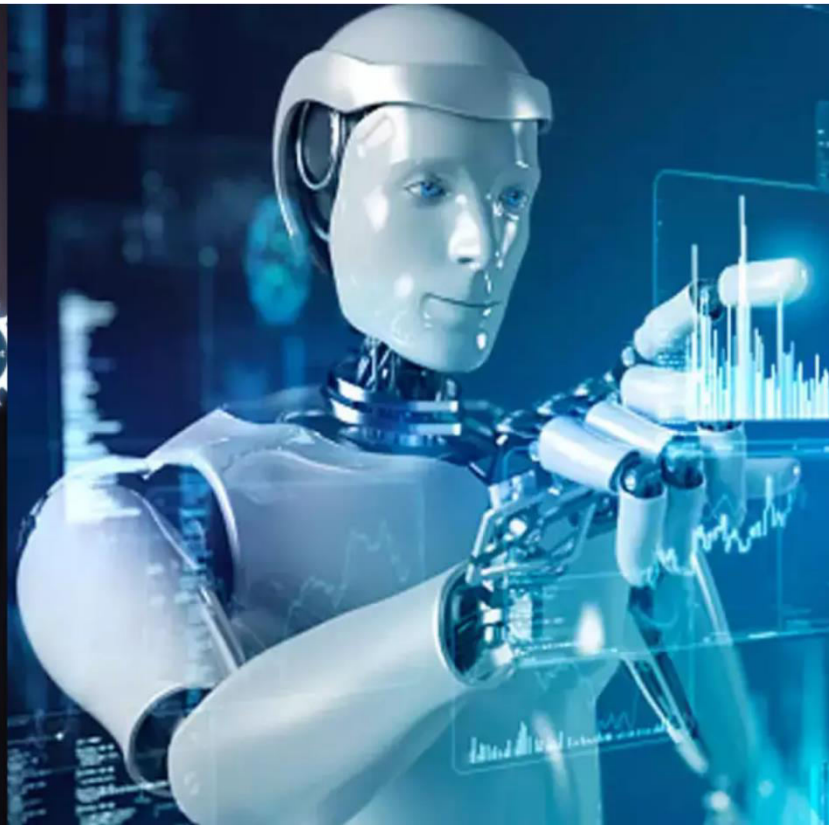
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403053|

SDN-Guard: Reinforcement Learning-based Anomaly Detection and Adaptive Defense Algorithm for Secure Software-Defined Networks

Ms.Geetha.M[1], Dr.P.Suresh Babu[2]

Research Scholar, Department of Computer Science, Bharathidasan College of Arts and Science, Erode, Tamil Nadu, India[1]

Associate Professor & Head, Department of Computer Science, Bharathidasan College of Arts and Science, Erode, Tamil Nadu, India[2]

ABSTRACT: Software-Defined Networking (SDN) has been a flexible and scalable networking paradigm; however, the centralized control plane is under siege by newly developed cyber threats such as Distributed Denial-of-Service (DDoS) attacks, intrusion attempts, and Advanced Persistent Threats (APT). To that end, this paper introduces SDN-Guard, a new reinforcement learning-based anomaly detection and adaptive defense algorithm designed to enhance SDN security. SDN-Guardintegrate Deep Q-network-based Anomaly Detection (DQN-AD) to identify in real-time the threats by using network flow features which are able to distinguish normal traffic from malicious. Therefore,it involves the Adaptive Policy Enforcement Module (APEM) as the dynamically changing module in a firewall, in the flow of table updates and routing policies, regarding the evolving pattern of attacks, while continuously perfecting the algorithms for detection and mitigation methods by reward-based learning. Experiments assess that SDN- Guard brings high detection accuracy with a very low false positive, and efficient for cybersecurity in modern networks with low network latency and finally characterizes a very effective and feasible SDN defense.

KEYWORDS: Adaptive Policy Enforcement Module (APEM), Anomaly Detection (AD), Cybersecurity, Deep Q-Network (DQN), Distributed Denial-of-Service (DDoS), Software Defined networks (SDN)

I. INTRODUCTION

SDN is an architectural network that decouples the control plane from the data plane for centralized control of the network. This makes SDN a very good solution in enhancing network management, efficiency, and scalability due to the flexibility of the system. This central approach, however, also opens up new vulnerabilities since an attacker is able to compromise the whole network by exploiting the control plane. Such anomalies include Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and other malicious activities that can break the normal operation of SDN networks, hence calling for highly efficient security mechanisms.

With the continuous deployment of SDN in different fields, its security must be further developed to ensure the integrity and confidentiality of the network by preventing and reducing such attacks.

Recently, reinforcement learning has been actively pursued as a very promising approach to enhance the mechanisms of anomaly detection and defense in SDN environments. In fact, RL is well-suited to learn from interactions with the network and adapt to new attack scenarios in securing SDN infrastructures. For example, Nadeem et al.[6] come up with a deep learning approach for the classification of DDoS attack traffic in SDN environments using machine learning to improve accuracy in detection time. Their work has shown the importance of real- time traffic analysis in the identification of malicious activities and reduction in the impact of DDoS attacks. Similarly, in this integration of deep learning with blockchain technology, the work by Ramadass et al. [7] focuses on additional values related to decentralized control and security afforded by blockchain in the detection and mitigation of DDoS attacks on SDN. Much emphasis is given in the works to integrate the advanced techniques of machine learning with SDN for attack detection and mitigation.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403053|

For example, Nawrin et al. [8] articulate machine-learning and networking algorithms for the enhancement of SDN security. These authors explain how the general resilience of SDN- based networks to all kinds of attacks can be improved, proving that the integration of machine learning with SDN could result in a more robust and adaptive defense mechanism. Contributing to this debate further, Okon et al. [9] focus on multi-operator network handovers by using blockchain-enabled SDN architectures. This work will show how this blockchain can be used in network handover security in SDN, and generally, potential threats in multi-operator setups. This contribution points out ways to integrate the most advanced technologies in SDN frameworks for security against a wide variety of challenges.

While great improvement have been made, the design of dynamic and adaptive defense systems capable of keeping up with a wide range of evolving threats remains a huge challenge in SDN security. A recent example is the work of Alhaj et al. [10] on the design of strong security layers for SDNs, which has proven the need for multi-layered security architectures in dealing with different attack vectors. Likewise, Garba et al. [11] work on SDN-based detection and mitigation of DDoS attacks in smart homes, further raising the growing need for securing IoT devices that are increasing in number and becoming part of SDN networks. In particular,
Fartitchou et al. [12] apply IOTA 2.0 smart contracts to the SDN ecosystem for security and demonstrate one of the ways new blockchain technologies could be brought into play to improve SDN network security and trustworthiness.

With increasing complexity in the SDN environment, the mentioned research efforts are trying to shed some light on the development of intelligent, adaptive, and secure SDN systems capable of countering newly emerging threats in real time.

In the face of these challenges and advances, SDN-Guard proposes a reinforcement learning-based anomaly detection and adaptive defense algorithm tailor-made for securing SDN networks. SDN-Guard borrows the idea of RL to detect anomalous behavior and adjust its defense policies based on the real-time dynamics of the network. This would definitely help meet the growing demand for intelligent, proactive security solutions for SDN, which ensures that the network is able to learn from attack patterns and, hence, evolve its defense mechanisms. The proposed model, therefore, builds on previous works and methodologies—deep learning, blockchain integration, and machine learning—to provide an intensive and robust security framework in SDN environments.

II. LITERATURE REVIEW

The most prominent security and privacy issues of SDN-enabled IoT systems are discussed in Rahdari et al. [1]. This study explores vulnerabilities and causes of attacks on networks and devices in the IoT environments and provides solutions proposed for such mitigations. Their work also proposes future research directions in an SDN-enabled IoT context. The authors provide solutions to their own existing models against new threats in an in-depth literature review. This work will contribute to the emerging discussions on securing IoT in SDN- based systems.

Alashhab et al. [2] present a solution for DDoS attack detection and mitigation in SDN environments. In the improvement of the process of detection, authors introduced the ensemble online machine-learning model. This research is an attempt in improving, through machine learning, the precision of the response in time of DDoS defense systems; the design is set to adapt to new attack vectors in real-time. This research work reflects the increasing call for the need to have adaptive security mechanisms within SDN.

Kim et al. [3] focuses on the enhancement of security in SDN through the categorization of different types of attacks and suggesting strategies to defend from the perspective of
penetration testing. This work systematizes the security threats faced by SDN networks and suggests methods to address them. The authors show that proactive security measures are needed in order not to suffer or minimize attacks. This paper is about the theoretical and practical solution to improve resilience in SDN. It serves as a roadmap for the researcher and practitioners to secure SDN infrastructures.

Hnamteet. al. [4] points to the betterment of ARP spoofing attack detection and mitigation in SDN environments. The authors propose an efficient method for enhancing the security of SDN from this kind of attack, which has the potential to cause a huge disruption in communication over the network. This research highlights the challenges that SDN faces in dealing with such attacks and further proposes a novel approach for the same. It evaluates the performance of the proposed solution in real-world scenarios. The paper contributes to the strengthening of the overall security framework

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403053|

of SDN-based networks.

Similarly, the SDN security model, proposed by Pradeep et al. [5], namely EnsureS, is designed in such a way that it would assure security against data breaches by lightweight service path validation, batch hashing, and tag verification. The model has been designed with an eye on leading toward efficiency while still keeping most of the critical security measures under consideration. This is the biggest study epitomizing the importance of network path verification in SDN for data integrity and security. It will provide the most feasible way to enhance SDN system security in an enterprise environment. The research is a useful contribution to SDN security model development.

III. PROBLEM IDENTIFICATION

With this increased adoption of SDN, new security issues arise due to the centralized control structure that exposes SDN to quite several attacks, for instance, DDoS and intrusion attacks. The dynamic and ever-changing nature of the threats in the SDN environments are found not suitable to be handled using traditional security approaches. Most of the current anomaly detection and defense systems lack real-time adaptivity to emerging attack patterns, so they might react late to ongoing attacks. Further, the SDN infrastructures require the solution in more efficiency and automation while detecting anomaly mitigation attacks. This, of course, requires an adaptive, intelligent security mechanism that will be able to learn and evolve continuously with the behavior of the network in order to guarantee adequate protection against evolving threats.

IV. MATERIALS AND METHODS

SDN-Guard include a reinforcement-learning framework in the SDN control plane to increase the efficacy of the anomaly-detection and defense mechanisms. Its system uses real- time data from network traffic, including information about flows and packets at the level of single packets, to train and tune the model of RL. The trained model will continue to monitor the environment of SDN for any deviation from normal behavior, which may flag potentially dangerous security threats.

SDN GUARD FOR ENHANCING SDN SECURITY

SDN-Guard is a novel, reinforcement-learning-based anomaly detection and adaptive- defense algorithm for the security of SDNs. SDN-Guard exploits reinforcement learning for dynamic learning in network-traffic patterns to tune its defense mechanism in real-time, providing real-time capabilities in detection and mitigation against new and complex security threats, including DDoS attacks and network intrusion. The algorithm will continue to adapt to changed attack strategies for better detection accuracy and reduced harm from malicious activities. The SDN-Guard algorithm core is a reinforcement learning model that rewards the agent based on its actions. The reward function is defined as:

$$R_t = \alpha \cdot D_t - \beta \cdot C_t \quad (1)$$

This equation 1 represents the tradeoff between accurate anomaly detection and computational or network cost associated with defense actions. The agent tries to maximize the reward by increasing the detection accuracy and decreasing the cost for defense.

This is the state transition function—the way the system will change given the agent's actions in reinforcement learning. The state transition for SDN-Guard can be modeled as:

$$S_{t+1} = f(S_t, A_t) \quad (2)$$

This equation 2, performance modeling how the SDN environment changes over time as the RL agent interacts with it; that is, the actions by the agent—either blocking malicious traffic or adjusting network flow—impact the next state of the system, and the agent has to adjust its strategy accordingly to maximize security.A simplified SDN-Guard expression in the line of anomaly detection and adaptive defense of SDN security can be illustrated with the following example:

$$D_t = \alpha \cdot P(Anamoly_t | X_t) - \beta \cdot C_t \quad (3)$$

This equation 3 is used in the decision of whether the anomaly is anomalous enough to take an action in defense,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403053|

because of the right balance in detecting anomaly and reducing the cost of the implementation of defense. SDN-Guard tunes its parameters with α and β to choose the optimal security response strategy, under which only required defenses could be triggered for enhancing efficiency and effectiveness in SDN security.

Deep Q-Network based Anomaly Detection (DQN-AD)

Deep Q-Network based Anomaly Detectionis a very strong approach in the real-time identification of threats in network environments, especially in the distinction between normal and malicious nodes. This technique uses a Deep Q-Network (DQN), a model of reinforcement learning, to keep analyzing network traffic and behavior patterns for the classification of nodes as either benign or malicious. By using deep learning techniques, QN-AD helps the system learn from historical data and adapt to dynamic network conditions for the recognition of very slight anomalies, which may signal illegitimate activity. The model will observe the state of the network and, through trial and error, optimize its detection strategy in order to maximize its accuracy over time. It assigns rewards based on the correctness of classification, hence encouraging behaviors identifying malicious nodes, while penalizing actions of the opposite nature, ensuring effective and accurate real-time detection with dynamic protection in place against more complex and sophisticated threats that now appear in modern network infrastructures.Q-function represents the expected future return for taking an action in a state.

$$Q(S_t,A_t)=R_t+\gamma \max Q(S_{t+1},A') \quad (4)$$

This equation 4 allows the system to choose the best defense action based on previous experiences and estimated future rewards.State representation captures the characteristics of the network environment for normal or anomalous behavior.

$$S_t=f(X_t,T_t) \quad (5)$$

Equation 5 maps real-time network features into a state representation used by the DQN for anomaly detection.The reward function represents how good a particular anomaly detection and defensive action is.1

$$R_t = \begin{cases} -1 \\ 0 \end{cases} \quad (6)$$

This equation 6 allows the DQN model to learn which actions, such as blocking or alerting, contribute to successful threat detection, hence securing SDN with experience.

Adaptive Policy Enforcement Module (APEM)

Adaptive Policy Enforcement Module isa security mechanism that dynamically tries to update the firewall rules and flow table updates, along with traffic routing adjustments, in order to strengthen networks against new attack patterns that are evolving over time. APEM will automatically analyze the threat presented by the incoming data in real-time monitoring of network traffic. It updates, therefore, the firewall rules in order to block malicious traffic, and updates also the flow tables for the optimization of legitimate data handling according to the detected anomalies or possible security breaches. The traffic is rerouted in such a way to ensure that the critical network resources are protected. With this adaptive approach, a network can be maintained at high-security posture because it swiftly changes with new and evolving attack strategies without any manual intervention. APEM, using real-time data and automated decision-making, assures that the network will keep up with emerging threats while having minimal impact on legitimate services. The change is modeled in firewall rules based on perceived threats on the network.

$$R_t=f(T_t,A_t) \quad (7)$$

Equation 7 shows that APEM only updates the firewall rules in order to raise the security level against malicious traffic due to the action of a detected threat.Update of the flow table is determined by the legitimate traffic behavior on the network.

$$F_t=g(L_t,T_r) \quad (8)$$

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403053|

Above formula shows how APEM keeps on optimizing traffic flow by updating the flow tables in relation to observations of patterns over previous routing rules.This equation 8 models the rerouting of traffic in response to detected attacks or anomalies.

T_r=h(S_t,A_t) ---------- (9)

According to Equation 9, APEM, upon detecting an attack, will reroute the traffic to secure paths in the network with minimum disturbance and no loss of the integrity of the network.

V. RESULTS AND DISCUSSION

Table 1: Comparison of Performance metrics across various algorithms

Algorithms	Throughput (Mbps)	End-to-End latency (ms)	Packet Delivery Ratio (%)	Detection Accuracy (%)
SDN-IDS	150	10	97	89
DDoS-Guard	140	20	99	93
DoS Guard	130	25	94	83
SDN Guard (Proposed)	200	5	99.5	97

Table 1 shows theperformance comparison between the four algorithms, SDN-IDS, DDoS-Guard, DoSGuard, and the proposed SDN-Guard, in terms of four metrics: throughput, end-to-end latency, packet delivery ratio, and detection accuracy. SDN-Guard shows the best performance regarding throughput, latency, and detection accuracy, while having the highest delivery ratio.

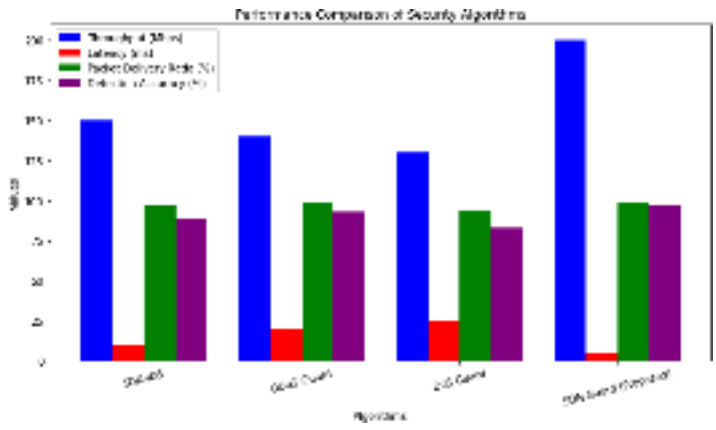


Figure 1: Performance metrics comparison over varied algorithms

Figure 1 shows the comparison of the performances in terms of throughput, end-to-end latency, packet delivery ratio, and detection accuracy of these four algorithms. SDN-IDS reaches a throughput of 150 Mbps at an end-to-end latency of 10ms, delivering 97% of packets with a detection accuracy of 89%. DDoS-Guard scores a bit lower at 140 Mbps throughput but has a better latency time at 20ms, with a higher 99% packet delivery ratio and a 93% detection accuracy score. The lowest throughput was that of DoSGuard at 130 Mbps, with the worst latency of 25ms, a packet delivery ratio of 94%, and a detection accuracy score of 83%. The proposed SDN-Guard has the best throughput at 200 Mbps, the lowest latency at 5ms, and a near-perfect packet delivery ratio of 99.5%, with a detection accuracy rate of 97%.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403053|

VI. CONCLUSION

This paper presents mechanisms to improve SDN security by using SDN Guard while evaluating the throughput, end-to-end latency, packet delivery ratio, detection accuracy in which SDN-Guard proved better than other machine-learning models including SDNs. It also has the optimal detection accuracy rate for improving SDNs security with a maximum rate of 97%. SDN-Guard enhances the security of a software-defined network, detects anomaly, and adaptivedefense leverages reinforcement learning. It can identify malicious activities in an effective manner, mitigate threats in real time, and optimize network performance. This is achieved through the continual learning of network behavior so as to be able to adapt to any new attacks with a very minimal intervention of humans. The proposed approach improves threat response accuracy while reducing false positives. Its integration strengthens SDN resilience against evolving cyber threats. In a nutshell, SDN-Guard offers a strong, intelligent security framework for today's modern networks.

REFERENCES

1. Rahdari, A., Jalili, A., Esnaashari, M., Gheisari, M., Vorobeva, A. A., Fang, Z. &Tahaei, H. (2024). Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions. Computers, Materials & Continua, 80(2).
2. Alashhab, A. A., Zahid, M. S., Isyaku, B., Elnour, A. A., Nagmeldin, W., Abdelmaboud, A. &Maiwada, U. (2024). Enhancing DDoS attack detection and mitigation in SDN using an ensemble online machine learning model. IEEE Access.
3. Kim, J., Seo, M., Lee, S., Nam, J., Yegneswaran, V., Porras,P& Shin, S. (2024). Enhancing security in SDN: Systematizing attacks and defenses from a penetration perspective. Computer Networks, 110203.
4. Hnamte, V., & Hussain, J. (2024). Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation. Telematics and Informatics Reports, 14, 100129.
5. Pradeep, S., Sharma, Y. K., Lilhore, U. K., Simaiya, S., Kumar, A., Ahuja, S &Chakrabarti, T. (2023). Developing an SDN security model (EnsureS) based on lightweight service path validation with batch hashing and tag verification. Scientific Reports, 13(1), 17381.
6. Nadeem, M., Dwivedi, S., Akhtar, R., Ansari, S. A., Singh, S., Siddiqui, E. F., & Kumar, R. (2024). Deep Learning Approach for Classifying DDoS Attack Traffic in SDN Environments. Journal of Information Security and Cybercrimes Research, 7(2), 109-126.
7. Ramadass, P., shreeSekar, R., Srinivasan, S., Mathivanan, S. K., Shivahare, B. D., Mallik, S &Ghribi, W. (2024). BSDN-HMTD: A blockchain supported SDN framework for detecting DDoS attacks using deep learning method. Egyptian Informatics Journal, 27, 100515.
8. Nawrin, M., Aurid, M. E. U. R., Saad, E. A. K., & Shrestha, M. A. (2024). Enhancing security in software defined Networking using machine learning and networking algorithm (Doctoral dissertation, Brac University).
9. Okon, A. A., Sallam, K., Hossain, M. F., Jagannath, N., Jamalipour, A., &Munasinghe, K. S. (2024). Enhancing Multi-Operator Network Handovers with Blockchain-Enabled SDN Architectures. IEEE Access.
10. Alhaj, A. N., Patel, N. D., Singh, A., Bondugula, R. K., Dar, M. F., &Ahamed, J. (2024). Design and analysis of a robust security layer for software defined network framework. International Journal of Sensor Networks, 46(1), 1-14.
11. Garba, U. H., Toosi, A. N., Pasha, M. F., & Khan, S. (2024). SDN-based detection and mitigation of DDoS attacks on smart homes. Computer Communications, 221, 29-41.
12. Musa, N. S., Mirza, N. M., Rafique, S. H., Abdallah, A., &Murugan, T. (2024). Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks-current research solutions. IEEE Access.
13. Fartitchou, M., Lamaakal, I., Maleh, Y., El Makkaoui, K., El Allali, Z., Pławiak P & A. Abd El-Latif, A. (2024). IOTASDN: IOTA 2.0 Smart contracts for securing software-defined networking ecosystem. Sensors, 24(17), 5716.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details