A Robust Security System Using SHA-512 with Reinforcement Learning in Wireless Sensor Networks

C. Anuradha
Department of Electrical and Electronics Engineering, Faculty of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India
anuradhc@srmist.edu.in (corresponding author)

A. V. Mayakkannan
Department of Electronics and Communication Engineering, Kings Engineering College, Chennai, Tamil Nadu, India
avmayakkannan@gmail.com

R. Vinodha
Department of Electronics and Communication Engineering, ULTRA College of Engineering and Technology, Madurai, Tamil Nadu, India
vinodhaphd.2019@gmail.com

K. Narsimha Reddy
Department of Electronics and Communication Engineering, Vardhaman College of Engineering, Hyderabad, Telangana, India
simha.vce@vardhaman.org

B. Annapurna
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vijayawada, Andhra Pradesh, India
dr.annapurnagandrety@gmail.com

T. Bhargava Ramu
Department of Electrical and Electronics Engineering, MLR Institute of Technology, Hyderabad, Telangana, India
bhargava.ramu@mlrinstitutions.ac.in

T. M. Nithya
Department of Computer Science and Engineering, K.Ramakrishnan College of Engineering, Tiruchirappalli, Tamil Nadu, India
nithusiva123@gmail.com

C. Srinivasan
Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, Tamil Nadu, India
srinivasanchelliah@gmail.com

Received: 13 August 2025 | Revised: 12 September 2025 | Accepted: 24 September 2025

 DOI: https://doi.org/10.48084/etasr.14048

ABSTRACT

Routing in Wireless Sensor Networks (WSNs) is highly vulnerable due to the unreliable wireless medium and limited node resources. Routing attacks can severely degrade network performance. This paper proposes a Robust Security system using Reinforcement Learning (RSRL) and the Secure Hash Algorithm 512 (SHA-512) for secure and efficient routing in WSNs. The primary objective of the RSRL mechanism is to detect malicious nodes and enhance system security. In the RSRL mechanism, the Base Station (BS) performs aggregator verification using SHA-512 to ensure data integrity without burdening low-power sensor nodes. A Reinforcement Learning (RL) agent, executed at the BS, dynamically learns optimal policies to detect malicious sensor nodes based on node Response Time (RT), Consumed Energy (CE), and Loss Ratio (LR). The RSRL system selects reliable nodes for route selection to improve routing efficiency. The proposed RSRL model is implemented in Network Simulator 2.35. Simulation results demonstrate a 26.44% improvement in Packet Forwarding Ratio (PFR) and 95% detection accuracy compared to a conventional secure routing mechanism. The results confirm that RSRL effectively mitigates routing attacks while maintaining high network performance.

Keywords-Reinforcement Learning (RL); Wireless Sensor Networks (WSNs); Secure Hash Algorithm 512 (SHA-512); malicious node detection; reward function

I. INTRODUCTION

Wireless sensor networks (WSNs) deployed in military applications require high security, making the use of reliable nodes and links essential [1]. Over the years, various approaches have been proposed to enhance data aggregation, routing, and data security [2]. Despite these efforts, most existing methods remain limited by factors such as high time complexity, vulnerability to malicious attacks, and data uncertainty [3]. To strengthen network protection, Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) have been widely adopted, as they combine resource efficiency with strong data security in WSNs [4]. However, although cryptographic approaches effectively mitigate security vulnerabilities, they often suffer from reduced throughput [5]. As a result, the efficient detection of malicious sensor nodes has become a significant factor.

Reinforcement Learning (RL) provides an adaptive framework capable of learning from network behavior [6]. RL is a machine learning model in which an agent interacts with the environment, makes decisions, and receives rewards to learn an optimal strategy. It offers adaptiveness, robustness, and scalability, enabling security policies to evolve alongside attack strategies. Moreover, RL provides robust protection even against unknown attacks [7], minimizes false alarms in malicious detection, and enhances the Packet Forwarding Ratio (PFR).

The Secure Hash Algorithm 512 (SHA-512) generates hash values for encrypting input data, ensuring both data integrity and authentication. This hash-based grouping process also improves routing efficiency. In this process, network sensor nodes are distributed into several groups, with each group comprising multiple sensor nodes and an aggregator node that manages local communication within the group [8]. In general, group members (sensor nodes) communicate with the aggregator, which aggregates and fuses the collected data to conserve energy.

The Secure Authentication and Key Management Scheme (SAKMS) based on ECC provides secure and trustworthy authentication between devices in wireless networks. This mechanism utilizes hashing, Exclusive OR (XOR), and ECC multiplication operations. Furthermore, dynamic key updating ensures resilience against potential key leakage. However, frequent dynamic key updates across nodes introduce additional transmission and processing overhead. The regular-window method accelerates ECC multiplications, but cryptographic operations, including hashing, hidden credential handling, and dynamic key cooperation, still require significant resources and introduce latency in sensor node communication. In addition, this mechanism requires interactions for authentication and key agreement, which can impact battery life. Moreover, the ECC algorithm is susceptible to timing and power analysis attacks [9].

To overcome these challenges, this paper introduces a Robust Security system using SHA-512 with RL (RSRL) for WSN. The RSRL framework leverages SHA-512 to ensure strong security, whereas the RL agent provides adaptability in resource-constrained and attack-prone environments. The main contributions of RSRL are summarized as follows. The Base Station (BS) verifies the aggregator using a hash code value computed by the SHA-512 algorithm. This hash code is generated from the node identity, personal identification number, and sensor node location to detect malicious aggregators. Additionally, the RL model calculates a node reward function based on node Response Time (RT), Consumed Energy (CE), and Loss Ratio (LR), efficiently detecting malicious sensor nodes. Afterward, the aggregator node forwards the sensor data to the BS through reliable nodes. The results demonstrate that RSRL improves the detection ratio while minimizing delay and packet loss in WSNs.

II. LITERATURE REVIEW

Artificial intelligence algorithms have been applied to identify Denial of Service (DoS) attacks and alleviate their effects. In addition, ensemble-based methods aggregate multiple classifiers to enhance detection accuracy [10]. The Rabin–Karp method is a lightweight algorithm that verifies transmitted data packets using hash values. This mechanism maintains high detection accuracy while reducing computational overhead, improving the reliability of WSNs [11]. Furthermore, the homomorphic encryption technique encrypts and decrypts messages to address key distribution

issues for secure transmission during secret key generation [12].

In [13], a cryptographic data security mechanism for reliable WSNs applies the ECC method for key generation, whereas the Advanced Encryption Standard (AES) algorithm performs encryption and decryption to enhance security. This technique also utilizes a grouping process to improve energy efficiency. In [14], the Elliptic Curve Digital Signature Algorithm (ECDSA) using SHA-512 encrypts the data and checks the integrity of the received data. If an attacker alters the received data, the ECDSA notices it and signals the transmitter for retransmission.

Misdirection attacks cause malicious nodes to divert network traffic to improper paths, leading to packet drops, increased energy consumption, and transmission failures. In [15], a misdirection attack detection and prevention scheme that utilizes an RL algorithm efficiently detects such attacks with minimal computational cost [15].

Secure aggregation is an efficient solution for providing privacy in federated learning-based WSNs. Traditional secure aggregation for sensor nodes relies on Shamir's secret sharing to achieve dropout robustness but restricts scalability and dropout tolerance. In [16], an improved secure aggregation method utilizes a non-colluding server and motivator nodes to reach almost complete (up to $n-2$) corruption and dropout tolerance. It exploits discrete logarithm-based extractable and equivocal commitments to achieve malicious security. Furthermore, in [17], a random forest-based selective forwarding attack detection mechanism observes node behavior, such as packet loss rate, size of packet, forwarding rate, and energy utilization, to identify malicious activities in WSNs.

In [18], a security-enhanced certificateless designated verifier anonymous aggregate signature approach provides strong security against several attacks. In addition, the You Only Speak Once (YOSO) model introduces a dynamic and volatile committee for system initialization and key distribution. In [19], an adaptive fusion biometric key generation framework integrates palm vein biometric features with state-of-the-art cryptographic methods to detect Man-in-the-Middle (MIMT) attacks in the network [19]. Moreover, authors in [20] proposed an RL-based intrusion detection mechanism that applies repeated node classification to detect intrusions. It measures sensor node behavior based on link quality, which is computed from the PFR and the residual energy of each node.

III. PROPOSED METHOD

In WSNs, security has become a critical issue, as existing techniques for malicious node detection often adopt a one-time, centralized decision-making approach. With this paradigm, errors are difficult to avoid, and reproducibility and traceability are challenging. Hence, conventional WSN malicious node detection methods cannot assure the traceability and fairness of the detection process.

WSNs are vulnerable to an extensive range of attacks, in which the malicious nodes can obtain the identities of middle nodes or incorrectly construct identities before linking to the network. External attacker nodes may eavesdrop on node-to-node communication and propagate incorrect information through the network. There are many methods to perform attacks. For example, malicious nodes may communicate directly with legitimate nodes, assume the identity of a legitimate node to transmit false data, or initiate DoS attacks to weaken the resources of reliable nodes.

To address these challenges, the proposed work introduces SHA-512 combined with an RL algorithm to improve secure routing in WSNs. Figure 1 illustrates the block diagram of the proposed RSRL mechanism. The RSRL mechanism consists of registration, group formation, malicious node categorization, and the data transmission process in WSNs.

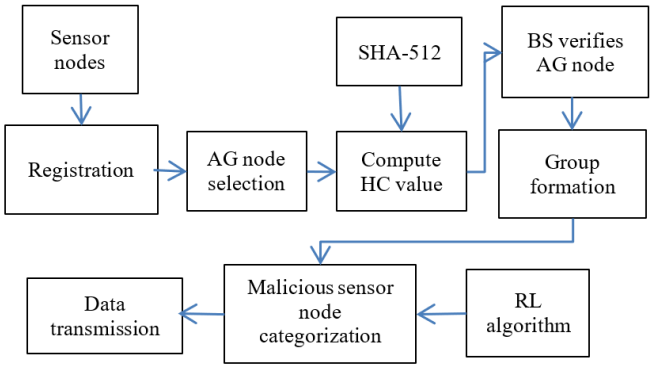

Fig. 1. Block diagram of the proposed RSRL system.

In a WSN, multiple sensor nodes sense the environment and forward information to an aggregator (AG) node. The AG node collects this information, removes redundant data, and transfers it to the BS. The objective of applying SHA-512 is to authenticate the sensor nodes. The BS verifies AG nodes before they communicate with other AG nodes or sensor nodes. In addition, the AG node authenticates each sensor node when it joins the group. The RL algorithm isolates malicious nodes to protect the integrity and confidentiality of transmitted data.

A. Registration

All sensor nodes have unique Media Access Control (MAC) addresses. The BS handles the registered sensor node details, and this information is stored in the database. The BS broadcasts a request message to all sensor nodes to select the AG. Some sensor nodes respond with a reply message indicating their willingness to act as an AG.

The RSRL system utilizes the SHA-512 algorithm to compute the AG Hash Code (HC) value. Before selecting AG nodes, the BS verifies the HC value and MAC address. Consider an AG node with $\mathrm{ID_{AG}}$ (AG identity), $\mathrm{Loc_{AG}}$ (AG location), and $\mathrm{PIN_{AG}}$ (personal identification number). The SHA-512 algorithm computes the HC as follows:

$$\mathrm{HC} = \mathrm{hf}(\mathrm{ID_{AG}}||\mathrm{Loc_{AG}}||\mathrm{PIN_{AG}}) \quad (1)$$

where hf indicates the hash function. The PIN is a 4-digit random number between 0 and 9. If the computed HC value matches the AG node's HC, the BS confirms that the AG node

is normal and broadcasts its role as an AG to the entire network. Otherwise, the BS notifies the network that the AG node is malicious. Thus, the RSRL system, using the SHA-512 algorithm, can detect external attacks such eavesdropping, DoS, and node capture attacks in the WSN.

B. Group Formation

Each sensor node forwards a join request message within the communication range of the AG nodes to form groups. The AG nodes receive these request messages and respond to allow the sensor nodes to join their groups. The BS verifies whether each sensor node is normal or malicious by applying the RL algorithm. The RL algorithm computes a reward function for each sensor node based on its LT, RT, and CE. If a sensor node is identified as malicious, the BS broadcasts a notification message to all nodes. When a sensor node is verified as reliable, it is associated with a group and receives data uninterruptedly. The AG node acts as the leader of the group, and the member nodes forward their data through the AG node. The AG node accepts the data from the normal nodes, removes duplicates and forwards the important data.

C. Malicious Sensor Node Categorization Using Reinforcement Learning

Conventional security approaches increase computational costs and create a single point of failure, causing sensor nodes to act selfishly due to the lack of resources. To address these problems, RL is applied with reward function estimation. The RL agent, such as the BS, computes each sensor node's reward function based on node LR, RT, and CE.

LR indicates the amount of packet loss per unit time during data communication in the network. The following equation calculates LR:

$$\mathrm{LR} = \frac{\text{Loss packets(n)}}{\mathrm{T}} \quad (2)$$

Here, T indicates the time interval, and n denotes the sensor node. CE describes the amount of energy consumed from a sensor node's battery during the execution of supervisory and data transmission processes. The following equation calculates CE:

$$\mathrm{CE} = \text{Initial Energy} - \text{Residual Energy} \quad (3)$$

RT indicates the entire time between request initialization and fulfillment. The following equation calculates RT:

$$\mathrm{RT} = \frac{\frac{\mathrm{pb}}{\mathrm{nb}} + \frac{\mathrm{pd}}{\mathrm{ps}} + \mathrm{st}}{\mathrm{T}} \quad (4)$$

where pb denotes the number of packet bits, pd indicates the propagation distance, st represents the serving time, ps refers to the propagation speed, nb describes the network bandwidth, and T indicates the time.

The RL agent, such as the BS, computes each sensor node's reward function based on node LR, RT, and CE. Here, the RL sense environment is defined as a Markov Decision Process (MDP), which is established with an optimum rule theory to recognize the maximum rewards over time. The RL agent interacts with the environment and takes an action (AT) in each state (ST) and waits for a response. The agent observes the environment states (LR, RT, and CE) for any updates and optimizes the received reward (RW) via updating rules.

In the RL technique, the agent evaluates the state-value function to adjust all states and actions. For each iteration, if the AT result is lower than the RW, the output table is updated. In every ST, the agent takes an AT, such as malicious, reliable, or suspicious, detects the RW for that action, and then transitions to the next ST, adjusting the Evaluated Quality (EQ) as specified below:

$$\mathrm{EQ}(\mathrm{ST}, \mathrm{AT}) \leftarrow (1-\gamma)\mathrm{Q}(\mathrm{ST}, \mathrm{AT}) + \gamma(\mathrm{RW} + \max \mathrm{Q}(\mathrm{ST}, \mathrm{AT})) \quad (5)$$

LR, RT, and CE compute the RW value for isolating malicious nodes. The nodes with the highest RW value nodes are identified as malicious nodes. The reward computation for a sensor node is specified below:

$$\mathrm{RW} = \gamma^{\mathrm{D}}(\mathrm{LR} + \mathrm{RT} + \mathrm{CE}) \quad (6)$$

where $\gamma \in [0, 1]$ and D represents a discount factor that determines the influence of future rewards on the present one. The RW value of +1 denotes accurate detection, whereas 0 indicates an uncertain decision corresponding to a suspicious node. Finally, the sensing information is forwarded through reliable AG nodes in the network. Table I demonstrates how the BS categorizes malicious nodes.

TABLE I. RL ALGORITHM-BASED MALICIOUS NODE DETECTION IN A WSN

ID	RT (ms)	LR (%)	CE (J)	RL output	Sensor node classification	EQ value	RW
SN1	15	1.5	0.015	0	Normal	0.93	+1
SN2	25	4	0.045	1	Suspicious	0.68	0
SN3	40	8	0.09	2	Malicious	0.81	+1
SN4	4	0.9	0.05	0	Normal	0.95	+1
SN5	110	12	0.07	2	Malicious	0.85	+1

The pseudocode of the RSRL mechanism is specified below.

```
#Pseudocode of the RSRL mechanism
Initialization: BS, sensor nodes (SN), AG
nodes, HC, RL algorithm
Registration of AG nodes:
 For AG = 1, 2,..., k do {
    BS computes the HC value using SHA-512
    If (BS HC = = AG HC) {
       AG is legitimate
       AG is assigned as an aggregator
    } else {
       AG is malicious
       AG node is removed from the network
    }
 }
Registration of SN nodes:
 For SN =1, 2, …., n do {
    BS computes RW based on RT, LR, and CE
    If RW indicates SN is reliable {
       SN shares its ID and location with
       related AG
```

```
      SN joins the group
    } else {
    SN is malicious
    AG discards the join request
    }
  }
Data transmission:
  AG selects the route to forward the data
  SN data are forwarded through the
  selected AG route
  BS receives the data
```

IV. SIMULATION ANALYSIS

This section presents a simulation-based evaluation of the RSRL model for detecting malicious nodes in WSNs. The Network Simulator 2.35 tool is used to model the network environment and compare the performance of the proposed RSRL with the existing SAKMS model. The simulation uses a 500 × 600 m² topology, with 150 randomly distributed sensor nodes, each having a communication range of 50 m and an initial energy of 1 J. The simulator employs a two-ray ground propagation model.

The RSRL system utilizes the KDDCup'99 dataset [21] to detect malicious sensor nodes in the WSN. Data packets of size 1024 bytes are forwarded through the network, and the SHA-512 algorithm authenticates aggregator nodes to protect the data from external attackers.

PFR indicates the ratio of the sensor nodes that forward the data packets to the BS successfully. Figure 2 demonstrates the PFR with respect to the number of sensor nodes.

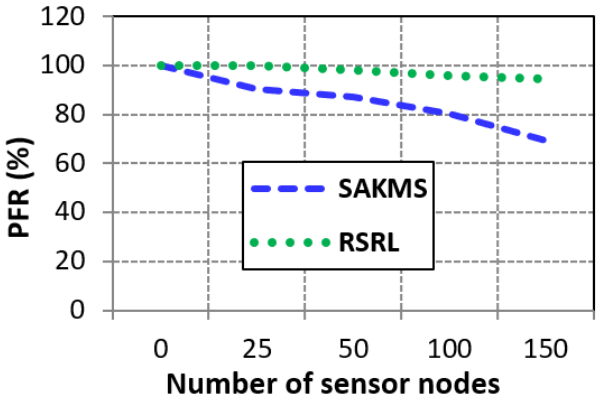

Fig. 2. PFR of SAKMS and RSRL models versus the number of sensor nodes.

As shown in Figure 2, the PFR decreases as the number of sensor nodes increases. A higher number of sensor nodes contributes to increased communication, which raises delay and computational overhead. However, the proposed RSRL model achieves a higher PFR than the existing SAKMS model. By utilizing the SHA-512 algorithm combined with an RL reward function, the RSRL model efficiently detects the malicious nodes. In contrast, the existing SAKMS model relies on the ECC algorithm, which increases computational complexity and delay. Overall, the proposed RSRL model improves PFR by 26.44% compared to SAKMS.

The Malicious Detection Ratio (MDR) is defined as the ratio between the number of accurately acknowledged malicious sensor nodes and the total number of malicious sensor nodes. It is computed as:

$$\text{MDR} = \frac{\text{MAL}_{\text{Ack}}}{\text{MAL}_{\text{Total}}} \quad (7)$$

Figure 3 shows MDR accuracy with respect to the number of sensor nodes. As the number of sensor nodes increases, MDR decreases due to missed detections. As shown in the figure, the proposed RSRL model detects malicious sensor nodes more efficiently than the existing SAKMS model.

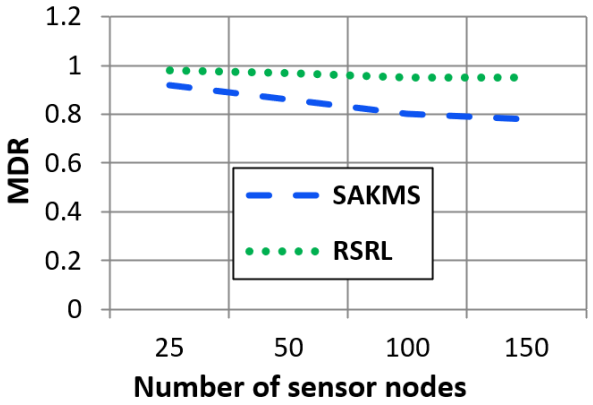

Fig. 3. MDR of SAKMS and RSRL models versus the number of sensor nodes.

Delay represents the time between the sender forwarding the data packet and the destination receiving it. It is calculated as:

$$\text{Delay} = \sum_{i=0}^{m}(\text{Time of packet received} - \text{Time of packet sent}) \quad (8)$$

where m denotes the number of sensor nodes. Figure 4 illustrates the Delay of SAKMS and RSRL models with respect to the number of sensor nodes.

Malicious nodes can drop data packets and do not provide a proper response, requiring multiple retransmissions. The proposed RSRL mechanism utilizes the SHA-512 algorithm to authenticate sensor nodes and the reward function to detect malicious sensor nodes efficiently. In addition, data are transmitted through reliable AG nodes, minimizing the delay. As a result, RSRL reduces delay by 30.52% compared to the SAKMS mechanism.

Packet Loss Ratio (PLR) is defined as the number of forwarded packets not received at the BS:

$$\text{PLR} = \sum_{i=0}^{m}(\text{Forwarded packets} - \text{Received packets}) \quad (9)$$

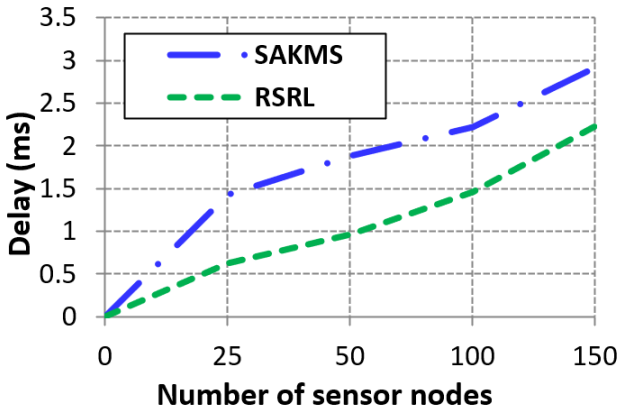

Fig. 4. Delay of SAKMS and RSRL models versus the number of sensor nodes.

Figure 5 shows the PLR of SAKMS and RSRL models with respect to the number of sensor nodes. As the number of sensor nodes increases, PLR also increases due to the increase in the number of hops and the presence of malicious nodes. The proposed RSRL mechanism, using SHA-512 with RL, detects malicious sensor nodes efficiently and transmits data through reliable AG nodes, reducing PLR by 28.83% compared with SAKMS.

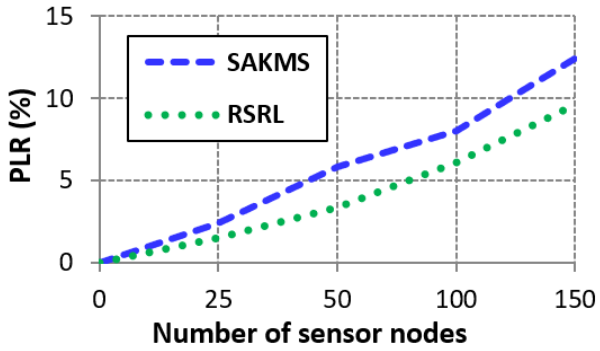

Fig. 5. PLR of SAKMS and RSRL models versus the number of sensor nodes.

V. CONCLUSIONS

This paper proposes an integrated approach using the Secure Hash Algorithm 512 (SHA-512) and Reinforcement Learning (RL) to secure Wireless Sensor Networks (WSNs) against malicious nodes. The SHA-512 algorithm authenticates aggregator (AG) and sensor nodes, whereas the RL agent effectively detects malicious nodes. The Base Station (BS) verifies the aggregator using the SHA-512 algorithm. The RL agent learns optimal policies to identify malicious behavior based on node Response Time (RT), Consumed Energy (CE), and Loss Ratio (LR).

The proposed Robust Security with Reinforcement Learning (RSRL) system forwards data through reliable AG nodes, ensuring network reliability and routing efficiency. Simulation results demonstrate that the RSRL mechanism reduces packet loss by 28.83% and delay by 30.52% compared to the existing Secure Authentication and Key Management Scheme (SAKMS), and enhances malicious node detection accuracy.

The RSRL system is suitable for applications such as critical infrastructure protection, transportation hubs, urban security, and disaster management, which require reliable and continuous monitoring. A limitation of the RSRL system is the increase in communication overhead and energy consumption. Future work includes applying federated learning for distributed RL agents and integrating real-time blockchain technology to further enhance security and reliability.

REFERENCES

[1] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," *Sensors*, vol. 22, no. 13, Jul. 2022, Art. no. 4730, https://doi.org/10.3390/s22134730.

[2] Vikas, B. B. Sagar, and M. Munjul, "Security issues in wireless sensor network – A survey," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 5, pp. 1415–1427, Jul. 2021, https://doi.org/10.1080/09720529.2021.1932937.

[3] P. William, N. Chinthamu, A. Saxena, T. R. V. Lakshmi, and M. Tiwari, "Integration of Secure Data Communication with Wireless Sensor Network Using Cryptographic Technique," in *Forth International Conference on Mobile Radio Communications and 5G Networks*, Kurukshetra, India, 2023, pp. 589–605, https://doi.org/10.1007/978-981-97-0700-3_46.

[4] S. Nirmalraj, D. N. S. Ravikumar, Krishnamoorthy, R. Babu, G. Immanuel, and P. Rajasekaran, "Securing data in Wireless Sensor Network using Hybrid ECC + AES Cryptographic Approach," in *2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems*, Chennai, India, 2023, pp. 1–5, https://doi.org/10.1109/ICSES60034.2023.10465343.

[5] S. Vadlamani, A. Byri, I. Khan, S. Krishnamurthy, O. Goel, and M. Hussien, "A Cryptography-Based Approach to Wireless Sensor Network Security," in *Proceedings of International Conference on Next-Generation Communication and Computing*, Ghaziabad, India, 2024, pp. 169–182, https://doi.org/10.1007/978-981-96-3728-7_14.

[6] P. Kumar *et al.*, "Machine Learning Enabled Techniques for Protecting Wireless Sensor Networks by Estimating Attack Prevalence and Device Deployment Strategy for 5G Networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, Apr. 2022, Art. no. 5713092, https://doi.org/10.1155/2022/5713092.

[7] Z. Qu, H. Xu, X. Zhao, H. Tang, J. Wang, and B. Li, "An Energy-Efficient Dynamic Clustering Protocol for Event Monitoring in Large-Scale WSN," *IEEE Sensors Journal*, vol. 21, no. 20, pp. 23614–23625, Oct. 2021, https://doi.org/10.1109/JSEN.2021.3103384.

[8] S. Hussain *et al.*, "An Adaptive Intrusion Detection System for WSN using Reinforcement Learning and Deep Classification," *Arabian Journal for Science and Engineering*, vol. 50, no. 15, pp. 12463–12477, Aug. 2025, https://doi.org/10.1007/s13369-024-09769-x.

[9] W. Yang, C. Hou, Y. Wang, Z. Zhang, X. Wang, and Y. Cao, "SAKMS: A Secure Authentication and Key Management Scheme for IETF 6TiSCH Industrial Wireless Networks Based on Improved Elliptic-Curve Cryptography," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 3, pp. 3174–3188, May 2024, https://doi.org/10.1109/TNSE.2024.3363004.

[10] G. A. Sukkar and S. Al-Sharaeh, "Enhancing Security in Wireless Sensor Networks: A Machine Learning-based DoS Attack Detection," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19712–19719, Feb. 2025, https://doi.org/10.48084/etasr.7191.

[11] T. Devapriya, V. Ganesan, and S. Velmurugan, "Efficient Malicious Node Detection in Wireless Sensor Networks using Rabin-Karp Algorithm," *International Journal of Advances in Signal and Image Sciences*, vol. 10, no. 2, pp. 24–36, Dec. 2024, https://doi.org/10.29284/ijasis.10.2.2024.24-36.

[12] G. Ramalingam and P. Uthirapathy, "Optimizing Secure Data Transmission in Cognitive IoT-WSN: An Energy-Aware Approach With Hybrid POA-SCA and Block Chain Technology," *International Journal of Communication Systems*, vol. 38, no. 8, May 2025, Art. no. e70081, https://doi.org/10.1002/dac.70081.

[13] S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, and S. Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network," *Alexandria Engineering Journal*, vol. 72, pp. 37–50, Jun. 2023, https://doi.org/10.1016/j.aej.2023.03.061.

[14] S. E. Mathe, L. Boppana, and R. K. Kodali, "Implementation of Elliptic Curve Digital Signature Algorithm on an IRIS mote using SHA-512," in *2015 International Conference on Industrial Instrumentation and Control*, Pune, India, 2015, pp. 445–449, https://doi.org/10.1109/IIC.2015.7150783.

[15] I. Mustafa *et al.*, "RL-MADP: Reinforcement Learning-based Misdirection Attack Prevention Technique for WSN," in *2020 International Wireless Communications and Mobile Computing*, Limassol, Cyprus, 2020, pp. 721–726, https://doi.org/10.1109/IWCMC48107.2020.9148445.

[16] J. Tang, H. Xu, M. Wang, T. Tang, C. Peng, and H. Liao, "A Flexible and Scalable Malicious Secure Aggregation Protocol for Federated Learning," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4174–4187, 2024, https://doi.org/10.1109/TIFS.2024.3375527.

[17] N. U. Bhanu, S. R. Mallick, S. R. Chappidi, and K. Sangeethalakshmi, "RF-SFAD: A Random Forest Model for Selective Forwarding Attack Detection in Mobile Wireless Sensor Networks," *International Journal of Advances in Signal and Image Sciences*, vol. 11, no. 1, pp. 104–116, Jun. 2025, https://doi.org/10.29284/ijasis.11.1.2025.104-116.

[18] X. Li, L. Zhou, X. Yin, and J. Ning, "A Security-Enhanced Certificateless Designated Verifier Aggregate Signature Scheme for HWMSNs in the YOSO Model," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 10865–10879, Mar. 2024, https://doi.org/10.1109/JIOT.2023.3327505.

[19] A. Mohamed, A. Salama, and A. Ismail, "Enhancing Ad Hoc Network Security using Palm Vein Biometric Features," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 20034–20041, Feb. 2025, https://doi.org/10.48084/etasr.9481.

[20] K. S. Madhuri and J. Mungara, "Reinforcement Learning for Intrusion Detection and Improving Optimal Route by Cuckoo Search in WSN," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 6, pp. 1760–1770, Dec. 2021, https://doi.org/10.21817/indjcse/2021/v12i6/211206024.

[21] "kddcup99 | TensorFlow Datasets." TensorFlow. [Online]. Available: https://www.tensorflow.org/datasets/catalog/kddcup99.