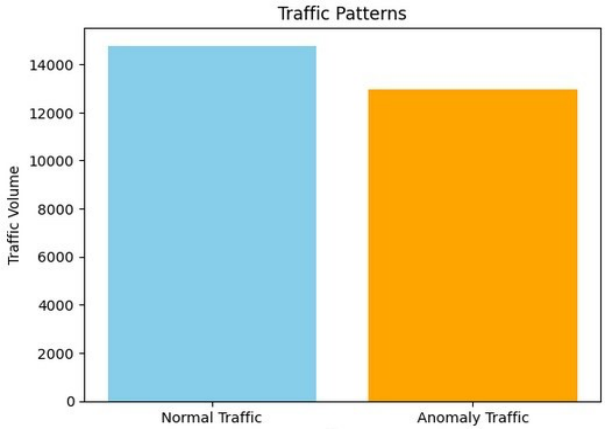

Figure 2. Normal and malicious traffic classification

In this section, the study discusses the approaches taken to implement the proposed scheme. The detection scheme was implemented in Google Collab, and the dataset was split into 70% training and 30% testing [13]. The proposed scheme was trained using the Random Forest (RF) for the classification of network traffic as either standard or malicious. The algorithm uses the Bayesian to update the beliefs about the attacker's type, based on the observed anomalies and then uses the Stackelberg Game framework to compute the optimal strategies for both the defender and the attacker by utilizing the updated beliefs.

We preprocessed the data to ensure accuracy and consistency. Normal data has missing values, inaccuracies, or imbalanced data that should be corrected to improve quality. The dataset consists of 115 features, and a filter-based was used to select only features relevant to the study and to increase the prediction accuracy of the algorithms used. After updating the beliefs using the Bayesian updat- ing, we calculated the Stackelberg equilibrium, which enhances the accuracy detection for the proposed scheme, such as anticipating the attackers' behavior, robustness anal- ysis, and the optimal defense strategy. We also computed the regret metric to ensure efficient resource utilization.

Fig. 3 shows the convergence of beliefs over time for the proposed model. The results indicate that the convergence metric changes over time, sharply decreasing before s t a b i l i z i n g as time progresses. Fig. 4 demonstrates that the proposed model achieved a stable accuracy of 100% over the number of iterations the simulation was executed.

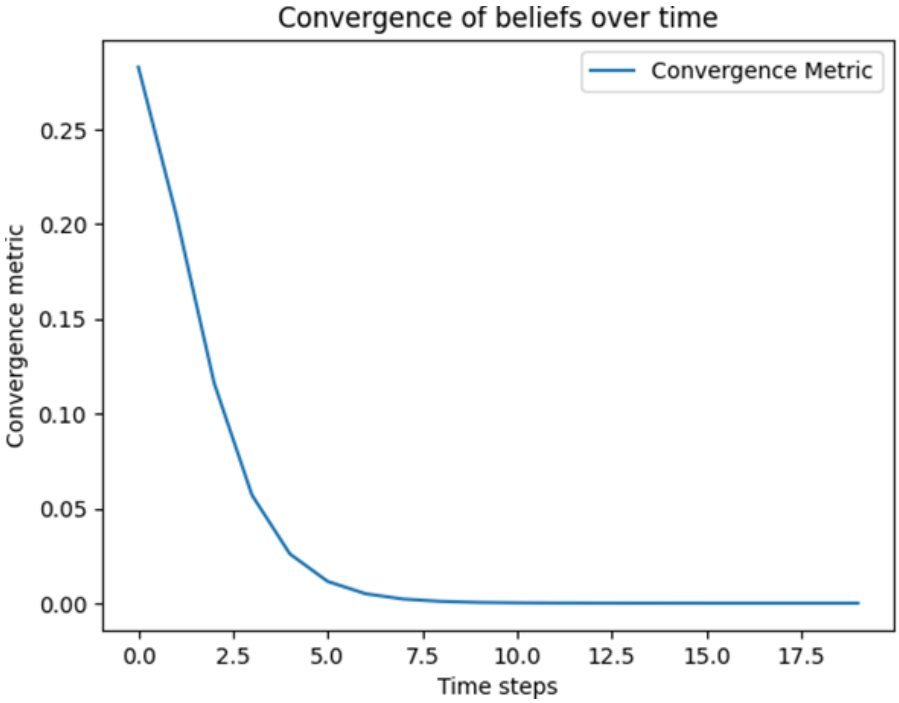

Figure 3. Convergence of beliefs over time

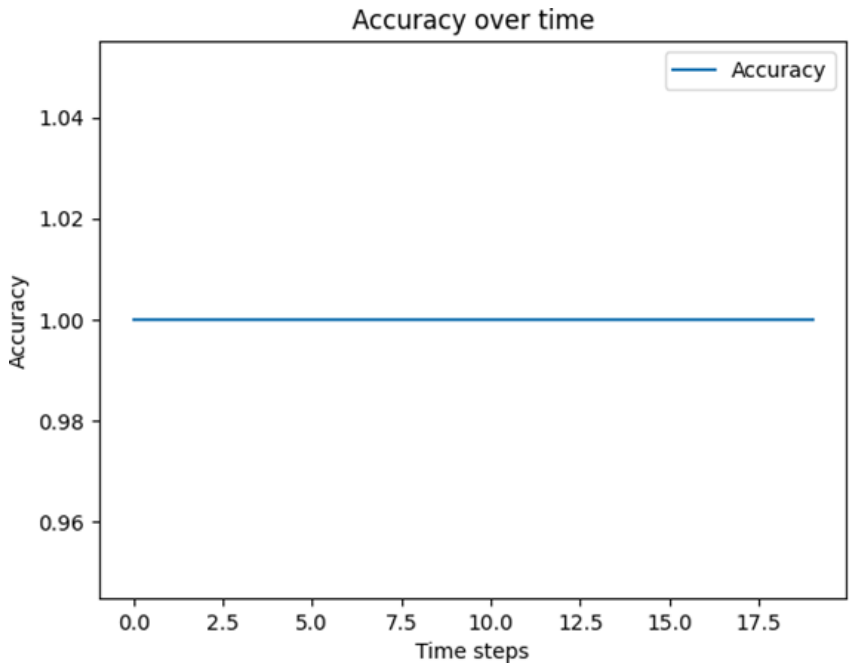

Figure 4. Accuracy over time

In Fig 5, the results show that the defenders regret initially increase as the convergence metric decreases. This is due to the defender experimenting with different strategies to counter the attacker's moves. During this phase, the defender tries to determine the most effective defense mechanisms, leading to higher regret as suboptimal strategies are tested. Once the defender establishes a more effective strategy or adapts to the attacker's tactics, the regret stabilizes, indicating an adaptation or learning process.

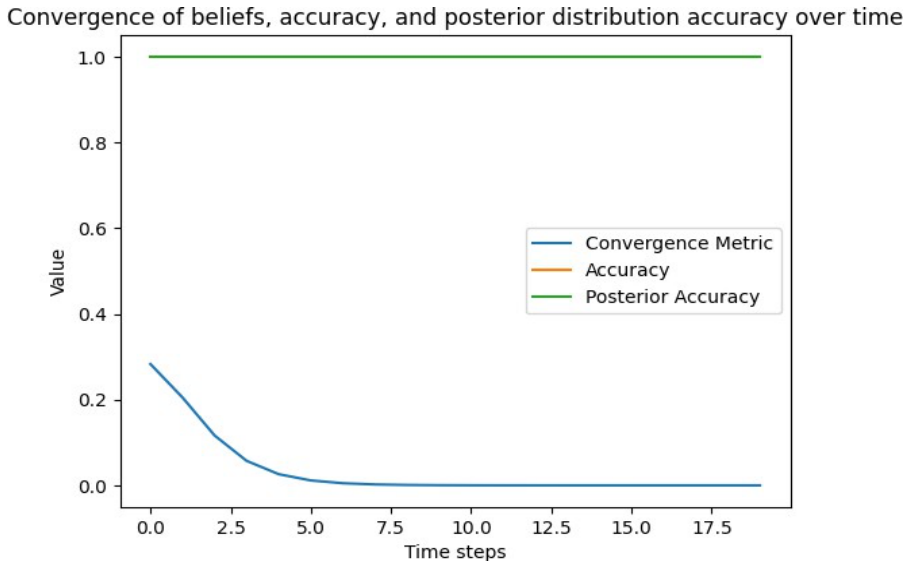

Figure 5. Posturing results over time

In Fig. 6, when the attacker's regret remains low, the attacker learns from past actions and adjusts its strategy accordingly. A stable strategy over time indicates that the attacker has found a reliable approach that works well in the given environment. This stability arises because the attacker possesses a deep understanding of the system they are targeting, enabling them to anticipate the system's responses and accurately predict the outcomes of their actions. This knowledge allows the attacker to exe- cute well-planned, consistent strategies that minimize unpredictability and maximize the effectiveness of their attacks. While the attacker's regret remains low, indicating various dynamics in making decisions or a stable strategy over time.

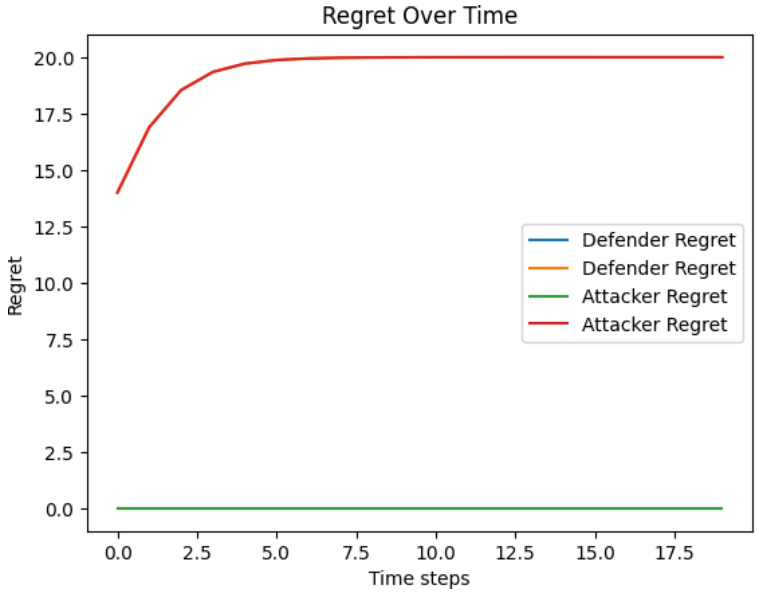

Figure 6. Regret over time results

Fig. 7 illustrates the game theory that visualizes the interaction between two parties labeled as the defender, the attacker, and its payoff matrix. The figure shows the surfaces (purple and blue) which represent various outcomes based on the strategies of the defender and the attacker [9]. The figure helps us to understand how strategies impact their payoff, which is crucial in cybersecurity. By analyzing these surfaces, we can identify optimal strategies for both parties, enabling us to effectively predict and mitigate potential cyber threats.

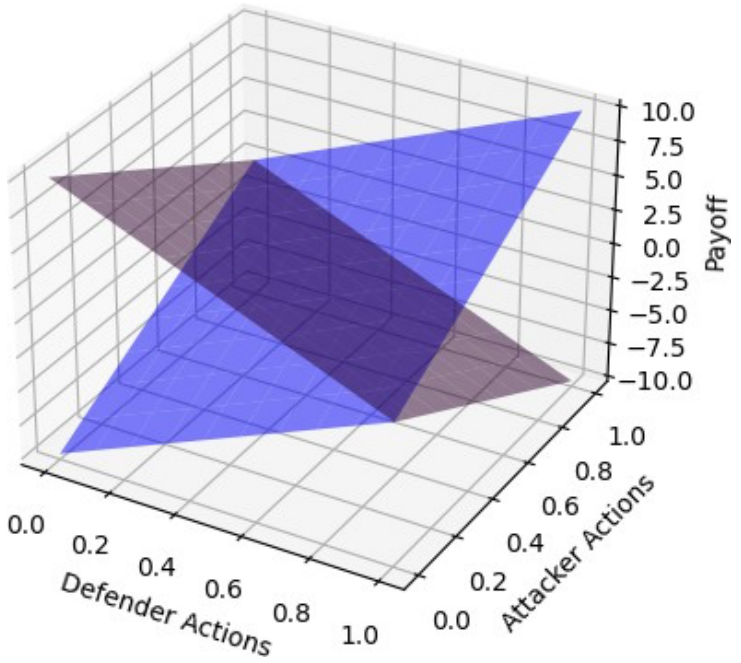

Figure 7. Decision analysis between the defender and the attacker's action.

Table 1 records the outcomes of the Bayesian Dynamic Stackelberg game theory as our proposed model and other algorithms used in our study. We ran the simulation five times to observe the changes over time between the algorithms. The decision tree and the Support Vector Machine algorithms were also modeled using the Stackelberg Game Theory, and the results were generated. It can be observed in Table 1 that the proposed scheme outperformed both the Decision Tree and SVM schemes over time. Table 1 also depicts the recall, precision, and F1-score metrics, indicating that the proposed scheme outperformed the Decision tree and SVM schemes.

The proposed scheme achieved a higher precision than the Decision tree and SVM scheme, indicating that the scheme does not incur many false positives. The higher recall means that the scheme correctly detected most events positively. Finally, the proposed scheme achieved good results because it captures the balance between preci- sion and makes informed decisions about the scheme's predictions about the defender and the attacker's actions over time.

Table 1. Model Performance Comparison

Iteration	Model	Metrics				
		Precision	Recall	F1-score	Accuracy	Cross-validate
1	Proposed Model	0.997806	0.997675	0.997739	0.997751	0.997278
2	Proposed Model	0.997692	0.997524	0.997606	0.997618	0.996692
3	Proposed Model	0.996585	0.996245	0.996409	0.996428	0.996630
4	Proposed Model	0.997387	0.997193	0.997288	0.997301	0.995951

5	Proposed Model	0.995479	0.995086	0.995273	0.995293	0.995368
1	Decision Tree	0.991059	0.991066	0.991062	0.991097	0.991134
2	Decision Tree	0.988095	0.995370	0.988749	0.994044	0.989411
3	Decision Tree	0.992972	0.992935	0.992954	0.992988	0.991862
4	Decision Tree	0.993525	0.993557	0.993541	0.993569	0.992696
5	Decision Tree	0.990019	0.990258	0.990135	0.990176	0.989679
1	SVM	0.982682	0.980782	0.981577	0.981691	0.974791
2	SVM	0.976191	0.976190	0.975198	0.976166	0.970208
3	SVM	0.984747	0.983785	0.984216	0.984293	0.985179
4	SVM	0.987038	0.986519	0.986765	0.986835	0.986601
5	SVM	0.988591	0.988602	0.988597	0.988647	0.987536

Fig. 8 presents the accuracy results. We can observe that the proposed model was able to predict accurately. This improves the reliability of the scheme for threat detection, data analysis, and decision-making. The Support Vector Machine had a steep drop, and then it increased, indicating that all the schemes performed better, with the proposed scheme being superior. The proposed model consistently performs well, maintaining a score of at least 99.5% across all iterations due to robust feature selection, effective preprocessing, and advanced algorithm design. Additionally, high- quality training data and careful hyperparameter tuning further enhance its ability to generalize and deliver stable, accurate results. Fig. 9 is the validation of the proposed model, which provides a more accurate estimate of how the model performs in the real- world.

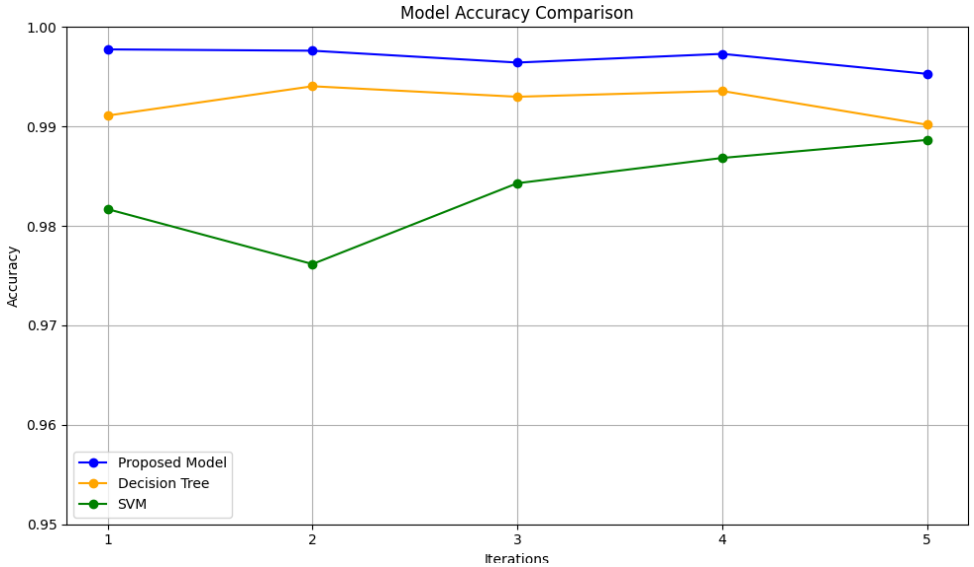

Figure 8. Accuracy results

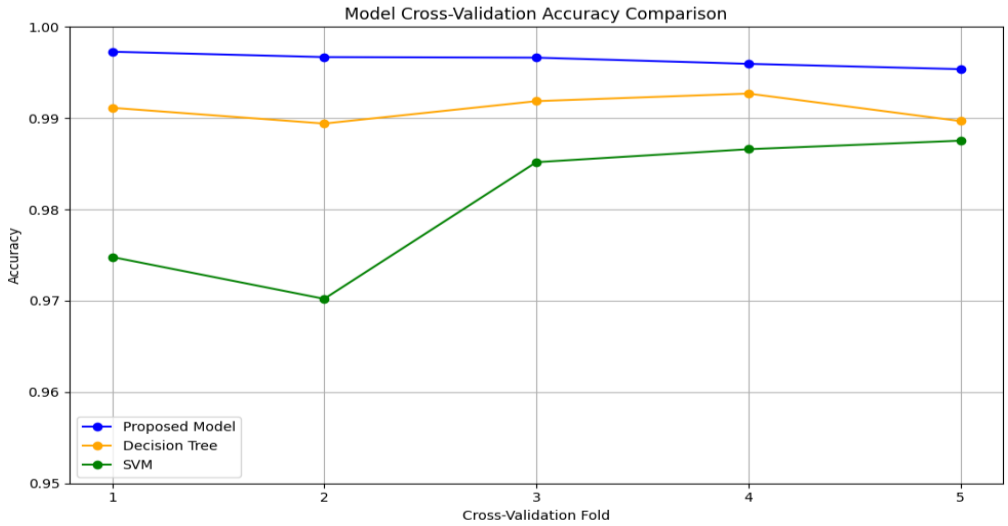

Figure 9. Cross-validation results

5.2 Scenario 2

The study also used the HIKARI Network Intrusion dataset. The dataset is based on real and encrypted synthetic attack traffic and was generated to provide a comprehen- sive understanding of network intrusion. The dataset has 555 278 instances, of which 93.2% (517582) are normal traffic while 6.8% (37696) are malicious traffic, as shown in Fig. 10 [14].

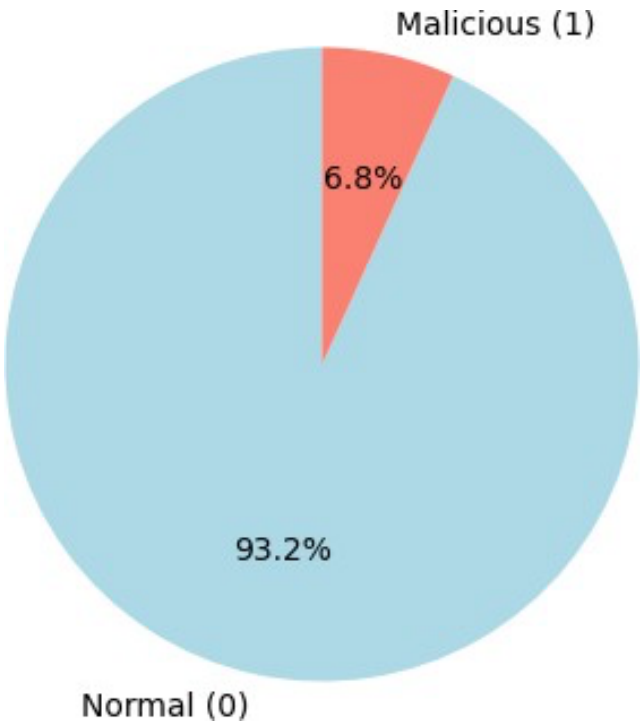

Figure10. Dataset traffic classification [14]

The simulation results show that the proposed model is performing well, achieving an accuracy of 100% and a cross-validation score of 0.999979. In Table 1, we can observe that, while utilizing the ARP-SDN dataset, the model performed well with an accuracy of 0.997751 and a cross-validation score of 0.997278. Hence, there is an improvement of 0.002721 accuracy and 0.002701 in cross-validation. The performance is maintained because the model is likely well-generalized, meaning it effectively captures the underlying patterns in the data without overfitting specific datasets. This robustness is achieved through comprehensive preprocessing, representative training data, and a well-designed algorithm capable of adapting to variations in the datasets.

Fig. 11 shows the results of the proposed model's regret over time for the defender and the attacker. The figure shows that the defender and the attacker start with a low regret and gradually increase, but they become more constant, close to the maximum possible regret (around 20). The results imply that since the regret is not increasing, the defender's strategy is effective over time, as the regret does not increase beyond a certain point.

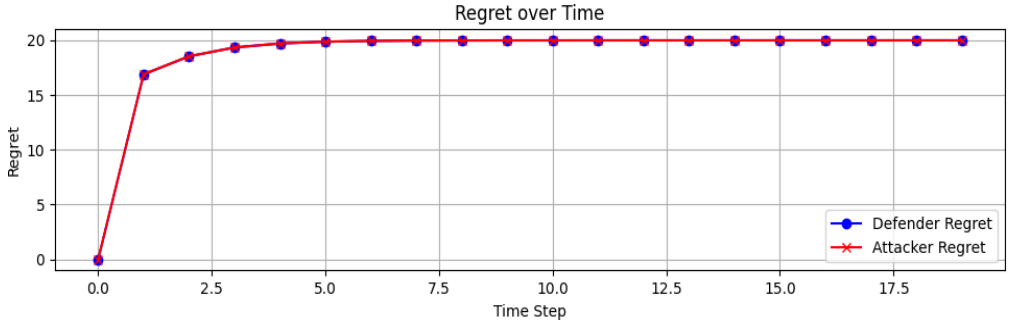

Figure 11. Proposed Model regret over time

6. Conclusion

In this study, we developed a robust detection scheme and utilized a Bayesian Dynamic Stackelberg game theory to model and mitigate MitM attacks in MEC. The study modeled the interactions between defenders and attackers to counter cyber threats by anticipating the defender's and attacker's actions. The simulation results show that the game framework approach could predict the defender and the attacker's actions accurately, with a significant increase in detection accuracy and a reduction in the success rate of the attacks. The study further evaluated the model's performance using the HIKARI network intrusion dataset. The results show that the proposed model maintained its performance across both datasets, with an observed improvement of 0.002721 accuracy and 0.002701 in cross-validation metrics, respectively.

The model's improved performance can be attributed to its ability to generalize effectively across various datasets, likely due to robust preprocessing techniques that handle data inconsistencies, such as imbalanced data, missing values, or noise. Addi- tionally, the observed improvements in accuracy and cross-validation metrics suggest that the model is well-optimized through fine-tuned hyperparameters and an architec- ture designed to adapt to diverse

patterns in the data. The iterative training process also plays a role, ensuring convergence to a high-performing solution with minimal overfitting.

Including the Bayesian update mechanism significantly improved the robustness of the interaction between the defender and the attacker, leading to more adaptive and resilient defense strategies. These findings have significant implications for the development of cyber defense schemes, particularly in industries where Mobile Edge Computing is prominent, such as telecommunications and autonomous systems. How- ever, the study assumes a single attacker and focuses on relatively low-uncertainty environments. There is a need to explore more complex scenarios, such as more attackers and higher uncertainty levels. Further investigations on integrating resource constraints and network dynamics can be helpful in improving the applicability of the proposed approach.

Declaration

Availability of data and materials The data sets used and analyzed during the current study were obtained from Kaggle. All relevant data supporting the findings of this study are publicly available on the Kaggle platform. Further inquiries can be directed to the corresponding author.

Competing Interests

The authors declare that they have no financial or non- financial competing interests related to this manuscript.

Funding

This research was funded by the University of Limpopo. The funding body had no role in the design of the study, the collection, analysis and interpretation of the data, or the writing of the manuscript.

Authors' Contributions

Ramahlapane Lerato Moila was responsible for the research design, data collection, analysis, and interpretation of the data, and drafting the manuscript; Mthulisi Velempini conceptualized the idea, supervised a post-graduate student, and revised the manuscript.

Abbreviations

- ABC - Artificial Bee Colony
- ARP-SDN - Address Resolution Protocol - Software Defined Network
- EWMA - Exponentially Weighted Moving Average
- IDPS - Intrusion Detection and Prevention System
- IoMT - Internet of Medical Things
- MEC - Mobile Edge Computing
- MitM - Man-in-the-Middle
- RAP - Resource Allocation and Pricing

- RAN - Radio Access Network
- RSSI - Received Signal Strength Indicator
- SVM - Support Vector Machine

7. References

[1] Xavier, R., *et al.*: Integrating multi-access edge computing (mec) into open 5g core. Telecom **5**(2), 433–450 (2024) https://doi.org/10.3390/telecom5020022

[2] Wang, C., et al.: The Security and Privacy of Mobile Edge Computing: An Artificial Intelligence Perspective. arXiv (2024). http://arxiv.org/abs/2401.01589

[3] Thudumu, S., *et al.*: A comprehensive survey of anomaly detection techniques for high dimensional big data. Journal of Big Data **7**(1), 42 (2020) https://doi.org/ 10.1186/s40537-020-00320-x

[4] Pakmehr, A.: Task Offloading in Fog Computing with Deep Reinforcement Learn- ing: Future Research Directions Based on Security and Efficiency Enhancements. arXiv (2024). http://arxiv.org/abs/2407.19121

[5] Mohammed Alotaibi, F., *et al.*: Rap-mec: Robust authentication protocol for the mobile edge computing services. IEEE Access **12**, 109673–109689 (2024) https://doi.org/10.1109/ACCESS.2024.3438618

[6] Ogunlola, Y., *et al.*: A theoretical game approach to attacker-defender interaction. International Journal for Information Security Research **12**(1), 1017–1023 (2022) https://doi.org/10.20533/ijisr.2042.4639.2022.0115

[7] Garg, S., *et al.*: Security in iot-driven mobile edge computing: New paradigms, challenges, and opportunities. IEEE Network **35**(5), 298–305 (2021) https://doi. org/10.1109/MNET.211.2000526

[8] Alotaibi, B.: A survey on industrial internet of things security: Requirements, attacks, ai-based solutions, and edge computing opportunities. Sensors **23**(17), 7470 (2023) https://doi.org/10.3390/s23177470

[9] El Kafhali, S., El Mir, I., Hanini, M.: Security threats, defense mechanisms, challenges, and future directions in cloud computing. Archives of Computational Methods in Engineering **29**(1), 223–246 (2022) https://doi.org/10.1007/ s11831-021-09573-y

[10] Ahmed, S.F., *et al.*: Insights into internet of medical things (iomt): Data fusion, security issues and potential solutions. Information Fusion **102**, 102060 (2024) https://doi.org/10.1016/j.inffus.2023.102060

[11] Maccarone, L.T., Cole, D.G.: Bayesian games for the cybersecurity of nuclear power plants. International Journal of Critical Infrastructure Protection **37**, 100493 (2022) https://doi.org/10.1016/j.ijcip.2021.100493

[12] Kumari, P., Toshniwal, D.: Real-time estimation of covid-19 cases using machine learning and mathematical models - the case of india. In: 2020 IEEE 15th International Conference on Industrial and Information Systems (ICIIS), pp. 369–374. IEEE, RUPNAGAR, India (2020). https://doi.org/10.1109/ICIIS51140.2020.9342735

[13] Gu, X.: Mapping and Optimizing an Electric Vehicle Triple Supply Chain:

Electric Vehicles, Energy Supply and Batteries (n.d.)
[14] Ferriyan, A., *et al.*: Generating network intrusion detection dataset based on Real and encrypted synthetic attack traffic. Applied Sciences **11**(17), 7868 (2021) https://doi.org/10.3390/app11177868