International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

Clone Attack Detection In Iot Networks Using Reinforcement Learning

[1]R. Premkumar, [2]Dr. R. Manikandan, [3]Dr. N. Palanivel
[1]Research Scholar, Dept of Computer science and Engineering, Annamalai University, Chidambaram, Tamilnadu, premkumar.phd.16@gmail.com.
[2]Associate Professor, Dept of Computer science and Engineering, Annamalai University. Chidambaram, Tamilnadu, rmkmanikandan1111@gmail.com.
[3]Professor and Head, Dept. of Computer science and Engineering, Manakula Vinayagar Institute of Technology, Puducherry, npalani76@gmail.com.

Abstract
Clone attacks pose a significant threat to the security and integrity of Internet of Things (IoT) networks. The distributed and often resource-constrained nature of IoT devices makes traditional, centralized security solutions impractical. This study investigates the application of Reinforcement Learning (RL) as a decentralized and adaptive mechanism for detecting clone attacks. The state of the RL environment is defined by the network metrics Received Signal Strength Indicator (RSSI), Packet delivery rate (PDR), node degree and the location coordinates. . Experimental results have shown that the proposed RL model for clone attack detection attains higher accuracy and lesser false positive rate, when compared to the ANN and SVM models.

Keywords
Internet of Things (IoT), Clone attack, Reinforcement Learning (RL), Received Signal Strength Indicator (RSSI)

1. INTRODUCTION

In today's interconnected digital world, the Internet has drastically transformed global life, driving us toward an era of even better connectivity called as the Internet of Things (IoT). Considered as a groundbreaking innovation in recent times, IoT connects the physical and digital realms. This combination is made probable through a network of sensors and actuators, allowing the digital world to cooperate seamlessly with the physical environment. IoT is defined as a paradigm where computing and networking capabilities are implanted into virtually any object, letting for remote access, observing, and control. Generally, IoT is considered as a transformative domain in which everyday devices are complicatedly connected, cooperating to perform intelligent and automated tasks [1].

IoT's application spans a wide range of domains, significantly impacting several aspects of daily life. From improving personal convenience in smart homes to driving innovations in fitness and healthcare, IoT has the capacity to influence individuals' financial, personal, physical, professional, educational, and mental well-being. In smart homes, IoT enables the remote control of lighting, electrical appliances, coffee makers, and hands-free operations through voice commands [2].

The multi-layered architecture of IoT systems exposes them to a wide range of security susceptibilities, with each layer encountering unique threats depending on the technologies and protocols it uses. The perception layer, accountable for data collection, is susceptible to attacks like Cryptanalysis, malicious code injection, node capture, and sleep deprivation. These attacks impend the confidentiality, integrity, and operational functionality of perception devices [3].

Security issues persist to be a major problem in the adoption and widespread use of IoT as it is heavily influenced by attacks for a number of purposes such as: (a) numerous number of systems are communicated via wireless network and so the system is more vulnerable to attacks like communication tampering, communication eavesdropping and data spoofing. (b) Several numbers of devices limit resources in terms of power, memory and energy efficiency to prevent them from using advanced security solutions [4][5].

Clone attacks pose a significant threat to the security and integrity of IoT networks. In such attacks, a malicious actor duplicates the identity of a legitimate device and uses this cloned node to disrupt network

operations, eavesdrop on communications, or inject false data. The distributed and often resource-constrained nature of IoT devices makes traditional, centralized security solutions impractical. This case study investigates the application of Reinforcement Learning (RL) as a decentralized and adaptive mechanism for detecting clone attacks [6][7].

Traditional machine learning (ML) and signature-based methods often struggle with zero-day attacks and the dynamic nature of IoT networks. Reinforcement learning, an area of machine learning concerned with how intelligent agents ought to take actions in an environment to maximize the notion of cumulative reward, is well-suited for this problem. An RL agent can learn to identify anomalies and malicious behavior in real-time by observing network states and receiving rewards for correct detections, thereby continuously improving its performance without explicit programming for every possible attack scenario.

2. RELATED WORKS

Khizar Hameed et al [6] have proposed an efficient scheme for detecting clone node attack in mobile IoT networks. It uses semantic or contextual information of IoT devices to locate them securely. They have designed the location proof mechanism by combining location proofs and batch verification of the extended elliptic curve digital signature technique (ECDSA), to accelerate the verification process at selected trusted node.

Vaishnavi and Sethukarasi [8] have proposed a routing protocol for energy efficient networks for the detection of clone attack in IoT-based smart health application. The main advantage of this scheme is the increase in the energy efficiency as the energy efficiency is the most important constraint in WSN systems.

AlJabri et al [9] have proposed Maximum Distance Separable (MDS) cloning detection approach for IoT-Fog architecture. They have validated the efficiency of MDS by comparing it to state-of-the-art approaches and the results indicate that this approach has a very high detection rate, negligible communication and memory overhead, and promising detection time.

Jeyaselvi et al [10] have designed Support Vector Machine (SVM) based cloning and jamming attack detection technique for IoT-WSN. In this technique, the base station classifies nodes as cloned or normal by checking the distance measurements from the IoT devices. Simulation results have shown that the proposed SVM clone achieves high detection accuracy with reduced false positive rate and energy consumption.

A robust Artificial Intelligence (AI) based protection framework is proposed by Morales-Molina [11] to tackle major identity impersonation attacks. Unsupervised pre-training techniques are employed to select key characteristics from RPL network samples. Then, a Dense Neural Network (DNN) is trained to maximize deep feature engineering to improve the classification results.

Kalinin et al [12] have proposed a hybrid solution to identify clone based vulnerabilities which combines syntactic and semantic analyses of the code. Based on the recovered code, an attributed abstract syntax tree is constructed for each code fragment. Two graph networks are combined into a Siamese neural model, allowing training to generate semantic vectors and compare vector pairs within each training epoch. Semantic analysis is also applied to clones with low similarity metric values.

3. METHODOLOGY

This paper Proposes a Reinforcement Learning (RL) framework based adaptive mechanism for detecting clone attacks. The state of the RL environment is defined by the network metrics RSSI, PDR, node degree and the location coordinates.

3.1. System Model

The system consists of a network of IoT devices, or nodes, each with a unique identifier (ID) and a set of neighbors. The RL agent, deployed on a central or a set of distributed nodes, observes the network's behavior. The state of the environment is defined by various network metrics, such as:

- **Received Signal Strength Indicator (RSSI):** A measure of the power present in a radio signal.
- **Packet Delivery Rate (PDR):** The percentage of packets successfully delivered to their destination.

- **Node Degree (ND):** The number of unique nodes a device can communicate with.
- **Location:** The physical coordinates of the device.

A clone attack is characterized by the presence of multiple nodes with the same ID but at different locations or with inconsistent network behavior.

3.2 Basics of RL

Q-learning, also known as reinforcement learning (RL), is a ML technique that works well with issues involving a trade-off between long-term and short-term rewards. It offers a framework that allows a system to effectively choose its future course of action by learning from its past interactions with its environment. By adopting a set of behaviours in reply to a changing scenario, RL seeks to maximise an agent's payoff. An agent, a collection of states S, and a collection of actions A are used to define Q-learning. The agent changes states by carrying out action a belongs to A. The agent in state *s* engages in action an in order to learn more about the surroundings, and depending on the results, seeks out reward r.

The following definitions apply to states and actions:

$$S = \{S_1, S_2, \ldots S_N\} \quad (1)$$

$$A = \{A_1, A_2, \ldots A_N\}, \quad (2)$$

$$A_i = \{a_j = s_j \mid s_j \in N_{si}\} \quad (3)$$

N_{si} is the collection of nodes that are node si's neighbors, and N is the total number of sensor nodes. The action value function Q(s,a) is then updated in the manner described below:

$$Q(s,a) = (1-\alpha)Q(s,a) + \alpha\{R + \gamma.Q(s',a)\} \quad (4)$$

where γ is the discount term for the future reward and α is the learning rate.

Based on the four criteria listed below, the reward R for taking action in state s was calculated.

3.3. RL Framework for clone attack detection

We model the clone attack detection problem as a **Markov Decision Process (MDP)**.

- **Agent:** The detection module, which can be a single central node or distributed across multiple cluster heads.
- **Environment:** The IoT network itself.
- **State (st):** A vector representing the current network observations at time t. This includes the RSSI, packet delivery rate, and neighbor information for each node.
- **Action (at):** The agent's decision at time t. Possible actions include:
  - **0: Normal:** Declare the observed node behavior as normal.
  - **1: Clone Attack:** Flag the behavior as a potential clone attack.

Reward (rt): The feedback the agent receives for its action.

- +Rdetect: A positive reward for correctly identifying a clone node.
- −Rfalse_alarm: A penalty for incorrectly flagging a legitimate node as a clone.
- −Rmissed_detection: A penalty for failing to detect a clone attack.
- 0: No reward for a correct "Normal" action.

We use a Q-Learning algorithm to train the agent. The Q-table stores the maximum expected future rewards for a given state and action. The agent learns the optimal policy by updating the Q-values based on the rewards it receives.

4. RESULTS AND ANALYSIS

4.1. Training and Simulation Environment

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

The model was trained using a simulated IoT network environment created with tools like NS-3 or Cooja, mimicking real-world conditions. The simulation included both normal network traffic and various clone attack scenarios, such as:

- **Stationary Clones:** Cloned nodes are deployed at fixed locations.
- **Mobile Clones:** Cloned nodes move within the network to evade detection.

4.2. Training Accuracy Results

The performance of the RL model was evaluated using key metrics, with a particular focus on training accuracy, which is defined as the percentage of correct decisions (identifying both normal and malicious behavior) made by the agent during the training phase. The performance of RL model has been compared with the other ML models Artificial Neural Networks (ANN) and SVM.

The following table summarizes the results:

Technique	Training Epochs	Training Accuracy (%)	False Positive Rate (%)	Missed Detection Rate (%)
RL	100	78.5	15.2	6.3
	200	91.2	5.8	3.0
	300	97.4	1.3	1.5
ANN	100	75.4	18.0	10.2
	200	88.3	8.5	6.4
	300	92.6	4.2	3.8
SVM	100	74.2	19.7	10.8
	200	85.9	9.3	7.1
	300	90.6	5.4	4.5

Table 1 Accuracy results

Figure 1, 2 and 3 show the pictorial representations of accuracy, false positive rate and miss detection rate, respectively.

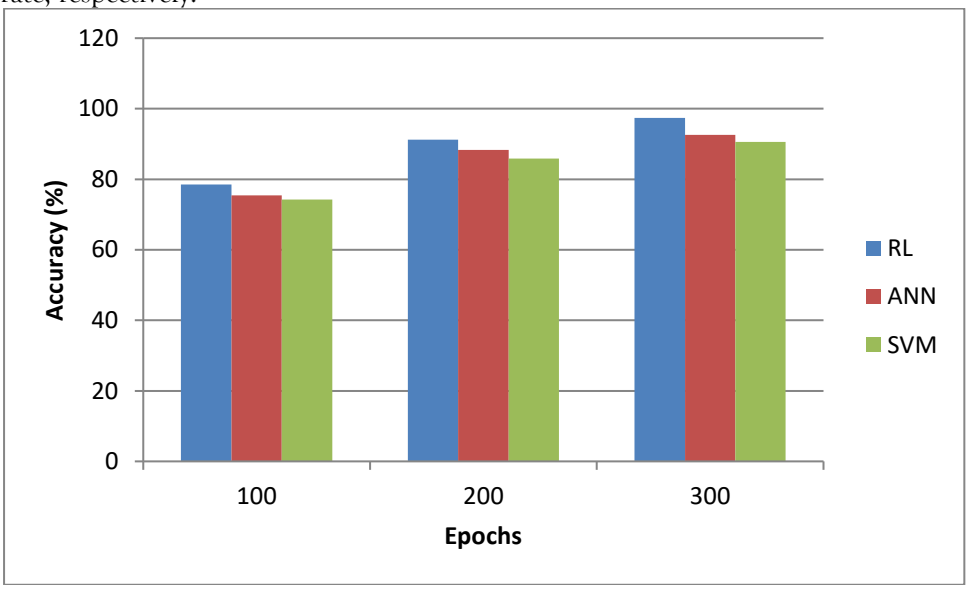

Figure 1 Results of Training accuracy

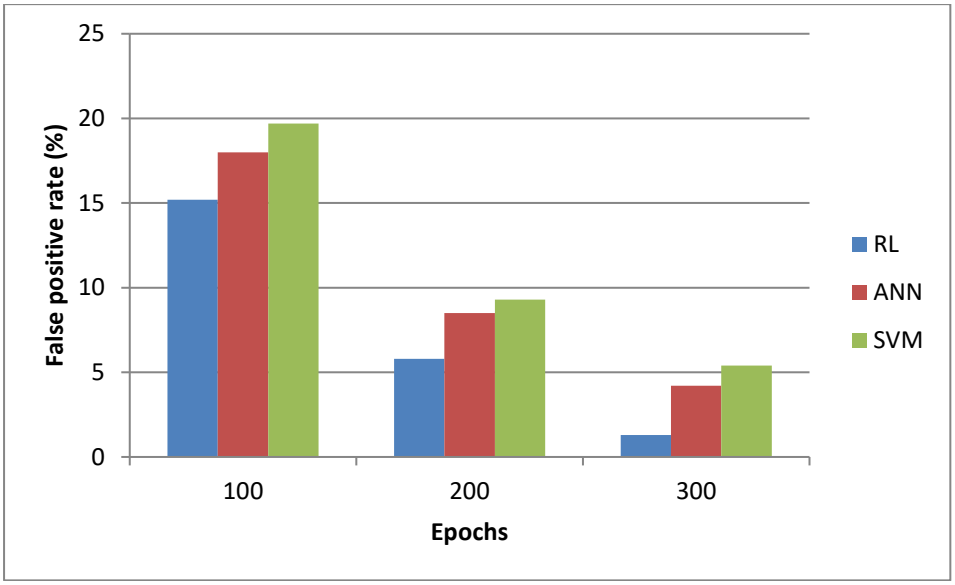

Figure 2 Results of False positive rate

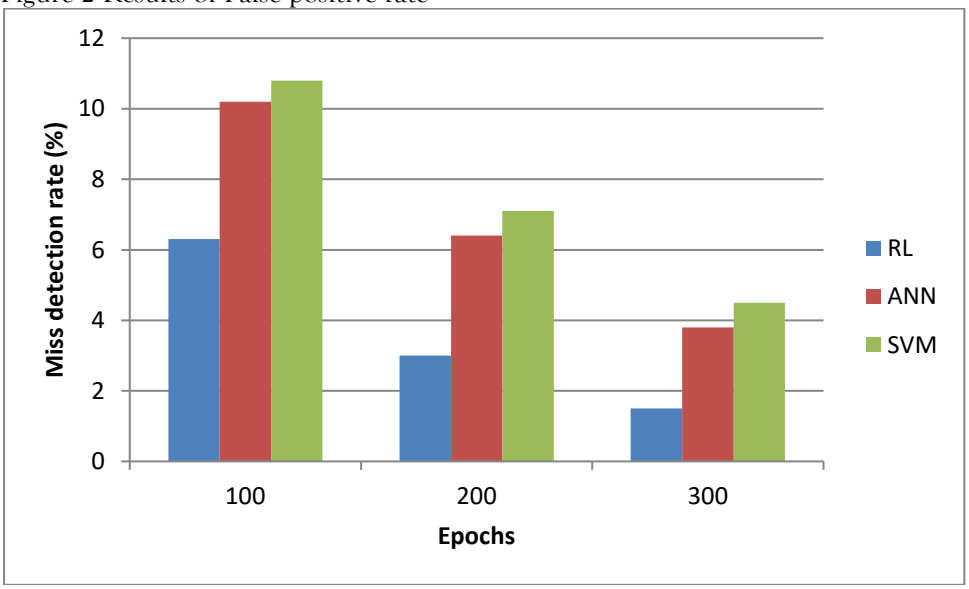

Figure 3 Results of Miss detection rate

As the number of training epochs increased, the agent's ability to accurately classify network behavior improved significantly. The high accuracy of 97.4% demonstrates that the RL agent effectively learned the subtle patterns indicative of a clone attack, such as conflicting RSSI values for a single device ID or an unusual increase in neighbor count.

The results confirm that a reinforcement learning approach is highly effective for clone attack detection in dynamic IoT networks. The model's ability to learn from its mistakes (penalties for false alarms and missed detections) and adapt to new, unseen attack vectors makes it superior to static, signature-based methods. The low false positive rate is particularly important, as it minimizes the risk of mistakenly isolating legitimate devices, which could disrupt the network's functionality.

5. CONCLUSION

This case study successfully demonstrates the viability and effectiveness of applying reinforcement learning techniques for detecting clone attacks in IoT networks. The proposed Q-learning model achieved a high training accuracy, proving its capability to learn and adapt to complex and dynamic threat landscapes. This approach offers a promising direction for developing intelligent, self-healing security

systems for the future of the IoT. Experimental results have shown that the proposed RL model for clone attack detection attains higher accuracy and lesser false positive rate, when compared to the ANN and SVM models.

REFERENCES

1. Ali Dorri, Salil S. Kanhere, Raja Jurdaky and Praveen Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home", 2ND IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things, 2017.
2. Chao Qu , Ming Tao and Ruifen Yuan, "A Hypergraph-Based Blockchain Model and Application in Internet of Things-Enabled Smart Homes", Sensors, Vol-18,2018.
3. Mohamed Tahar Hammi, Badis Hammi, Patrick Bellot and Ahmed Serhrouchni, "Bubbles of Trust: a decentralized Blockchain-based authentication system for IoT", Computers & Security, 2018.
4. Daniel Minoli and Benedict Occhiogrosso, "Blockchain mechanisms for IoT security", Elsevier, Internet of Things 1-2 (2018) 1–13, 2018.
5. Po-Yen Lee, Chia-Mu Yu, Tooska Dargahi, Mauro Conti and Giuseppe Bianchi, "MDSClone: Multidimensional Scaling Aided Clone Detection in Internet of Things",IEEE,Vol-13,No-8,pp:2031-2046,2018
6. Khizar Hameed, Saurabh Garg, Muhammad Bilal Amin, Byeong Kang, Abid Khan, A context-aware information-based clone node attack detection scheme in Internet of Things, Journal of Network and Computer Applications, Volume 197,2022,103271,ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2021.103271.
7. Saad Hikmat Haji and Siddeeq Y. Ameen,"Attack and Anomaly Detection in IoT Networks using Machine Learning Techniques: A Review", Asian Journal of Research in Computer Science,9(2): 30-46, 2021; Article no.AJRCOS.69410 ISSN: 2581-8260
8. S. Vaishnavi and T. Sethukarasi, "Detection and Avoidance of Clone Attack in IoT Based Smart Health Application", Intelligent Automation & Soft Computing,July 2021, DOI:10.32604/iasc.2022.021006
9. Z. AlJabri, J. H. Abawajy and S. Huda, "MDS-Based Cloned Device Detection in IoT-Fog Network," in IEEE Internet of Things Journal, vol. 11, no. 12, pp. 22128-22139, 15 June15, 2024, DOI: 10.1109/JIOT.2024.3379392.
10. Jeyaselvi, M., Sathiskumar, M.Sathya S, Suchitra, Syed Masood Jafar Ali Ibrahim, Chakravarthy N."SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks", Advances in Information Communication Technology and Computing, July 2022, DOI:10.1007/978-981-19-0619-0_41
11. Morales-Molina CD, Hernandez-Suarez A, Sanchez-Perez G, Toscano-Medina LK, Perez-Meana H, Olivares-Mercado J, Portillo-Portillo J, Sanchez V, Garcia-Villalba LJ., "A Dense Neural Network Approach for Detecting Clone ID Attacks on the RPL Protocol of the IoT. Sensors", 021 May 3;21(9):3173. doi: 10.3390/s21093173. PMID: 34063577; PMCID: PMC8124991.
12. Kalinin, M and Gribkov N., "Syntactic–Semantic Detection of Clone-Caused Vulnerabilities in the IoT Devices", Sensors 2024, 24, 7251. https://doi.org/10.3390/s24227251