ISSN 2394-739X

IJRSET AUGUST Volume 10 Issue 8

International Journal for Research in Science Engineering & Technology (IJRSET)

https://www.doi.org/10.5281/zenodo.8323712

DEVELOPING AN ADAPTIVE AND PROACTIVE CYBERSECURITY DEFENSE MECHANISM (APCDM) USING DEEP REINFORCEMENT LEARNING IN WSN

[1] Dr. S. Rajeshwari,
[1] Assistant Professor, Department of Computer Science,
[1] Hindusthan College of Arts & Science,
[1] TamilNadu, India.

ABSTRACT - In the domain of Wireless Sensor Networks (WSNs), where resources are limited and dynamic threats persist, there's a growing requirement for cybersecurity defenses that can adapt and act ahead of time. This research introduces an innovative strategy to tackle this challenge by harnessing the capabilities of Deep Reinforcement Learning (DRL). The study proposes an original method for an Adaptive and Proactive Cyber security Defense Mechanism (APCDM) utilizing Deep Reinforcement Learning within WSNs. The approach entails constructing a simulated cybersecurity environment that accurately imitates real-world threats and network behaviors, allowing for the training and assessment of a DRL agent. This agent engages with the environment, acquiring optimal defensive strategies through advanced DRL algorithms such as Advantage Actor-Critic (A2C) or Trust Region Policy Optimization (TRPO). The agent's goal is steered by a meticulously crafted reward system that encourages actions minimizing vulnerabilities and effectively countering attacks. The resulting mechanism represents a notable advancement in WSN cybersecurity, providing an automated, adaptable, and forward-looking approach to protecting these networks against an ever-changing landscape of threats.

Keywords: [Wireless Sensor Networks, cyber security, Deep Reinforcement Learning, agent.]

1. INTRODUCTION

Wireless Sensor Networks (WSNs) have found extensive practical use in diverse applications, such as forest fire monitoring, military detection, medical and scientific research, and even within our homes. However, WSNs face significant security challenges due to their use of broadcast communication and lack of tamper resistance. This vulnerability allows attackers to eavesdrop on communication, inject malicious packets, replay old messages, or compromise sensor nodes. The primary security concerns for sensor nodes are privacy preservation and node authentication. Privacy entails maintaining data confidentiality through security measures, ensuring secure network communication between sensor nodes and the central station. Meanwhile, a robust authentication mechanism prevents unauthorized nodes from deceitfully joining the network and accessing sensitive information. Consequently, numerous methods have been proposed to enhance communication security within WSNs.

The cybersecurity of Wireless Sensor Networks (WSNs) holds utmost significance due to their distinct characteristics and vulnerabilities. WSNs comprise numerous small, resource-limited sensor nodes that communicate wirelessly, collecting and transmitting data from the physical environment. These networks serve various domains, including environmental monitoring, industrial automation, healthcare, agriculture, and more. However, their inherent characteristics make them susceptible to cybersecurity threats:

Resource Constraints: Sensor nodes in WSNs are typically resource-constrained in terms of processing power, memory, energy, and communication bandwidth. This limitation affects the implementation of complex security mechanisms, making it challenging to ensure strong protection against attacks.

Limited Communication Range: The communication range of sensor nodes is often limited, which makes it necessary to relay data through intermediate nodes. This introduces additional opportunities for attackers to intercept or manipulate data during transmission.

Distributed Nature: WSNs are distributed systems with no centralized control makes it difficult to implement traditional security solutions that rely on centralized authentication and access control.

Unattended Deployment: WSNs are often deployed in remote or hostile environments where physical access control is not possible. This exposes sensor nodes to physical attacks and unauthorized tampering.

Wireless Communication: Wireless communication introduces vulnerabilities such as eavesdropping, jamming, and spoofing. Attackers can intercept sensitive data or disrupt communication, affecting the integrity and availability of the network.

Limited Battery Life: Sensor nodes are typically powered by batteries with limited energy capacity. Energy-efficient security mechanisms are crucial to avoid excessive energy

consumption, which could lead to nodes running out of power prematurely.

Data Aggregation: WSNs often aggregate data from multiple nodes before forwarding it to the sink node or base station. Malicious nodes can inject false data or tamper with aggregated data, leading to inaccurate analysis and decisions.

Authentication confirms the identity of a participant in a sensor network. Integrity ensures data remains unaltered or undestroyed without authorization. Data integrity assures sensor data remains unmodified during transmission, processing, or storage. Trustworthiness prevents unauthorized access to data. Protected sensor network data includes indirect information accessed through transmission or monitoring processes.

2. LITERATURE SURVEY

Perrig and Tygar proposed several secure broadcast schemes suitable for wireless sensor networks. Their methods incur reasonable computational costs for small sensor motes. They introduced a hashed key-chain approach for generating encryption/decryption keys in sequence for sensor motes, all without alerting other devices.

Ye et al. proposed a detection scheme called SEF: Statistical En-route Filtering (SEF) is a method for identifying injected false data during transmission. It enables both the base station and nodes along the route to identify false data with certain likelihood. SEF capitalizes on the extensive and closely spaced deployment of sensor networks to ascertain the accuracy of each report through joint decision-making by numerous detecting nodes. Additionally, it enables multiple forwarding nodes to collectively identify false reports..

Turkanović et al. proposed a novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks. The plan facilitates a remote user in securely establishing a session key with a generic sensor node through a lightweight key agreement protocol. This method guarantees mutual authentication among the user, sensor node, and gateway node (GWN), even without direct user-GWN communication. The approach has been tailored to suit the resource-limited design of the WSN. As a result, it relies solely on uncomplicated hash and XOR calculations.

Amin and Biswas designed a novel architecture for the WSN environment, a approach has been introduced for user authentication and key agreement, addressing the previously mentioned security issues. This method rectifies the identified vulnerabilities while also incorporating BAN logic to validate its security. By leveraging this logic, the protocol achieves secure mutual authentication and session key agreement among the participating entities. Apart from mitigating the previously outlined security flaws, this proposed protocol fulfills comprehensive security prerequisites. Notably, it ensures energy efficiency, user anonymity, mutual authentication, and a convenient user-friendly password change process.

Cam et al. proposed a secure energy-efficient data aggregation (ESPDA) to prevent redundant data transmission in data aggregation. Their approach differs from traditional techniques in that it prevents duplicate transmissions from sensor motes to the aggregator. Before sending detected data, every sensor communicates a protected example to the aggregator. This solid example is created by connecting unique information with an irregular number. Instead of transmitting the actual "real" data, the sensor mote sends the secure pattern to the cluster-head before transmitting anything else. These safe patterns are then used by the cluster-head to recognize sensors that have identical readings. Subsequently, the cluster-head instructs specific sensor motes to proceed with transmitting their actual data. Only sensors with distinct data are permitted to forward their information to the cluster-head. However, due to the necessity of each sensor to transmit a packet containing a pattern at least once, there is a limitation to power conservation. Furthermore, each sensor mote employs a consistent encryption key for encrypting data, which implies that data privacy cannot be adequately preserved within their proposed scheme.

Othman, S. B., Trad, A., Youssef, H., & Alzaid, H. (2013) introduce a novel way to provide confidential and integrity preserving aggregation in wireless sensor networks. The proposed method employs homomorphic encryption, specifically the ECEG (Elliptic Curve ElGamal) algorithm, to ensure data confidentiality while enabling in-network aggregation. Additionally, a homomorphic MAC algorithm derived from Message Authentication Codes is utilized to guarantee the integrity of the aggregated data. The conservation of energy is a fundamental objective in designing communication protocols for Wireless Sensor Networks, given the limited energy capacity of sensor batteries and the impracticality of frequent replacements. Notably, over 70% of energy is consumed by transmissions in WSNs. Thus, data aggregation holds the potential to significantly diminish energy consumption since a considerable portion of the sensed data is redundant due to the proximity of sensors. However, security stands as another imperative consideration in the formulation of communication protocols for WSNs. Regrettably, while aggregation reduces redundancy, leading to energy savings; it complicates the process of verifying data integrity as the received data becomes singular. Addressing this, a novel approach is introduced, employing homomorphic encryption alongside Message Authentication Codes (MAC) to achieve confidentiality, authentication, and integrity in secure data aggregation for wireless sensor networks.

Jilani, S. A., Koner, C., & Nandi, S. (2020) proposed a novel detection algorithm, ready to identify intrusions in real time scenarios progressively situations. The required detection system must possess resilience and ensure consistent monitoring at both the system and host levels. This capability empowers users to identify emerging issues promptly, granting them the capacity to thwart attacks proactively. Once more, establishing dependable security within Wireless Sensor Networks remains an expansive realm of research. Numerous researchers have presented their contributions to enhancing security in Wireless Sensor Networks, yet energy consumption remains a persistent challenge. Another facet of ensuring security involves the implementation of a shared key mechanism.

3. PROPOSED METHODOLOGY

The proposed approach aims to establish an intelligent cybersecurity defense system using Deep Reinforcement Learning (DRL), which is a widely used technique for enhancing security. In this study, we introduce the Adaptive and Proactive Cybersecurity Defense Mechanism (APCDM) through the application of Deep Reinforcement Learning within Wireless Sensor Networks (WSN). The initial step involves creating a simulated environment mirroring real-world cyber threats and vulnerabilities. Subsequently, an intelligent agent is developed to interact within this environment. By employing DRL algorithms like A2C or TRPO, the agent learns effective defense strategies. These strategies are guided by a carefully designed reward structure aligned with system security objectives, such as threat prevention and vulnerability reduction. The process encompasses agent training across multiple episodes, potentially using genuine or artificially generated data. It also involves refining hyperparameters and assessing performance using metrics like attack detection rate and response time. To ensure practicality, the methodology considers its applicability to real systems. Furthermore, it explores the integration of adversarial training methods to bolster resilience.

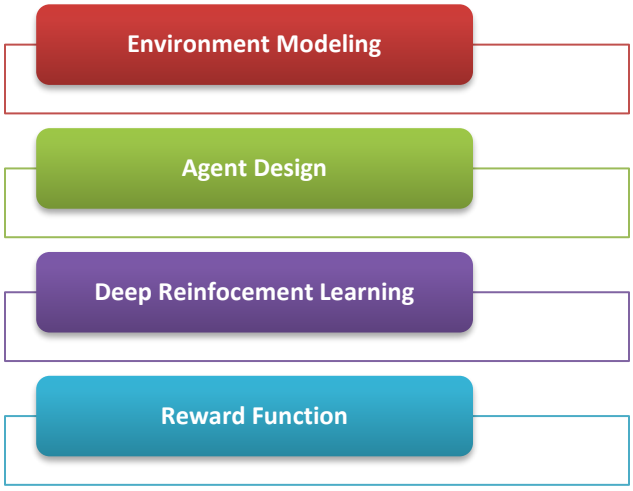

Figure 1.Workflow of the proposed method

Deep Reinforcement Learning (DRL) constitutes an AI and machine learning subset that merges deep learning methods with reinforcement learning principles. This fusion empowers agents to grasp intricate and ever-changing environments, learning and deciding optimally. DRL's essence lies in teaching agents to select actions within an environment, aiming to maximize the cumulative reward signal across durations.

Components of Deep Reinforcement Learning (DRL):

Agent: The agent is an entity that interacts with an environment. It observes the current state of the environment, selects actions, and receives feedback in the form of rewards. The agent's objective is to learn a policy—a strategy that maps states to actions—to maximize the total expected reward over its lifetime.

Environment: The environment represents the external system with which the agent interacts. It provides feedback to the agent based on its actions and the current state. The environment can range from simple simulations to complex real-world systems.

State: A state is a representation of the environment's current situation. It encapsulates all relevant information that the agent needs to make decisions.

Action: An action is a decision made by the agent based on its current state. The agent's goal is to learn the best actions to take in different states to achieve its objectives.

Reward: A reward is a scalar feedback signal that the agent receives from the environment after taking an action in a specific state. It indicates how favorable or unfavorable the action was in achieving the agent's goals.

Policy: The policy is the strategy that the agent uses to select actions based on the observed states. It can be deterministic or stochastic, and the goal of the agent is to learn an optimal policy that maximizes the expected cumulative reward.

Value Function: The value function estimates the expected cumulative reward that an agent can achieve from a specific state while following a given policy. It helps the agent assess the desirability of different states.

DRL leverages deep neural networks to approximate complex policies and value functions, allowing agents to learn from high-dimensional and continuous state spaces. The agent improves its decision-making abilities through iterative learning, where it explores the environment, observes outcomes, and adjusts its policy to increase the total expected reward.

Algorithm: DRL-Based Cyber security Defense in WSN

Step 1: Start the process
Step 2: Create a simulated environment to mimic real-world cyber threats and vulnerabilities.
Step 3: Design an intelligent agent to interact with the simulated environment.
Step 4: Define agent's observations (states) and actions.
Step 5: Initialize neural networks for policy and value functions.
Step 6: Choose DRL algorithm (e.g., A2C or TRPO).
Step 7: Loop over episodes:
Step 8: Reset environment.
Step 9: Loop over timesteps:
Step 10: Observe state, choose action.
Step 11: Execute action, receive reward and new state.
Step 12: Update agent's networks using DRL algorithm's rules.
Step 13: Design reward function guiding agent's behavior based on security goals.
Step 14: Train agent using experiences from Step 4.
Step 15: Monitor learning progress and metrics (e.g., cumulative reward).
Step 16: Evaluate agent's performance in the simulated environment.
Step 17: End the process.

ISSN 2394-739X
IJRSET AUGUST Volume 10 Issue 8

4. EXPERIMENTAL RESULTS

4.1 Packet Delivery Ratio (PDR)

No of Nodes	SEF	ESPDA	Proposed APCDM
100	60	72	81
200	62	73	82
300	66	75	84
400	72	78	87
500	75	82	94

Table 1.Comparison Table of Packet Delivery Ratio (PDR)

The comparison table 1 of Packet Delivery Ratio (PDR) addressed the different values of existing (SEF, ESPDA) and Proposed APCDM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 60 to 75 and 72 to 82 and Proposed APCDM values start from 81 to 94. The Proposed APCDM gives the best result.

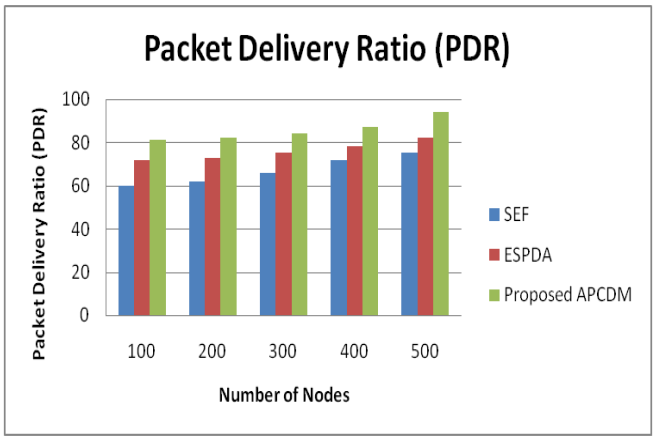

Figure 4.Comparison chart of Packet Delivery Ratio (PDR)

The figure 4 data Packet Delivery Ratio (PDR) describes the different values of existing (SEF, ESPDA) and Proposed APCDM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Packet Delivery Ratio (PDR) in Y axis. The existing values start from 60 to 75 and 72 to 82 and Proposed APCDM values start from 81 to 94. The Proposed APCDM gives the best result.

4.2 Overhead

No of Nodes	SEF	ESPDA	Proposed APCDM
100	56	43	32
200	66	63	54
300	74	78	65
400	87	81	71
500	93	85	67

Table 3.Comparison Table of Overhead

The comparison table 3 of Overhead describes the different values of existing (SEF, ESPDA) and Proposed APCDM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 56 to 93 and 43 to 85 and Proposed APCDM values start from 32 to 73. The Proposed APCDM gives the best result.

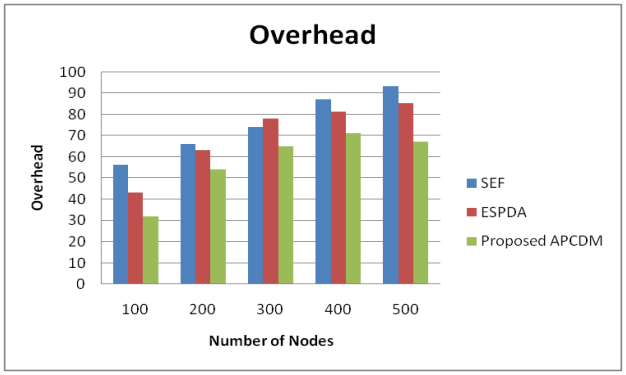

Figure 6.Comparison Chart of Overhead

The figure 6 overhead describes the different values of existing (SEF, ESPDA) and Proposed APCDM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and overhead in Y axis. The existing values start from 56 to 93 and 43 to 85 and Proposed APCDM values start from 32 to 73. The Proposed APCDM gives the best result.

4.3 Response Time

No of Nodes	SEF	ESPDA	Proposed APCDM
100	70	63	52
200	74	65	54
300	77	68	61
400	84	73	64
500	90	80	70

Table 2.Comparison Table of Response Time

The comparison table 2 of Response Time describes the different values of existing (SEF, ESPDA) and Proposed APCDM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 52 to 70, 63 to 80 and the Proposed APCDM values start from 70 to 90. The Proposed APCDM gives the best result.

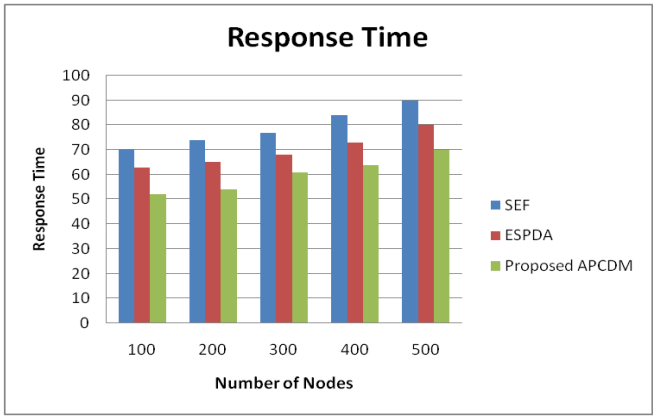

Figure 5.Comparison Chart of Response Time

The figure 5 Response Time describes the different values of existing (SEF, ESPDA) and Proposed APCDM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Response Time in Y axis. The existing values start from 52 to 70, 63 to 80 and Proposed APCDM values start from 70 to 90. The Proposed APCDM gives the best result.

CONCLUSION

The advancement of an Adaptive and Proactive Cyber security Defense Mechanism (APCDM) using Deep Reinforcement Learning (DRL) signifies a notable progress in enhancing the security of Wireless Sensor Networks (WSNs). This proposed approach harnesses the capabilities of DRL to craft a smart agent capable of acquiring and adapting defense strategies in dynamic and resource-limited WSN conditions. By emulating real-world cyber threats, vulnerabilities, and network actions, the system provides a secure experimentation environment for training and evaluating the DRL-based defense strategy. The agent's skill in foreseeing attack patterns and modifying responses, guided by a thoughtfully constructed reward system, highlights its potential to reduce risks and boost system resilience. As cybersecurity obstacles develop, this innovation unveils opportunities for flexible, self-governing, and proactive defense solutions that are well-prepared to safeguard WSNs against an ever-evolving threat panorama. Through consistent validation, enhancement, and real-world implementation, the fusion of DRL and cybersecurity in WSNs holds the potential to mold the future of network security with intelligent and adaptable approaches. DRL employs deep neural networks to approximate intricate policies and value functions, allowing agents to learn from complex and continuous state spaces. The agent enhances its decision-making process through incremental learning, where it explores the environment, observes consequences, and adjusts its policy to amplify the overall anticipated reward.

REFERENCES

[1]. Ahmed, K.A. Bakar, M.I. Channa, and A.W. Khan, “A secure routing protocol with trust and energy awareness for wireless sensor network”, Mobile Networks and Applications, vol. 21, no. 2, pp. 272-285, Jan. 2016.

[2]. Dey, S. Nandi, M. Sarkar, “Security Measures in IOT based 5G Networks”, In Proceedings of the International Conference on Inventive Computation Technologies, pp. 561- 566, 2018.

[3]. Wahid and P. Kumar, “A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network”, International Journal for Innovative Research in Science and Technology, vol. 1, no. 8, pp.189-196, Jan. 2015.

[4]. Amin, R.; Biswas, G.P. A secure light weight scheme for user authentication and key agreement in multigateway based wireless sensor networks. Ad Hoc Netw. 2016, 36, 58–80.

[5]. Beer, F., & Bühler, U., “Feature selection for flow-based intrusion detection using Rough Set Theory”, International Conference on Networking, Sensing and Control (ICNSC), IEEE, 2017.

[6]. Cam, H., Ozdemir, S., Nair, P., Muthuavinashinappan, D., & Ozgur Sanli, H. ESPDA: Energy-efficient secure pattern based data aggregation for wireless sensor networks. Computer Communication, 29, (2006). 446–455.

[7]. Chen, T.H.; Shih, W.K. A Robust Mutual Authentication Protocol for Wireless Sensor Networks. ETRI J. 2010, 32, 704–712.

[8]. Junqing Zhang, Trung Q. Duong, Roger Woods and Alan Marshall, “Securing Wireless Communications of the Internet of Things from the Physical Layer”, MDPI Publication, 2017.

[9]. K. Chelli, “Security issues in wireless sensor networks: Attacks and countermeasures”, In Proceedings of the World Congress on Engineering, vol. 1, no. 20, pp. 876-3423, 2015.

[10]. Rohini Anand Nimbekar, “Wireless Sensor Networking in the Internet of Things”, International Advanced Research Journal in Science, Engineering and Technology, vol. 4, issue 2, 2017.

[11]. Salehi, S., Razzaque, Mohammad Abdur, Naraei, Parisa & Farrokhtala, Ali, “Security in Wireless Sensor Networks: Issues and challenges”, International Conference on Space Science and Communication, IconSpace. pp.356-360, 2013.

[12]. Turkanovic, M.; Brumen, B.; Hölbl, M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Netw. 2014, 20, 96–112.

[13]. V. Pahune, and S. Khode, “Security issues, attacks and challenges in Wireless Sensor Network”, IJESRT, vol. 4, no. 6, pp.56-87, Jun. 2015.

[14]. Wong, K.H.M.; Zheng, Y.; Cao, J.; Wang, S. A Dynamic User Authentication Scheme for Wireless Sensor Networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Taichung, Taiwan, 5–7 June 2006; pp. 244–251.

[15]. Yeh, H.-L.; Chen, T.-H.; Liu, P.-C.; Kim, T.-H.; Wei, H.-W. A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. Sensors 2011, 11, 4767–4779.