Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2561–2571
DOI : 10.47974/JDMSC-2340

Exploring diverse network threats on cyber-physical systems

K. Rajendra Prasad *
Department of Computer Science and Engineering (Data Science)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

R. Raja Kumar †
Department of Computer Science and Engineering
Rajeev Gandhi Memorial College of Engineering and Technology
Neerawada, X Roads
Nandyal 518501
Andhra Pradesh
India

Sajja Suneel §
Department of Computer Science and Engineering (Data Science)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

Rajasekhar Nuvvusetty ‡
Department of Information Technology
Gokaraju Rangaraju Institute of Engineering and Technology
Nizampet
Hyderabad 500090
Telangana
India

This research was conducted during the NREUP at Michigan State University and it was sponsored by NSF grants DMS-1156582 and DMS-1359016.

* *E-mail:* krprgm@gmail.com (Corresponding Author)
† *E-mail:* rajakumar.rajaboina@gmail.com
§ *E-mail:* sajja.suneel@gmail.com
‡ *E-mail:* drnrajasekhar@gmail.com

Durgam Nishitha [@]
Department of Computer Science and Engineering (Cyber Security)
Institute of Aeronautical Engineering
Dundigal
Hyderabad 500043
Telangana
India

Abstract

Many essential infrastructures are built on Cyber-Physical Systems (CPS), which are complex systems that combine physical operations and computational components. Sensors, actuators, and control mechanisms that are man- aged by embedded computational and communication resources enable these systems to communicate with the real world in a range of applications, including smart grids, healthcare monitoring, transportation networks, and industrial automation. Because of their intrinsic interconnectedness and complexity, CPS are extremely vulnerable to different types of cyberattacks, which can negatively affect their dependability, security, and performance. Such attacks are common, which emphasizes how urgently we need sophisticated security solutions that can protect these essential systems. This study looks into the impact of simultaneous cyberattacks on CPS, investigating attack techniques such as remote hijacking, MitM attack, and DDoS, along with any possible repercussions. We assess how well the Sequential Monte Carlo Probability Hypothesis Density (SMCPHD) filter of the Random Finite Set (RFS) theory framework detects and mitigates these risks. By analyzing the time complexity and memory utilization of a parallel batch computing strategy in comparison to conventional sequential alternatives. The outcomes demonstrate significant decreases in processing time while maintaining effective memory use, providing a strong remedy for improving CPS security against several simultaneous attacks. One of the models to considers the quantity based on demand and investment in this research, compare the other model focus on realistic connection between the quantity, demand and the price.

Subject Classification: *94A60, 94A62.*

Keywords: *Cyber-physical systems (CPS), Random finite set theory (RFS), Distributed denial-of service (DDoS), Parallel batch computing, Mitigation strategies.*

1. Introduction

Modern technologies called Cyber-Physical systems (CPS) integrate physical and computational capabilities to allow for control, communication, and computation in the physical environment. Future

[@] *E-mail:* **nishithadurgam@gmail.com**

technological developments, such as driverless cars, advanced aircraft, hybrid cars, and brain-controlled prosthetics, depend on them. After being first presented by the (NASA) in 1992, the idea of CPSs was subsequently further developed by Khaitan and McCalley [1]. CPS Combining cyber physical and computer processes, these systems improve automation and efficiency across a range of industries, including transportation, smart grids, and industrial control. Actuators and sensors are used by CPS to continuously monitor and manage physical environments.[3]

These systems are susceptible to a variety of attacks, though. Individual assaults concentrate on taking advantage of specific weaknesses in the system. For example, phishing scams try to trick users into divulging personal information, while SQL injection attacks have the ability to damage web systems. numerous attacks, on the other hand, entail concerted efforts to concurrently compromise numerous system components or weaknesses [11]. Examples include Advanced Persistent Threats (APTs), which employ cunning techniques to gradually penetrate and compromise systems, and Distributed Denial of Service (DDoS) attacks, which overcome systems with excessive traffic. Both forms of attacks highlight the importance to safeguard CPS [12].

Cyber-Physical Systems (CPS) combine computing, communication, and control (3C) technologies to effectively monitor activities [2]. There are three main layers in the CPS framework. The sensors and actuators of the Physical Execution Layer gather data and carry out orders in order to interact with the environment directly. Reliable connection between computational systems and physical components is ensured by the data transmission layer [3]. Through a variety of apps, users can communicate with and control the CPS thanks to the services and functionalities provided by the Application Control Layer. For the smooth operation and integration of digital and physical processes in CPS, each layer is essential Fig 1. To detect multiple attacks combining parallel batch computing with Random Finite Set (RFS) theory's and the PHD filter (SMNP) significantly enhances the detection of numerous attacks in CPS. Real-time detection of several simultaneous threats like replay, data injection, and (DoS) attack, depends on this technique [18]. Because it estimates the quantity and states of numerous attacks without requiring the user to track each one individually, the SMC-PHD filter is especially well-suited for this task.

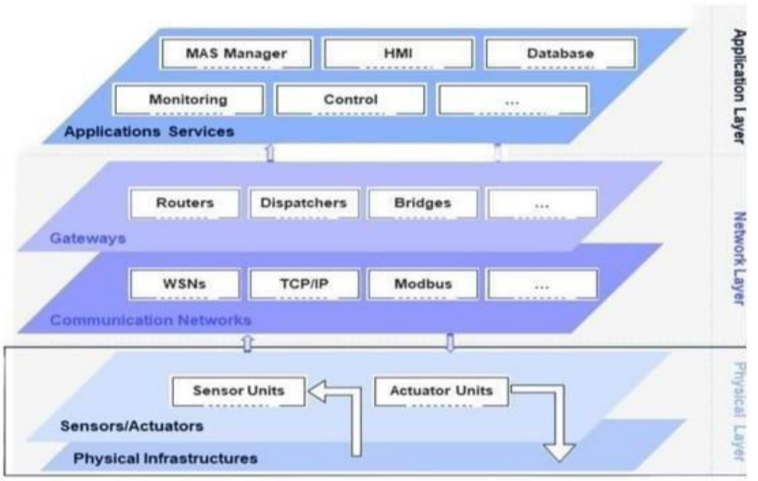

Figure 1

Architecture of cyber-physical system

This allows for a dynamic reaction to the unpredictable nature of attacks in CPS [4]. The efficient distribution of the computational burden among several processors made possible by parallel batch computing allows for the quick and scalable processing of massive data sets and sensor data. Figure 1. This effective combination ensures that CPS can efficiently monitor their environments, maintain optimal performance, and react quickly to various simultaneous threats, thereby improving security and resilience.

2. Categorization of Multiple Network Attacks

Cyber-Physical Systems (CPSs) are recognized to be susceptible to three distinct forms of network attacks: attacks which is an application control layer that take advantage of control software flaws, attacks on the data transmission layer that disrupt communication channels, and attacks based on the perception implementation layer that target sensors and actuators [19][20]. Every layer needs to be considered in order to ensure CPS security [5].

2.1 *Multiple Attacks on Perception Execution Layer*

Attackers can target the system's sensors and actuators by attacking the PE layer of Cyber Physical Systems (CPSs)—which are essential for

gathering data [15] and facilitating physical interactions [11]. These attacks can involve denial of service (DoS) attacks, which disrupt communication channels, actuator manipulation, which affects the physical components' operations, sensor tampering, which modifies the accuracy of environmental measurements, sensor spoofing, which introduces fraudulent data to mislead the system, and sensor data injection, which introduces fraudulent data to misguide system responses [9]. The dependability and safety of the CPS might be seriously impacted by any of these threats, which emphasizes the necessity of strong security measures to safeguard this vital layer.

2.2 *Multiple Attacks on Data Transmission Layer*

Cyber-Physical Systems (CPSs) are becoming more and more susceptible to a variety of attacks on their data transmission layer, which aim to compromise or disrupt the channels used for exchanging data between system components. These attacks can be of several types: Denial of Service (DoS) attacks [14][17], which inject malicious or false data into the communication stream to undermine the integrity and reliability of the transmitted data; jamming attacks, which purposefully interfere with communication signals to cause transmission interruptions and possibly the loss of important data; and (MitM) attack, which intercept and possibly modify communications between system components, thereby posing a threat to the confidentiality, integrity, and performance of the system[9] [11]. These types of attacks provide substantial challenges to the security and stability of CPSs, underlining the necessity for effective defense measures to maintain dependable and secure data transfer.

2.3 *Multiple Attacks on Application Control Layer*

Vulnerability exploitation involves the use of control software flaws by attackers to manipulate or disrupt system operations. Privilege escalation involves the insertion of malicious software to escalate access or control beyond what was intended. Malware infections involve the introduction of harmful software to compromise system integrity. Configuration manipulation involves the alteration of system settings by attackers to cause improper behavior or security breaches [5][9]. These assaults have the potential to seriously impair the CPS's stability, security, and operation, underscoring the necessity of putting strong security measures in place to safeguard the application control.

3. Detecting Multiple Attacks with Parallel Batch Computing and SMCPHD in RFS

Cyber-Physical Systems (CPS) may detect several simultaneous attacks with great effectiveness when the (SMCPHD) filter is used with Parallel Batch Computing. This approach efficiently handles uncertainty and dynamic interactions between various threats by employing the Random Finite Set (RFS) theory. The core filter processes of sampling, prediction, updating, and resampling are accelerated by parallel batch computing, improving real-time performance and scalability [8]. Together, they provide reliable, effective detection and reaction to dynamic cyberthreats in intricate contexts.

3.1 *Parallel Batch Computing in RFS Using SMCPHD Filter*

Sequential batch computing approaches and parallel batch computing approaches have different performance characteristics in the field of multiple attack detection. When working with huge datasets or sophisticated computations, sequential batch computing can result in increased delay and decreased throughput as tasks are processed one after the other. Even though this method is easier to administer and put into practice, it could not be scalable when the need for computational power increases [10].

3.2 *Algorithm for SMCPHD Filter for Detection of Multiple Attacks*

Optimized SMCPHD Filter for Multiple Attacks Detection with Parallel Computing algorithm

1: Initialize: L, {xi_0, wi_0} for all i in L
2: for k = 1, 2, ... do
3: Method 1: Sampling (Parallelized)
4: Generate xi_k for i = 1 to Ik-1 in parallel using qk (xi_k | xi_k-1, k)
5: Generate xi_k for i = Ik-1+1 to Ik-1+Jk in parallel using pk (xi_k | k)
6: Method 2: Prediction (Parallelized)
7: Compute wi_k|k-1 = psfk|k-1 * wi_k-1 / qk (xi_k | xi_k-1, k) for i = 1 to Ik-1 in parallel
8: Compute wk|k-1 = γk(xi_k) * Jk * pk (xi_k | k) for i = Ik-1+1 to Ik-1+Jk in parallel
9: Method 3: Update (Parallelized)

10: Compute wi_k for i = 1 to Ik-1+Jk in parallel

11: Method 4: Resampling

12: Compute total_weight = sum of wi_k for i = 1 to Ik-1+Jk

13: Normalize weights w(i)_k = wi_k / total_weight for i = 1 to Ik-1+Jk in parallel

14: Apply resampling algorithm in parallel to obtain {˜ xi_k, ˜ wi_k} for i = 1 to Ik1+Jk

15: Compute rescaled weights ˜ wi_k = ˆnk * ˜ wi_k for all i = 1 to Ik-1+Jk in parallel

16: Update {xi_k, wi_k} = {˜ xi_k, ˜ wi_k} for all i = 1 to Ik-1+Jk 17: end for

4. Time Complexity of Parallel Batch Computing in RFS

Parallel computing greatly reduces the temporal complexity of the Optimized SMCPHD Filter for multiple attack detection. Because all of the main operations— sampling, prediction, updating, and resampling—are carried out concurrently, the time complexity of O(PIk−1+Jk) every iteration, where number of processors are P and Ik−1+Jk is the total number of particles. O(K.PIk−1+Jk) is the total time complexity for K iterations, indicating effective and scalable performance for actual time attack detection in (CPS) [10].

For the purpose of detecting numerous attacks, the Optimized SMCPHD Filter with Parallel Batch Computing has an overall time complexity of O (K. P/ N)[13]. The efficiency improvements from parallelizing the filter's operations are reflected in this complexity, which enables faster computation and scalability in real-time scenarios.

The SMCPHD Filter for Multiple Attacks Detection [16] (sequential version) has an overall time complexity of O (K. (I k−1+J /k)), where number of iterations are K and N is the total number of particles [7]. As the number of particles rises, this sequential technique becomes slower since it processes each particle individually.

4.1 *Evaluation of Parallel Batch Computing's Performance for Computing DDoS Attack Mitigation*

In this study, we examine the effectiveness of employing parallel batch computing techniques in conjunction with the hping3 tool to mitigate SYN Flood (DDoS) attacks. One prevalent and severe type of (DoS) assault is the SYN flood threat, in which an attacker floods a target

web server with SYN packets in an attempt to deplete its resources and force valid requests to be dropped. In our experiment, we used hping3 to simulate a SYN Flood DDoS attack, which entailed transmitting 2,771,276 packets over a 52.8-minute period. We used parallel batch computing, dividing the workload across 100 processors(assumption), to evaluate the effect of parallel processing. It took 52.8 minutes to process every packet sequentially, which could cause delays in the detection and mitigation of attacks [6] (Figure 2). On the other hand, the processing time was greatly

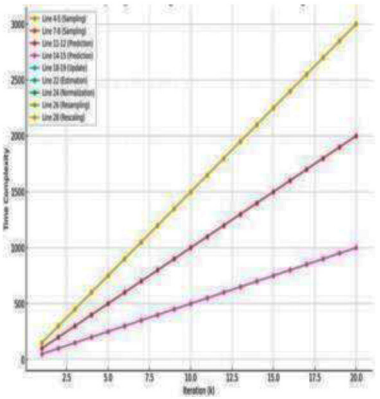

Figure 2

Sequential Time Stamp

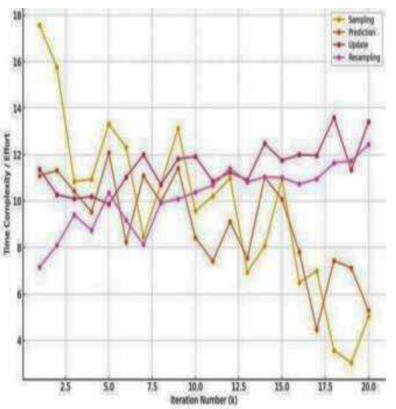

Figure 3

Parallel Time Stamp

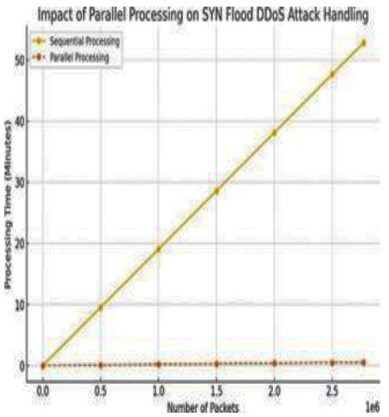

Figure 4

Memory Utilization

shortened to about 0.528 minutes using parallel batch computing. This significant decrease highlights how parallel processing (Figure 3) may quickly mitigate attacks. The system can handle high packet quantities more effectively by utilizing several processors (Figure 4), which improves web servers' resistance to DDoS attacks. This investigation demonstrates how parallel computing significantly enhances real time replies and overall efficacy of cybersecurity in conditions with high assault volume [6] [4].

5. Discussion and Conclusion

Adaptive algorithms that can react dynamically to different attack intensities and patterns can improve the filter's capacity to handle evolving cyberthreats. More reliable detection capabilities and prediction insights into possible attack vectors may be obtained by looking at combining machine learning and artificial intelligence with the SMCPHD filter. Finally, to evaluate this approach's actual applicability and improve its efficacy in operational settings, real world case studies and pilot implementations in various CPS situations would be beneficial.

In conclusion, this research shows that the (SMCPHD) filter, when combined with parallel batch computing, can effectively detect and mitigate many concurrent attacks on Cyber Physical Systems (CPS). By spreading the computational load across several processors, parallel batch computing significantly shortens the processing time for attack detection. Our results show a significant improvement in real-time threat mitigation, with the parallel technique able to reduce processing time from 52.8 minutes (sequential) to roughly 0.528 minutes. The system can react to high-volume attacks like SYN Flood DDoS attacks more quickly due to this processing time decrease, which raises CPS's overall security and resilience. The complexity is efficiently managed by the parallelized SMCPHD filter.

References

[1] Siddhartha Kumar Khaitan and James D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Systems Journal*, vol. 9, no. 2, pp. 350–365 (2014).

[2] Edward A. Lee, "Cyber physical systems: Design challenges," in Proc. 11th IEEE Int. Symp. on Object and Component-Oriented Real-Time Distributed Computing *(ISORC)*, *IEEE*, pp. 363–369 (2008).

[3] Liwei Cao, Xiaoning Jiang, Yumei Zhao, Shouguang Wang, Dan You, and Xianli Xu, "A survey of network attacks on cyber-physical systems," *IEEE Access*, vol. 8, pp. 44219–44227 (2020).

[4] Chaoqun Yang, Zhiguo Shi, Heng Zhang, Junfeng Wu, and Xiufang Shi, "Multiple attacks detection in cyber-physical systems using random finite set theory," *IEEE Transactions on Cybernetics*, vol. 50, no. 9, pp. 4066–4075 (2019).

[5] Tao Lu, Bo Xu, Xiaoqiang Guo, Liang Zhao, and Fei Xie, "A new multilevel framework for cyber-physical system security," in *Proc. 1st Int. Workshop Swarm Edge Cloud*, pp. 12 (2013).

[6] Yisroel Mirsky, Tomer Doitshman, Yuval Elovici, and Asaf Shabtai, "Kitsune: an ensemble of autoencoders for online network intrusion detection," arXiv preprint arXiv:1802.09089 (2018).

[7] Branko Ristic, Michael Beard, and Claudio Fantacci, "An overview of particle methods for random finite set models," *Information Fusion*, vol. 31, pp. 110–126, 2016.

[8] Tiancheng Li, Shudong Sun, Miodrag Bolić, and Juan M. Corchado, "Algorithm design for parallel implementation of the SMC-PHD filter," *Signal Processing*, vol. 119, pp. 115–127 (2016).

[9] Filipe Januário, António Cardoso, and Pedro Gil, "A distributed multi-agent framework for resilience enhancement in cyber physical systems," *IEEE Access*, vol. 7, pp. 31342–31357 (2019).

[10] [Duplicate of 4] Chaoqun Yang, Zhiguo Shi, Heng Zhang, Junfeng Wu, and Xiufang Shi, "Multiple attacks detection in cyber-physical systems using random finite set theory," *IEEE Transactions on Cybernetics*, vol. 50, no. 9, pp. 4066–4075 (2019).

[11] Sangjun Kim, Kyung-Joon Park, and Chenyang Lu, "A survey on network security for cyber–physical systems: From threats to resilient design," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1534–1573 (2022).

[12] [Duplicate of 11] Sangjun Kim, Kyung-Joon Park, and Chenyang Lu, "A survey on network security for cyber–physical systems: From threats to resilient design," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1534–1573 (2022).

[13] Yosef Ashibani and Qusay H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Computers & Security*, vol. 68, pp. 81–97 (2017).

[14] Rajendra Prasad, "An extended fuzzy C-means segmentation for an efficient BTD with the region of interest of SCP," *International Journal of Information Technology Project Management (IJITPM)*, vol. 12, no. 4, pp. 11–24 (2021).

[15] K. R. Prasad, G. R. Kamatam, M. B. Myneni, and N. R. Reddy, "A novel data visualization method for the effective assessment of cluster tendency through the dark blocks image pattern analysis," *Microprocessors and Microsystems*, vol. 93, 104625 (2022).

[16] Ganga Rama Koteswara Rao, Hayder M. A. Ghanimi, V. Ramachandran, Dokhyl Al-Qahtani, Pankaj Dadheech, and Sudhakar Sengan, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 27, no. 2-A, pp. 361–370 (2024).

[17] Prudviraj Jeripothula, Chalavadi Vishnu, and C. Krishna Mohan, "AAP-MIT: Attentive Atrous Pyramid Network and Memory Incorporated Transformer for Multi-Sentence Video Description," *IEEE Transactions on Image Processing* (2022), doi: 10.1109/TIP.2022.3195643.

[18] Ankit Kumar, Pankaj Dadheech, Vijander Singh, Linesh Raja, and Ramesh C. Poonia, "An enhanced quantum key distribution protocol for security authentication," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 499–507 (2019).

[19] D. Rajassekharan, V. Ramachandran, D. K. Sharma, T. Palanisamy, Y. V. Myilsamy, and R. C. Poonia, "An efficient wireless sensor network based intrusion detection system," in 2023 Int. Conf. on Communication, Security and Artificial Intelligence (ICCSAI), IEEE, pp. 444–449, doi: 10.1109/ICCSAI59793.2023.10421537.

[20] B. Prabha, M. Yaramadhi, A. Sharma, and K. Padmanaban, "Optimized auxiliary physics neural network based multi-target detection for edge-cloud in smart internet of things," *Peer-to-Peer Networking and Applications*, vol. 18, no. 2, pp. 1–21 (2025).

Received March, 2024