Enhancing Maritime Cybersecurity with Advanced Anomaly Detection using Semi-Markov Processes

Kamel Abbad
Unicaen, Ensicaen
Normandy Univ, CNRS, GREYC
14000, Caen, FRANCE
kamel.abbad@ensicaen.fr

Lyes Khoukhi
Unicaen, Ensicaen
Normandy Univ, CNRS, GREYC
14000, Caen, FRANCE
lyes.khoukhi@ensicaen.fr

Lionnel Mesnil
NEAC Industry
14000, Caen, FRANCE
lionnel.mesnil@neac-industry.fr

Alain Alliot
NEAC Industry
14000, Caen, FRANCE
alain.alliot@neac-industry.fr

***Abstract*—The swift evolution of digital technologies in maritime operations has highlighted the critical need for tailored cybersecurity measures, especially to mitigate Distributed Denial of Service (DDoS) attacks targeting essential communication protocols such as NMEA 2000. This study introduces an innovative solution based on stochastic semi-Markov processes, specifically tailored to strengthen the cybersecurity framework of maritime IoT systems. By capturing and analyzing the distinct state transitions within maritime networks, the proposed model effectively identifies abnormal activities and promptly alerts operators to potential DDoS attacks, ensuring robust and uninterrupted maritime communications. Comprehensive simulations demonstrate the model's superior accuracy, high detection efficiency, and minimal error rates, establishing it as a dependable and specialized approach to protecting critical maritime systems. This research significantly advances maritime cybersecurity by offering proactive and adaptive mechanisms to combat increasingly complex cyber threats.**

***Index Terms*—Maritime Cybersecurity,Distributed Denial of Service (DDoS),NMEA 2000 Protocol, Markov Chains, IoT Security**

I. Introduction

The increasing digitalization of maritime operations has made vessels heavily reliant on interconnected systems for navigation, communication, and cargo management. This heightened connectivity, while beneficial for operational efficiency, introduces significant cybersecurity vulnerabilities. In particular, the lack of robust security mechanisms in communication protocols such as NMEA 0183 and NMEA 2000 has made maritime IoT systems increasingly susceptible to various cyberattacks, including DDoS, Man-in-the-Middle (MitM), and message injection attacks. These attacks can severely disrupt the critical exchange of navigational and control data, posing risks to both vessel safety and economic operations.

IoT cybersecurity has explored various methodologies, ranging from deterministic models to stochastic and reputation-based techniques. While deterministic approaches have shown effectiveness in controlled environments, they often lack the flexibility required to cope with the dynamic and resource-constrained nature of maritime IoT systems. For instance, Pavur et al. [1] exposed critical vulnerabilities in maritime Very Small Aperture Terminal (VSAT) communication channels due to weak encryption and interceptability, yet their work did not account for energy efficiency or real-time constraints.

Reputation-based mechanisms, such as those proposed in [2], have demonstrated success in detecting black hole attacks in vehicular networks by dynamically evaluating node behavior. However, their applicability in maritime settings remains limited due to differences in network architecture and the overhead of maintaining reputational data. Similarly, resource-aware strategies based on Markov Decision Processes have been used for efficient data offloading in mobile cloud computing environments [3] [4], and distributed intrusion detection frameworks have been proposed for smart grids using fog computing to reduce latency and resource usage [5]. These solutions illustrate promising directions, yet they have not been adequately adapted to the unique characteristics of maritime NMEA-based communication, where bandwidth, power consumption, and computational capacity are severely constrained.

Previous research has addressed IoT cybersecurity using a variety of approaches. Traditional deterministic models, while effective in certain environments, often fail to adapt to the dynamic and complex behavior inherent to maritime IoT systems. Some studies have applied Markov models to anomaly detection in IoT environments, but these efforts have lacked practical implementations within maritime contexts, especially given the challenges posed by transitioning between coastal and open-sea communications. Moreover, the energy efficiency of these models has not been adequately considered, limiting their real-world applicability for vessels with limited power resources.

Unfortunately, despite substantial efforts in IoT cybersecurity, existing methods fall short in addressing the critical energy and real-time requirements of maritime IoT systems. This paper proposes an innovative solution to these challenges by leveraging:

- Semi-Markov processes that adaptively model state transitions for robust anomaly detection.
- Energy-efficient design that fits within the operational constraints of maritime vessels, particularly those with limited power availability.
- Real-time anomaly detection and alerting, enabling immediate operator intervention to maintain secure communications.

II. Related Work

The increasing number of cyberattacks on maritime systems has exposed significant vulnerabilities, highlighting the critical need for robust cybersecurity measures [1], [6]. Previous research efforts have largely focused on protecting digital systems involved in navigation, communication, and cargo management onboard ships. However, despite these efforts, many approaches fall short in addressing the dynamic and complex nature of maritime environments.

For instance, in IoT systems, Markov Chains have been used to detect false data injection (FDI) and denial-of-service (DoS) attacks [7]. However, the application of Markov Chains in maritime cybersecurity is still limited, with existing approaches often lacking practical implementations.

Traditional anomaly detection methods in maritime systems have relied on statistical techniques, such as threshold-based detection and statistical process control, which monitor deviations from normal behavior. While these methods are straightforward and easy to implement, they often fail to capture complex patterns in the data, especially in environments with high variability and complexity like maritime systems. Machine learning approaches, such as supervised and unsupervised learning, offer more flexibility and accuracy but are limited by the need for extensive training data and significant computational resources [8].

Furthermore, while Markov Chains provide a balanced approach by modeling temporal dependencies and detecting deviations in a probabilistic manner, their application in maritime systems remains underexplored. Most existing research has focused on theoretical models without offering practical implementations. For example, Kaminska et al. [8] developed a Markov Chain model for ship cybersecurity but did not provide a practical implementation, leaving a gap in the field that needs to be addressed.

Selamnia et al. [9] proposed a stochastic approach to securing IIoT networks against DDoS attacks, demonstrating the applicability of stochastic methods in detecting and mitigating cyber threats. Rogers et al. [10] focused on detecting CAN attacks on J1939 and NMEA 2000 networks, further emphasizing the vulnerabilities of these protocols and the need for advanced detection mechanisms.

However, there is a notable lack of practical implementations using Markov Chains specifically tailored for maritime cybersecurity, particularly in the context of the NMEA 2000 protocol. Existing studies often fail to address the unique challenges posed by the maritime environment, such as the high variability in data patterns and the need for real-time anomaly detection.

Our research builds on these findings by implementing a Markov chain-based anomaly detection model specifically tailored for NMEA 2000 messages. This approach not only addresses the specific challenges and vulnerabilities associated with the NMEA 2000 protocol but also provides a practical solution that can be implemented in real-world maritime systems, filling a critical gap in the existing body of research.

III. MARITIME IoT DDOS ATTACK PREDICTION

The integration of IoT networks in various industries, including the maritime sector, offers numerous benefits but also introduces a plethora of security challenges and potential failure points. The original design of these networks often did not fully account for security, and this is exacerbated by misconfigurations from developers who may lack full awareness of security needs, as well as vulnerable default settings provided by commercial solutions. Therefore, ensuring the security of these networks is essential.

We start by identifying and analyzing the potential attack scenarios that the system might encounter. Following this analysis, we propose a robust system architecture designed to counteract these threats. Once the architecture is established, we develop a detection model utilizing a Markov chain approach.

A. DDoS Attack Scenarios

To evaluate our detection model on NMEA2000 traffic, we simulate two core threats: (1)Message injection bursts of forged frames that swamp the bus, disrupt legitimate channels, and can crash onboard systems and (2) Network flooding a sustained high rate stream that clogs the bus, delaying or dropping critical navigation data.

B. Our Solution: A Functional Walk-through

As depicted in Figure 1, our proposed approach is focused on securing the NMEA 2000 interface within the network layer. The data exchanges, shown in the figure, originate from various devices such as LiDAR, radar, and AIS systems.

In maritime environments, when vessels are close to shore or within port areas, they typically rely on 5G base stations for communication. However, as these vessels move further out to sea, the communication shifts to satellite systems to maintain connectivity. While these transitions between 5G and satellite communications are crucial for maintaining uninterrupted service, they are not the primary focus of this paper. Consequently, we will not delve deeper into this topic, but relevant studies can be found in the literature on maritime communications and satellite integration into 5G networks [11].

AIS (Automatic Identification System) is a tracking system used on ships for identifying and locating vessels by electronically exchanging data with other nearby ships and AIS base stations [12]. Radar (Radio Detection and Ranging) uses radio waves to detect and determine the distance, speed, and other characteristics of objects [13].

These communications often contain sensitive information, making them potential targets for malicious activities. Attackers could exploit these channels to either inundate the system with massive amounts of data (DDoS attacks) or manipulate GPS coordinates to falsify location information. Our approach aims to detect and mitigate these types of attacks, ensuring the integrity and reliability of the data. We can delve further into how our approach will be utilized in Fig 2.

- IoT End Devices these are the source devices in the maritime network that generate data. They include sensors, navigation systems, and other IoT devices essential for maritime operations.

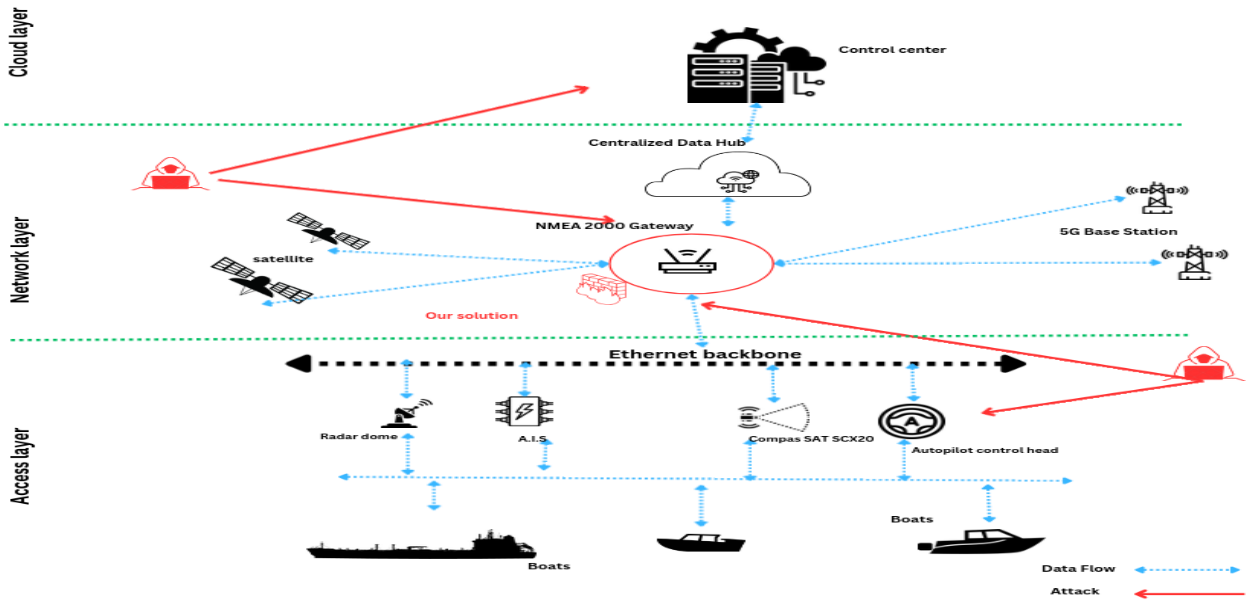

Fig. 1: Solution positioning for Maritime Networks

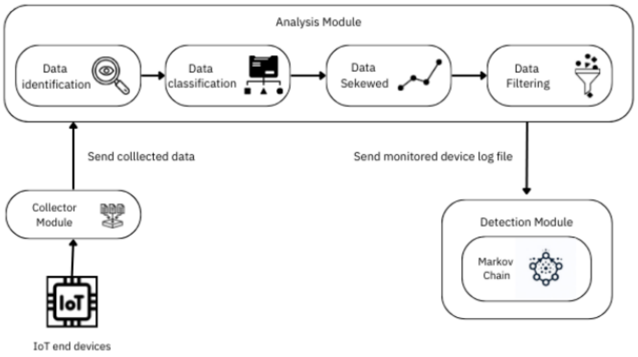

Fig. 2: System Architecture and Data Flow Analysis

- The Collector Module is responsible for gathering data from the IoT end devices. This data includes various types of information such as sensor readings, navigation data, and communication logs. Once collected, the data is sent to the Analysis Module for further processing.
- Analysis Module: This module consists of four sub-components:
  - Data Identification this sub-component identifies and tags the collected data based on its source and type. Accurate identification is crucial for subsequent analysis.
  - Data Classification the classified data is sorted into different categories based on predefined criteria. This step ensures that similar types of data are grouped together, facilitating more effective analysis.
  - Data Skewing here, the data is analyzed for any irregular patterns or anomalies. This step is critical for detecting signs of potential DDoS attacks. Skewed data often indicates unusual traffic patterns that may be symptomatic of such attacks.
  - Data Filtering the filtered data is cleansed to remove any irrelevant or redundant information. This process helps in focusing on the most pertinent data for the detection process, improving the accuracy and efficiency of the system.
- Detection Module this module utilizes Markov Chains for the detection of DDoS attacks. The processed data from the Analysis Module is used to model the state transitions within the network. The Markov Chain model helps in identifying deviations from normal state transitions, which are indicative of potential attacks. This probabilistic approach allows for real-time detection and mitigation of DDoS threats.

IV. Markov Chain for Attack Detection in Maritime IoT

We apply a semi-Markov stochastic model to analyze and predict security risks in autonomous maritime IoT networks navigating urban rivers, adapting to the vessels' constantly changing conditions.

A. *Range-Based Activity Sifting Policy :*

In order to accurately classify device behavior under varying maritime conditions, we introduce a range-based activity sifting policy. The policy aims to scrutinize the activity patterns of each maritime IoT device and assign it to discrete security risk levels, reflecting the likelihood of a security incident occurring. This classification considers the unique operational parameters of maritime IoT, such as navigation data, communication intervals, and environmental sensor feedback. We propose the following risk levels, delineated by thresholds determined from the historical log data of each device: authentic, low risk, medium risk, and high risk. These thresholds are established using the mean of the data distribution, with values securely logged within a private blockchain, ensuring tamper-proof recording of device activities.

B. Stochastic Modeling of Device Behavior :

Stochastic modeling is crucial for identifying the stationary state of an IoT device based on its previous behavior. We consider that a device can transition from an authentic state to an attack state by performing malicious activities on the network. To detect and predict security attacks in the network, we first use an activity filtering strategy based on defined ranges to represent the possible states of each device. Then, we use a Markov chain to predict the next transition state of a device based only on the current state.

1) **State Space:** Figure 3 illustrates the state transition diagram for an IoT device with predefined states. The state space is defined as follows:

$$S = \{N, SAD, TI, B\}$$

C. Transition Probabilities Between States:

In our Markov model, the system transitions between different states based on detected conditions in the maritime IoT environment. The following are the defined states and their associated transition probabilities:

- **Normal (N) → Suspicious Activity Detected (SAD):** The system transitions from a Normal state to a Suspicious Activity Detected state when it identifies unusual or potentially harmful traffic patterns.

$$P_{N \to SAD}$$

- **Suspicious Activity Detected (SAD) → Threat Identified (TI):** Upon detecting suspicious activity, the system further analyzes the pattern and transitions to a Threat Identified state if it confirms a potential attack.

$$P_{SAD \to TI}$$

- **Threat Identified (TI) → Action Required (AR):** If the threat is confirmed and deemed serious, the system transitions to the Action Required state, indicating that immediate measures need to be taken to mitigate the threat.

$$P_{TI \to AR}$$

- **Action Required (AR) → Normal (N):** Once the necessary actions have been taken and the system is secure, it can transition back to the Normal state.

$$P_{AR \to N}$$

These transition probabilities reflect the likelihood of the system moving from one state to another based on the detection and analysis of network traffic patterns. The model provides a robust framework for alerting operators to potential threats and guiding them on the necessary actions to maintain system integrity.

For instance, once a threat is identified, additional security measures such as Access List Control (ACL) [14] can be implemented to restrict access or isolate affected devices. Other complementary solutions include the use of Firewall-Based Access Control and Intrusion Prevention Systems (IPS) which could be considered in future developments to enhance the system's response capabilities.

It is important to note that our solution is primarily designed to detect and alert, rather than to automatically react to threats. This focus allows us to concentrate on developing an efficient and accurate detection mechanism. However, this leaves room for future work where we can explore integrating reaction mechanisms into our framework.

D. State of a Device:

The state of a device k at time t is denoted by a random variable $X(t)$. The transition probability p_{ij} is the probability of transitioning from state i to state j. This is defined as:

$$p_{ij} = \mathbb{P}(X_{t+1} = j | X_t = i)$$

Since the Markov chain is memory-less, we can write the transition probability as follows:

$$p_{ij} = \mathbb{P}(X_{t+1} = j | X_t = i, X_{t-1}, \ldots, X_0 = i_0)$$

E. Transition Probability:

The following $n \times n$ matrix represents the transition matrix of our stochastic system. The size of it is related to the cardinality of the state space (4 states in our case). Each entry of the matrix is the conditional probability of moving to state j given that the current state is i.

$$T = \begin{pmatrix} p_{NN} & p_{NAD} & \cdots & p_{NB} \\ p_{ADN} & p_{ADAD} & \cdots & p_{ADB} \\ \vdots & \vdots & \ddots & \vdots \\ p_{BN} & p_{BAD} & \cdots & p_{BB} \end{pmatrix}$$

The probability of each matrix entry for the device k is:

$$p_{k,ij} = p(x_k, t+1 = j | \cup_{k=1}^{n} x_{k,t} = i) = \frac{x_{ij}}{y_{ij}}$$

F. State Duration Distribution:

The state duration distribution H_i describes the time spent in each state before transitioning to another state, given by:

$$H_i = \sum_{j=0}^{n} I_{i,j} H_{i,j}$$

where $I_{i,j}$ is the probability function of the time $H_{i,j}$ spent in state i before transitioning to state j.

The transition probability matrix and state duration distribution enable us to model the dynamics of the semi-Markov process, providing a robust framework for predicting and mitigating DDoS attacks in maritime IoT environments.

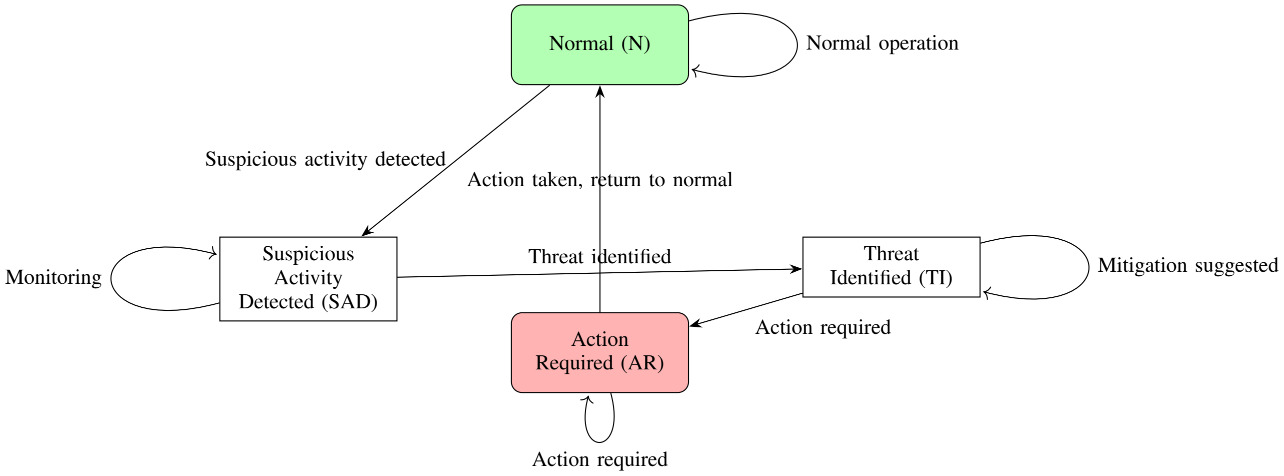

Fig. 3: State transition diagram for detecting DDoS attacks in a maritime IoT environment. Arrows indicate transitions based on detected conditions.

V. Simulation and Results

We validated our model in a controlled testbed that generated its own network logs under both normal maritime traffic conditions and injected DDoS scenarios, enabling precise assessment of detection accuracy. Under baseline operation established at 200 packets per millisecond, reflecting typical maritime patterns packet flows remained stable 4), preserving communication integrity. When we simulated a DDoS attack, traffic volumes spiked far beyond this threshold, immediately triggering the model's anomaly alarms and activating mitigation routines, thereby confirming the robustness and responsiveness of our detection mechanism against real world DDoS threats.

Upon simulating a DDoS attack, there was a significant increase in network traffic, with packet numbers drastically exceeding normal levels, indicating potential service disruptions as depicted in Figure 5. During the simulations, we generated the attack by sending an overwhelming number of packets, reaching up to 1,000 packets per millisecond. This extreme surge in traffic was designed to stress the network and observe its response under conditions far beyond normal operational thresholds.

We conducted two carefully crafted DDoS simulations against the NMEA2000 protocol maritime systems' core communication bus to rigorously stress test our detection model under realistic, high risk conditions because no public datasets met our needs, we generated synthetic traffic that let us tailor each scenario precisely and gauge the model's ability to spot and counter anomalous activity in a controlled yet representative maritime IoT environment.

Our predictive model demonstrated exceptional effectiveness in identifying and responding to these abnormal surges in network traffic. As depicted in Figure 6, the predicted attack patterns closely mirrored the actual DDoS data, showcasing the model's precision and reliability. This alignment underscores the robustness of our approach and highlights its potential as a valuable tool for safeguarding critical maritime communication protocols against evolving cyber threats.

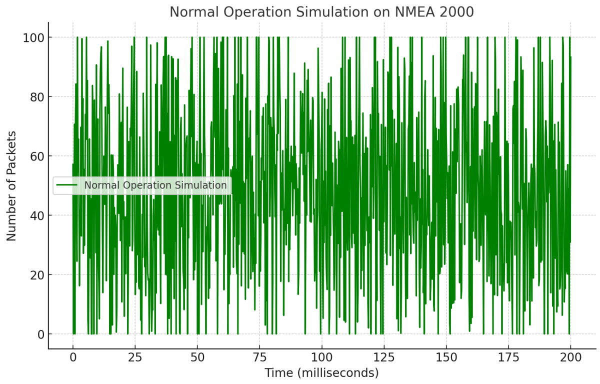

Fig. 4: Normal Operation of NMEA 2000: The figure demonstrates typical packet flow under normal conditions, highlighting the system's stability without external disruptions.

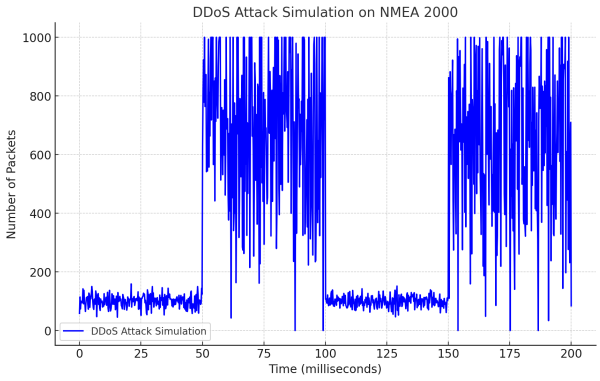

Fig. 5: DDoS attack on NMEA 2000.

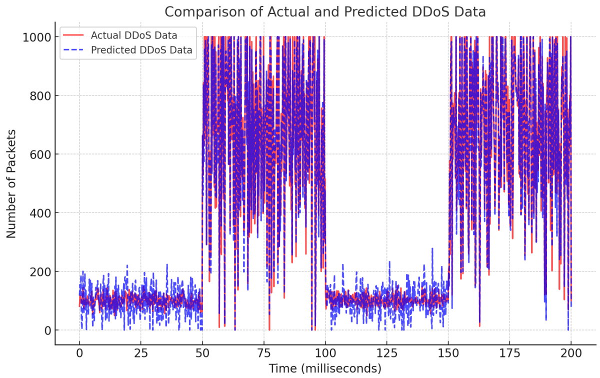

Fig. 6: Dynamic Response of Maritime IoT Systems to DDoS Threats: Real vs. Predicted Traffic Patterns Using the Advanced Markov Model.

Our advanced detection system showcases excellent performance metrics as demonstrated in the chart below. The high accuracy and detection rates confirm the effectiveness of our approach in identifying and mitigating potential threats. Furthermore, the extremely low error rate illustrates the precision of our model in classifying true threats versus normal behavior.

As shown in Figure 7, the system achieves an impressive accuracy rate of 98.5%, and an error rate that is almost negligible. These outstanding results underscore the robustness and reliability of our security model, making it a powerful tool in cybersecurity defenses.

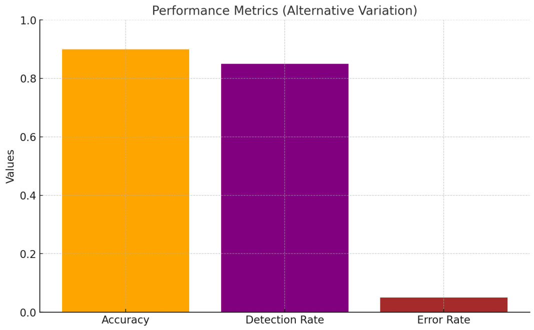

Fig. 7: Performance Metrics: This chart displays the accuracy, detection rate, and error rate of our system. The high accuracy and detection rate signify a robust capability in recognizing genuine threats, while the minimal error rate emphasizes the system's precision.

Our detection model already delivers impressive performance 98.5% overall accuracy with only three misclassifications in a 200 sample test set (confusion matrix [[99, 1], [2,98]]), confirming its strong precision and sensitivity yet its capabilities can be pushed further: by enriching the underlying Markov framework with additional states, we could monitor traffic at a finer granularity, spot subtler anomalies, and provide still tighter control over maritime IoT networks, ultimately elevating both security and reliability.

VI. Conclusion

This paper introduces a novel model based on stochastic semi-Markov processes to strengthen maritime IoT security, with a focus on the NMEA 2000 protocol. Comprehensive simulations demonstrated its effectiveness in detecting and mitigating Distributed Denial of Service (DDoS) attacks, essential for ensuring the reliability of maritime operations. Our model was tested under various scenarios, showcasing its ability to predict and block DDoS attacks with high accuracy while minimizing communication disruptions. These results highlight its potential as a robust solution for protecting critical maritime systems from advanced cyber threats. In conclusion, this model marks a significant step forward in maritime cybersecurity, offering a proactive and adaptive defense mechanism to address the growing challenges of cyber risks in maritime operations.

References

[1] J. Pavur, M. Strohmeier, V. Lenders, and I. Martinovic, "A tale of sea and sky: On the security of maritime vsat communications," in *SP 2020*, 2020. [Online]. Available: https://dblp.org/rec/conf/sp/PavurMSLM20

[2] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi, and A. Serhrouchni, "A reputation system for detection of black hole attack in vehicular networking," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*, 2015, pp. 1–5.

[3] D. Liu, L. Khoukhi, and A. Hafid, "Data offloading in mobile cloud computing: A markov decision process approach," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[4] ——, "Prediction-based mobile data offloading in mobile cloud computing," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4660–4673, 2018.

[5] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Fog-based distributed intrusion detection system against false metering attacks in smart grid," in *2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[6] N. Polatidis, M. Pavlidis, and H. Mouratidis, "Cyber-attack path discovery in a dynamic supply chain maritime risk management system," *Comput. Stand. Interfaces*, 2018. [Online]. Available: https://dblp.org/rec/journals/csi/PolatidisPM18

[7] D. Said, M. Elloumi, and L. Khoukhi, "Cyber-attack on p2p energy transaction between connected electric vehicles: A false data injection detection based machine learning model," *IEEE Access*, 2022. [Online]. Available: https://dblp.org/rec/journals/access/SaidEK22

[8] N. Kaminska, L. Kravtsova, H. Kravtsov, and T. Zaytseva, "Modeling ship cybersecurity using markov chains: an educational approach," in *CTE 2023*, 2023. [Online]. Available: https://dblp.org/rec/conf/cte/KaminskaKKZ23

[9] A. Selamnia, L. Khoukhi, M. Ayadi, and B. Ahmed, "Securing iiot against ddos attacks: A stochastic approach," in *GIIS 2024*, 2024.

[10] M. R. P. W. J. H. K. Rasmussen, "Detecting can attacks on j1939 and nmea 2000 networks," *IEEE TDSC*, 2023.

[11] N. S. B. S. O. M.-S. A. Fahad S. Alqurashi, Abderrahmen Trichili, "Maritime communications: A survey on enabling technologies, opportunities, and challenges," *Journal/Conference*, 2022. [Online]. Available: https://dblp.org/rec/journals/corr/abs-2204-12824

[12] Z. Jin, X. Ji, Y. Cheng, B. Yang, C. Yan, and W. Xu, "Pla-lidar: Physical laser attacks against lidar-based 3d object detection in autonomous vehicle," in *SP*, 2023. [Online]. Available: https://dblp.org/rec/conf/sp/JinJCYYX23

[13] N. Balemans, L. Hooft, P. Reiter, A. Anwar, J. Steckel, and S. Mercelis, "R2l-slam: Sensor fusion-driven slam using mmwave radar, lidar and deep neural networks," in *SENSORS*, 2023. [Online]. Available: https://dblp.org/rec/conf/ieeesensors/BalemansHRASM23

[14] J. Qian, "Acla: A framework for access control list (acl) analysis and optimization," in *Communications and Multimedia Security 2001*, 2001, accessed: 2024-08-15. [Online]. Available: https://dblp.org/rec/conf/cms/Qian01