Systematic Literature Review of Reactive Jamming Attacks Mitigation Techniques in Internet of Things Networks

Enos Letsoalo[1], Topside Mathonsi[2], Tshimangadzo Tshilongamulenzhe[3], Daniel du Duplesis[4]
Department of Information Technology, Tshwane University of Technology, Pretoria, South Africa[1, 2, 3]
Department of Computer Science, University of Johannesburg, Johannesburg, South Africa[4]

***Abstract*—Internet of Things (IoT) networks have become a prevalently exploited research area in academia and industry. IoT networks benefit from a variety of applications, including smart cities, smart homes, intelligent transportation, smart agriculture, monitoring, surveillance, etc. The security challenges associated with IoT networks have been broadly studied in the literature. This systematic literature review (SLR) is aimed at reviewing the existing research studies on IoT networks' reactive jamming attacks, challenges, and mitigation. This SLR examined the research studies published between 2019 and 2024 within the popular electronic digital libraries. We selected 45 papers after a rigorous screening of published works to answer the proposed research questions. The outcomes of this SLR reported three major IoT network performance issues. The results showed that the existing mitigation methods are categorized as machine learning based, deception-based, statistical-based, radio frequency-based, game theory-based, and encryption-based. The results show that most methods can detect reactive jamming attacks with accuracy. However, those methods still require additional infrastructure, encryption systems, and lead to prolonged training delays due to large datasets, resulting in computational overhead and transmission delays. Furthermore, the methods are unable to provide a better defense response to reactive jamming attacks. This is because the methods cannot adequately deal with the increased power consumption of IoT devices, cannot minimize transmission delays, and cannot improve the packet delivery ratio. As a result, reactive jamming attacks continue to be prevalent in IoT networks.**

***Keywords*—IoT networks; reactive jamming attacks; mitigation methods; systematic literature review; electronic digital libraries**

I. Introduction

Internet of Things (IoT) [10] networks are prevalent in distinct application domains that include smart cities, smart homes, intelligent transportation, agriculture, monitoring, etc. Applications of the IoT, such as smart agriculture [1], smart cities [2], and healthcare [3] aim to enhance the quality of life, health, and safety in both rural and urban communities. The demand for these applications is rapidly increasing, leading to a projected count of approximately 29 billion IoT devices by 2030 [4].

IoT networks are vulnerable to reactive jamming attacks (RJA). During reactive jamming, a malicious node sends high-power signals into active channels to disrupt legitimate communication through intentional interference [21]. The technologies such as Bluetooth low energy, RFID, and 802.15.4 have a few shortcomings, namely: they are restricted to communication with short distances, they provide low data rates, and provide low throughput. These technologies are vulnerable to jamming attacks. BLE is susceptible to a reactive narrow-band jammer. This type of jamming attack emits the jamming signal on a single BLE advertising channel when a jammer detects a frame transmission that must be attacked [36].

According to [38], RFID systems' components, such as tags and readers, are considered as single entities, and therefore, DoS attacks by signal jamming in the air interface affect both components. Jamming can result in communication being interrupted, which will make the reading process unavailable. IEEE 802.15.4 is the implementation of WSNs. Jamming of 802.15.4 affects the quality-of-service factors, namely the link quality of the channel, the delivery and delay of packets, and the energy consumption [37]. The widespread use of 802.11ah (Wi-Fi) devices has led to ubiquitous access of information. Jamming of 802.11ah networks can expose the weaknesses of the devices, namely, limited battery life and low processing power [31], [5]. The performance of power-constrained IoT devices is directly impacted by inefficient utilization of their resources.

RJA poses a cybersecurity threat for domains such as business and economy. In industrial intelligent systems, disruption due to RJA can result in financial loss. Smart agricultural systems can be left unmonitored due to communication disruptions. In smart transportation, if the systems are disrupted by RJA, passengers and goods are undelivered, which can lead to the unavailability of services. In real application systems, such as monitoring and surveillance, RJA can disrupt real-time communication.

Prior to this study, there were few survey studies that were done on jamming attacks in wireless networks. The authors in [23] surveyed jamming attacks across all types of wireless networks. The authors in [39] surveyed jamming and anti-jamming techniques in wireless networks. The authors in [40] surveyed jamming attacks in wireless networks. The authors in [41] surveyed jamming mitigation in cognitive radio networks. Unlike previous studies, this study surveys RJA detection and prevention techniques in IoT networks. Furthermore, this research study identified the research gaps left by existing mitigation techniques and proposes a smart channel hopping model to address those gaps.

This research study presents a comprehensive survey on reactive jamming attacks (RJAs) mitigation strategies in IoT networks. This research study will systematically review the papers that are available in the literature relating to challenges posed by jamming attacks, detection of jamming attacks, and mitigating jamming attacks in IoT networks. The research studies that are analyzed are those published in the last five years, i.e., from 2019 to 2024.

The objectives are to offer readers with a holistic knowledge landscape of existing RJAs mitigation techniques. This research also focuses on the performance evaluation of the IoT devices under RJAs. Furthermore, the strengths and weaknesses of the existing RJAs mitigation techniques are presented. The main findings of this research study are that the existing RJAs mitigation techniques can be categorized into six categories. We were able to answer the questions in Section III.

Unlike the previous studies, this study reviews RJAs mitigation techniques in IoT networks. It further categorizes the existing techniques of mitigating RJAs into: Machine learning (ML)-based, deception-based, statistics-based, radio frequency-based, game theory-based, and encryption-based. In addition, this study evaluates the strengths and weaknesses of the techniques using the metrics, namely: power consumption of IoT devices, transmission delays, and packet delivery ratio. The contributions of the study are as follows:

- Firstly, we conduct a survey of existing techniques for mitigating RJAs in IoT networks.
- Secondly, we discuss existing methods for detecting and preventing reactive jamming attacks. We tabulate the results and outline the strengths and weaknesses of the techniques.
- Thirdly, we briefly introduce the smart channel hopping model, which is proposed to address the gaps that were not addressed by the existing mitigation techniques.
- Finally, we provide the conclusion and the future direction of the research.

The rest of the study is organized as follows: Section II discusses research methods, Section III discusses results and discussion, Section IV introduces a technical overview of the smart channel hopping model, and Section V presents the conclusion and future research directions.

II. Research Method

A systematic literature review (SLR) as a research study method was used to assess and interpret the research topics available in the literature. Systematic literature analysis is another choice for SLR. Kitchenham guidelines are more specific for performing this SLR. The SLR procedure for this research study involves three subsections, namely: research questions, search strategy, and studies' inclusion and exclusion criteria.

A. Research Questions

The main objective of this research study is to examine the existing mitigation methods against reactive jamming attacks in IoT networks. This research also focuses on performance evaluation of mitigation strategies from significant existing research studies. To achieve the aims and objectives of this SLR, four research questions were formulated as follows:

- RQ1: What are the existing reactive jamming attacks mitigation methods?
- RQ2: What are the strengths of existing mitigation methods?
- RQ3: What are the limitations of the existing methods?
- RQ4: What are the research gaps left unaddressed by the existing methods?

B. Search Strategy

This section focuses on how the search criteria were conducted in terms of the use of search keywords, electronic sources, reference management tools, and a search strategy. Each process is described in the subsections that will follow:

1) Search keywords: The developed research questions were used to derive the search keywords and strings. We have also included synonyms and alternatives. We took synonym keywords from the relevant literature on reactive jamming attacks in IoT network topics. During the search process, the following keywords were used:

``reactive jamming attacks mitigation in IoT networks", ``reactive jamming attacks ",

``reactive jamming attacks detecting and prevention methods in IoT networks",

``mitigating reactive jamming attacks in IoT networks", ``jamming attacks in IoT networks", "jamming attacks mitigation".

2) Electronic sources: The popular electronic digital libraries were explored to extract the most relevant conference papers and journal articles related to jamming attacks mitigation. Table I shows the list of common digital libraries that have been used to search for research papers and articles.

TABLE I. List of Digital Libraries

Source	URL
IEEE Xplore	www.ieeexplore.org
Research Gate	www.researchgate.net
ACM	www.acm.com
Google Scholars	www.scholar.google.com
Science Direct	www.sciencedirect.com

These digital libraries are the major sources of publications on areas of computer network field.

3) Reference management: The search keywords and their alternative used in above search strategy yielded many studies from the above-mentioned electronic sources. There was no electronic or automatic tool that was used to manage the reference. The process of reference management was done manually.

4) Search process: We launched a search process on the digital libraries to retrieve the relevant literature from journal articles, conference papers, and books. This search process resulted in many studies. This search process was followed by a technique that was applied for the selection process to filter out the irrelevant papers.

C. Criteria for Inclusion and Exclusion of Studies

The criteria for including and excluding the studies is presented in Table II.

TABLE II. INCLUSION AND EXCLUSION CRITERIA

Inclusion criteria	Exclusion criteria
Research studies that discuss reactive jamming attacks mitigation in IoT networks	Research studies that are published before 2019
Research studies that discuss reactive jamming attacks detection and prevention in IoT networks	Research studies that discuss reactive jamming attacks mitigation in other types of networks than IoT network
Research studies that discuss reactive jamming attacks in IoT networks	Research studies that discuss reactive jamming attacks detection and prevention in other types of networks than IoT network
Research studies that discuss anti-jamming in IoT networks	Research studies that discuss reactive jamming attacks anti-jamming in other types of networks than IoT network
Research studies that discuss reactive jamming attacks mitigation in access and sensor IoT networks	Research studies that discuss reactive jamming attacks mitigation in IoT backhaul networks

Fig. 1 shows the filtering process that was executed after the search criteria were applied in the digital electronic libraries above.

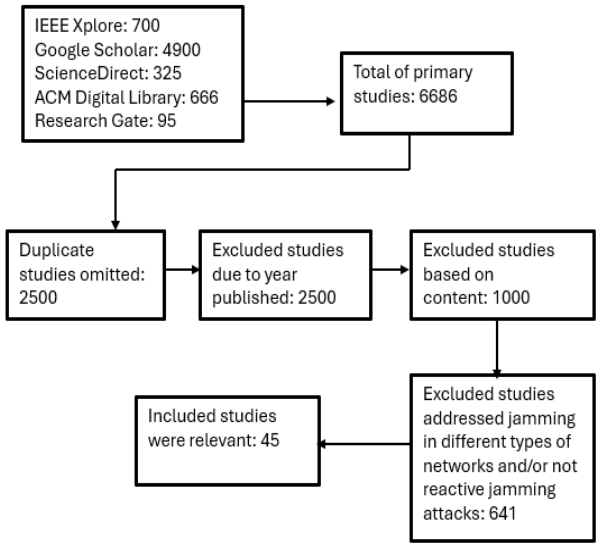

Fig. 1. Selection of studies process.

Fig. 2 presents the distribution of the selected papers by year. We note that 29% of the studies have been published in 2022 and then followed by 24% of the studies published in 2023.

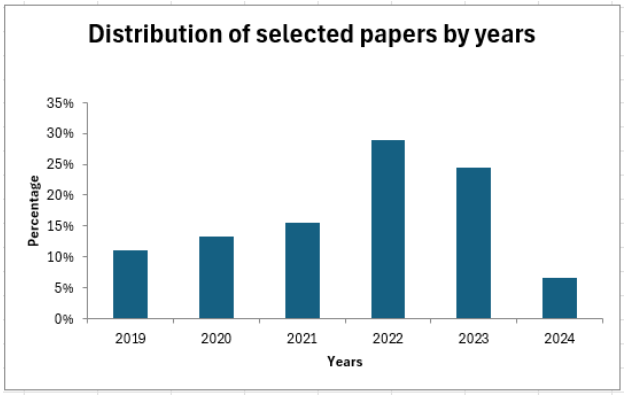

Fig. 2. Distribution of selected papers by years.

III. RESULTS AND DISCUSSIONS

In this section of our SLR, we analyze the most important solutions proposed, including an overview and comparison of categories of existing mitigation methods. Furthermore, analysis of the methods based on the metrics, namely strengths, limitations, the ability to respond to power consumption of IoT devices, transmission delays, and packet delivery ratio.

A. Categories of Mitigation Methods

In this section, the existing mitigation methods against reactive jamming attacks in IoT networks are presented. The techniques are categorized into six categories, namely: Machine learning (ML)-based, deception-based, statistics-based, radio frequency-based, game theory-based, and encryption-based.

1) ML-based methods: ML-based methods are those that employ machine learning techniques to detect and defend against RJAs. These methods utilize machine learning algorithms such as supervised learning. The pre-existing datasets are required for training the agents. They assume that the jammer does not change the jamming strategy, i.e., if the jammer changes the strategy, these methods may falter.

2) Deception-based methods: Deception-based methods use dummy frames or signals to lure the jammer into jamming the fake packets. Some methods use dedicated channels for deceiving the jammer. The transmitter requires to send fake signals prior to sending the real frames.

3) Statistics-based methods: Statistics-based methods use information extracted from the network to detect RJAs. The information may include received signal strength, packet delivery ratio, lack of acknowledgements, and packet error ratio. They lack defense response mechanisms.

4) Frequency-based methods: Frequency-based methods use frequency spectrum techniques for detecting and defending against RJAs. Techniques include patrolling the frequency channel through sensor nodes and using multiple antennas for signal backscattering during jamming attacks.

5) Game theory-based: Game theory-based methods are based on the concept of two players, namely the jammer and the legitimate node, who adjust power levels to defeat each order. Most methods use Q-learning algorithms to obtain the best policy for allocating optimal power to IoT devices to defeat

the jammer. The Q-learning algorithm often takes time to converge when the state space is too large.

6) Encryption-based methods: Encryption-based methods require encryption algorithms to be utilized to defeat reactive jamming attacks. IoT devices are constrained in terms of energy and computation. Therefore, it may not be feasible to implement encryption-based methods.

These mitigation methods are compared in Table III. The metrics that are used are computational overhead, defense response, and resource efficiency. Computational overhead assesses whether the method can be implemented with minimal strain on the energy and computational capacity of IoT devices. Defense response assesses whether the method can effectively mitigate the effects of reactive jamming attacks. Resource efficiency assesses if the method requires additional infrastructure for it to be implemented.

TABLE III. COMPARISON OF METHODS

Method	Computational Overhead	Defense response	Resource efficiency
ML-based	Medium. During agent training	Yes, when jammer not changing strategy.	Efficient
Deception-based	Medium. Frames sent for deception	Yes	Efficient
Statistics-based	Less	No	Efficient
Frequency-based	Medium. Requires sensor nodes and antennas.	Yes	Not Efficient
Game theory-based	Less	Yes, only after convergence	Efficient
Encryption-based	More. It requires encryption algorithms.	Yes	Not Efficient

B. Analysis of Mitigation Methods

This section presents the analysis of mitigation methods based on the metrics, namely strengths, limitations, the ability to respond to power consumption of IoT devices, transmission delays, and packet delivery ratio. Table III provides an analysis of the above-mentioned metrics. In addition, Table IV answers all the research questions raised in Section II A.

TABLE IV. STRENGTHS AND LIMITATIONS

Category	Author	Strength	Limitation	Power consumption	Packet delivery ratio	Transmission delays
Machine learning	Reynvoet et al. (2022)	High accuracy detection	Existing dataset reliance and training delays	Poor consumption due to overhead	Not considered	Increase due to overhead
	Upadyaya et al. (2019)	Detection accuracy	Introduce infrastructure and computational overhead	Poor during data collection and learning	Not considered	Increase due to overhead
(ML)-based	(Zahra et al., 2023)	95% detection accuracy	Training delays and centralized detection centre	Poor during data collection and learning collection and learning	Not considered	Increase due to algorithms complexity
	Lee et al. (2023)	High detection accuracy	Encryption leads to computational overhead	Improves by battery-drainage attack	Improves when users are less	Increases due to encryption
	Testi et al. (2023)	High detection accuracy	No defence response	Not considered	Not considered	Not considered
	Hussain et al. (2022)	86% detection accuracy	No defence response	Not considered	Not considered	Not considered
Deception-based	Thiha et al. (2019)	High detection accuracy	Overhead of sending fake frames	Poor consumption due to sending dummy frames	Improves when packet error ratio drops	Increases due to sending dummy frames
	Liu et al. (2021)	Increase throughput by 50%	Overhead of sending fake frames	Poor consumption due to sending decoy signals	Improves when packet error ratio drops	Increases due to sending decoy signals
	Pourranjbar et al. (2021)	Can efficiently deceive the jammer	Introduce additional channel and overhead of sending fake signals	Poor due to transmission into fake channel	Affects by delays	Increases due to transmission into fake channel
	Nan et al. (2020)	Can efficiently deceive the jammer	Introduce additional channel and overhead of sending fake signals	Improves when system has enough power budget	Not considered	Increases due to transmission into transmitter-receiver pair channel
	Hoang et al. 2020	Low packets drop ratio	Overhead of sending	Poor consumption	Affects by delays	Increases by sending

Category	Author	Strength	Limitation	Power consumption	Packet delivery ratio	Transmission delays
			fake frames			fake frames
	Huynh et al. 2021	Can efficiently deceive the jammer	Energy harvesting and backscattering only possible before channel jamming	Improves by energy harvesting techniue	Improves by backscattering	Increases during energy harvesting process
Statistics-based	Zhang et at. (2022)	High detection accuracy	No defence response	Not considered	Not considered	Not considered
	Singh et al. (2022)	PDR improved by 22%	No defence response	Not considered	Improves by 22%	Not considered
	Fadele et al. (2019)	High detection accuracy	High rates or bit errors and packet loss	Shows 3% power consumption improvement	Improved by 10%	Improved by 38%
	Abdollahi et al. 2023	High detection accuracy	Overhead is caused by states recording and reporting	Recording and reporting will drain the battery	Not considered	Not considered
Radio frequency-based	Arcangeloni et al, (2023)	99% detection accuracy	Introduces additional infrastructure and computational overhead	Poor due to computational overhead	Affects by computational overhead	Increases due to computational overhead
	Huynh et al. (2020)	Throughput can increase with more antennas	Requires more antennas	Poor due to power required by multiple antennas	Improves with addition of more antennas	Increases due backscattering
	Oukas et al. (2023)	99% detection accuracy	Energy harvesting will lead to low PDR	Improves by energy harvesting system	Not considered	Increases due many transition states
	Ali et al. 2023	Detection accuracy	Accuracy is affected by	Not considered	Affects by delays	Increases during NIC data
			NIC's vendor dependency			extraction phase
Game theory-based	Chkirbene et al. (2023)	Optimal power allocation can alleviate jamming attacks	Requires that the jammer does not rapidly change jamming strategy	Not considered	Improves after convergence	Convergence takes longer resulting in delays
	Gouissem et al. (2020)	Optimal power allocation can alleviate jamming attacks	Requires that the jammer does not rapidly change jamming strategy	Not considered	Improves after convergence	Convergence takes longer resulting in delays
	Gouissem et al. (2023)	Optimal power allocation can alleviate jamming attacks	Requires that the jammer does not rapidly change jamming strategy	Not considered	Improves after convergence	Converges faster but assumes jammer never change strategy.
Encryption-based	Navas et al. 2021	Resilient to jamming attacks	Introduces computational overhead dur to encryption	Power consumption due to computation	Affects by transmission delays	Increases due to computation

C. Discussion and Analysis

The ML-based studies proposed by [18], [25], [30], show that the reactive jamming attacks can be detected with high accuracy. However, these methods require that additional infrastructure and/or encryption systems be deployed as defense response mechanisms to the jamming attacks. This will lead to computational overhead which will result in transmission delays and low packer delivery ratio. The studies proposed by [15], [28], [32] indicate that the reactive jamming attacks can be detected with high accuracy. However, the proposed methods lack the defense response systems. This is because there is no mechanism for alleviating reactive jamming attacks when the attacks are detected. In addition, although prior knowledge of an un-jammed signal is unnecessary, ML-based jamming detection has difficulty in obtaining a large amount of training data, and the generalization ability of such

model is usually limited. Moreover, pre-existing datasets have a disadvantage that if the jammer rapidly changes the jamming strategy, they falter.

The deception-based studies proposed by [8], [14], [19], [20], [24], [29] show that sending fake frames into the normal channel or fake channel can deceive the reactive jammer into jamming fake frames. However, this will not be efficient in an environment where the sender must send many frames. This is because the IoT devices will spend more time sending fake frames between transmissions of real frames. This will lead to increased power consumption of power-constrained IoT devices, increased transmission delays of real frames, and a poor packet delivery ratio.

The methods that are proposed by [12], [27] show that reactive jamming attacks [26] can be detected with accuracy. The results show that packet delivery ratio can also be improved. In [27], the authors do not address the issue of power consumption and transmission delays. A study by [12] shows that transmission delays can be slightly improved under low traffic. Power consumption will increase when traffic increases due to congestion and retransmission. The method by [6], [33] shows that reactive jamming attacks can be detected with accuracy. However, the methods do not provide response mechanisms. The study by [6] introduces computational overhead. This is because IoT devices are required to regularly record channel states and send reports to the central node. This will quickly drain the IoT device battery. As a result, the issues of power consumption, packet delivery ratio, and transmission delays were not considered.

The methods proposed by [11], [16], [17] show that reactive jamming attacks can be detected with accuracy. However, the methods introduce additional infrastructure and computational overhead. This will impact transmission delays and packet delivery ratio. The proposed study by [22] achieves better detection accuracy and a response model. But the fact that it consists of many transition states brings several drawbacks, namely transmission delays, high power consumption and reduced packet delivery ratio. The study by [7] shows detection accuracy. However, the process of extracting information from the network interface card will introduce delays. In addition, since the NICs are manufactured by different vendors, this may affect the accuracy of method.

The methods proposed by [13], [34], [35] show that optimal power allocation to IoT devices can drastically reduce jamming attacks. However, these methods require the nodes to adjust or increase their transmission power levels to defeat reactive jammer. In addition, if the jammer has a higher power level, then jamming will not be controlled. Increasing power to the maximum levels will quickly drain the battery of the nodes. If the jammer can rapidly change the jamming strategy this method will fail. Furthermore, the prerequisite of network convergence for obtaining better defense policy may cause delays and affect throughput.

The encryption-based study proposed by [9] shows that the method can be resilient to jamming attacks. The strategy randomizes spread sequences used by the nodes in DSSS system. Every pair of communicating nodes will have a unique pairwise spreading sequence, only known by them. However, the study introduces a lot of computational overhead which will quickly consume the power of IoT devices. In addition, it will lead to transmission delays and low packet delivery ratio.

IV. Proposed Hopping Method

The smart channel hopping model (SCHM) is proposed for mitigating reactive jamming attacks in IoT networks. The formulation of the problem is modeled as the Markov Decision Process framework. The IoT devices interact with the environment and perform different actions in different states and eventually obtain best rewards. In contrast, the penalty reward will be allocated each time a bad action is taken. The next section summarizes the MDP framework for SCHM.

A. State Space

The legitimate IoT node can only observe the chosen channel for communication. Hence, the system's state space is illustrated using the following equation:

$$S = (c, j, q, e): c \in (0,1), j \in (0,1);\ q \in (0, \dots, Q);\ e \in (0, \dots, E)$$

where, c denotes the status of a radio channel, $c = 0$ signifies that a radio channel is idle and $c = 1$ signifies that the radio channel is busy. j denotes the status of the jammer, $j = 0$signifies that the jammer is not attacking a radio channel, $j = 1$ signifies that the jammer is attacking a radio channel. q denotes the number of data frames in the transmission queue, and e denotes the capacity of energy storage of the legitimate node. Q is the maximum data queue size, and E is the maximum capacity of energy storage. The system state space is then expressed as, $s = (c, j, q, e) \in S$.

B. Action Space

The legitimate node can execute any of the following actions, namely, remain idle, actively transmit frames, hop into another free radio channel, and transmit frames, when there is a jamming attack in the current selected channel: $A = (a: a \in \{1,2,3\}$.

a = { 1 the legitimate node remains idle,
2 the legitimate node transmits data,
3 the legitimate node hops into the new channel and transmits data.

C. Reward Function

The immediate reward for the system is defined in this section. It is described as the number of data frames that are sent to the receiver and positively acknowledged. The actions that the legitimate node takes must increase packet delivery ratio with minimum usage of energy and with less delays of the frames in the data queue.

D. Smart Channel Hopping Model

Double Deep-Q-Network (DDQN) is adopted for implementing SCHM. The DDQN reinforcement learning algorithm will be used to train the agent. The proposed model is shown in Fig. 3.

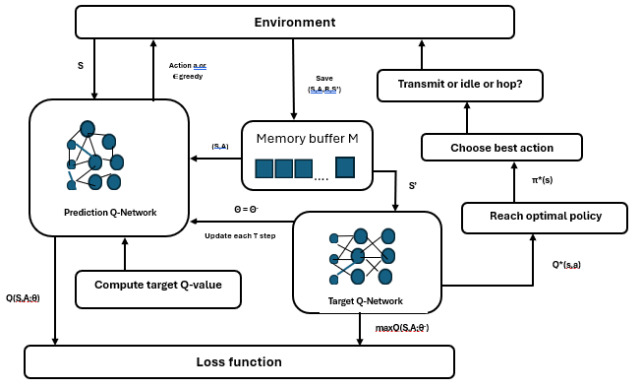

Fig. 3. Proposed smart channel hopping model.

The state space consists of four components, namely channel, jammer, buffer queue, and energy. The components form an important part of the actions that the agent will take during the mitigation process. The action space consists of three components, namely transmit, idle, and hop and transmit. The prediction Q-network, target Q-network, and the memory buffer are initialized. The agent observes the current state and takes the action, and then waits for the reward. Otherwise, it chooses the greedy action argmaxQ(s,a). The state-action pairs are stored in the memory buffer M for each episode. The mini-batch in the memory buffer is used to train the agent. The process continues until the network converges and an optimal policy is found.

V. CONCLUSION

In this research study, a systematic survey of literature review of methods for mitigating reactive jamming attacks in IoT networks was conducted. From the onset, the technologies that support IoT networks were presented. The conventional methods of defending against jamming attacks were discussed. That was followed by the discussion on how the popular online digital libraries were used to obtain conference papers and journal articles related to mitigating reactive jamming attacks. The research questions were raised regarding what the strengths and weaknesses of the existing mitigation methods are. In conclusion, this research study answered the questions.

This research study categorized the jamming mitigation methods into six, namely: Machine learning (ML)-based, deception-based, statistics-based, radio frequency-based, game theory-based, and encryption-based. The mitigation methods were further compared using the metrics, namely, computational overhead, defense response, and resource efficiency. The results in this research study suggest that most mitigation methods have strength of accuracy in detecting jamming attacks. Furthermore, the mitigation methods suffer from increased power consumption, less packet delivery ratio, and prolonged transmission delays.

The limitation of this SLR study is that the search strategy was manual and restricted to journal papers and conference papers. In the near future, the plan is to perform a broad automated search. Another limitation is the use of simplified search keywords for journal papers and conference papers. The use of search keywords can be generalized.

In retrospect, it is required to develop an efficient approach which detects and defends against reactive jamming attacks. As a future work, this research study proposed a smart channel hopping model for mitigating reactive jamming attacks in IoT networks. The model intends to reduce the power consumption of IoT devices, minimize packet errors, minimize packet loss, and minimize transmission delays, which will improve the packet delivery ratio. Furthermore, the research community will have a full knowledge of the limitations of existing RJAs mitigation techniques and will facilitate the advancement of improved mitigation techniques. Lastly, similar SLR studies can be considered for IoT cloud systems for addressing cybersecurity concerns and performance issues.

REFERENCES

[1] BUSINESS INSIDER (2020), Smart farming in 2020: How IoT sensors are creating a more efficient precision agriculture industry. Accessed: May 2025. [Online].Available at: https://www.businessinsider.com/smart-farmingiot-agriculture, 2020.

[2] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities". IEEE IoT journal, 2014.

[3] SEMTECH Smart healthcare. Accessed: May 2025. [Online]. Available at: https://www.semtech.com/lora/lora-applications/smarthealthcare, 2024.

[4] STATISTA (2021), Number of Internet of Things (IoT) connected devices. Accessed: May 2025. [Online]. Available at: https://www.statista.com/statistics/1183457/iotconnected-devices-worldwide/, 2021.

[5] A. Moussa, and I. Jabri, "Impact of RTS/CTS jamming attacks in IEEE 802.11ah dense networks". International Wireless Communications and Mobile Computing (IWCMC), 2021.

[6] M. Abdollahi, K. Malekinasab, W. Tu, and M. Bag-Mohammadi, "Physical-Layer Jammer Detection in Multihop IoT Networks". IEEE Internet Of Things Journal, Vol. 10, No. 23, 1 December 2023.

[7] A.S. Ali, S. Naser, and S. Muhaidat, "Defeating Proactive Jammers Using Deep Reinforcement Learning for Resource-Constrained IoT Networks". IEEE 34th Annual International Symposium on PIMRC, 2023.

[8] N. Huynh, D.T. Hoang, D.N. Nguyen, and E. Dutkiewicz, "DeepFake: Deep Dueling-Based Deception Strategy to Defeat Reactive Jammers". IEEE Transactions on Wireless Communications, VOL. 20, NO. 10, OCTOBER 2021.

[9] R.E. Navas, F. Cuppens, N.B. Cuppens, L. Toutain, and G.Z Papadopoulos, "Physical resilience to insider attacks in IoT networks: Independent cryptographically secure sequences for DSSS anti-jamming". Computer Networks Volume 187, 14 March 2021.

[10] N. Ahmed, D. De, F.A. Barbhuiya, and I. Hussain, "MAC Protocols for IEEE 802.11ah-Based Internet of Things: A Survey". IEEE INTERNET OF THINGS JOURNAL, VOL. 9, 2022.

[11] L. Arcangeloni, E. Testi, and A. Giorgetty, "Detection of Jamming Attacks via Source Separation and Causal Inference". IIE Transactions on Communications, Vol 71, No. 8, 2023.

[12] A.A. Fadele, M. Othman, I.A. Hashem, I. Yaqoob, M. Imran, and M. Shoaib, "A novel countermeasure technique for reactive jamming attack in internet of things", Multimedia Tools and Applications (2019) Vol 78, pp. 29899–29920, September 2019.

[13] A. Gouissem, K. Abualsaud, E. Yaacoub, T. Khattab, and M. Guizani, "IoT Anti-Jamming Strategy Using Game Theory and Neural Network". International Wireless Communications and Mobile Computing (IWCMC), 2020.

[14] D.T. Hoang, D.N. Nguyen, M.A. Alsheikh, S. Gong, E. Dutkiewicz, D. Niyato, and Z. Han, 2020. "Borrowing Arrows with Thatched Boats": The Art of Defeating Reactive Jammers in IoT Networks. Advances in Security And Privacy in Emerging Wireless Networks, 2020.

[15] A. Hussain, N. Abughanam, J. Qadir, and A. Mohamed, "Jamming Attacks in IoT Wireless Networks: An Edge-AI Based Approach", IoT

'22: Proceedings of the 12th International Conference on the Internet of Things pp. 57–64, 2022

[16] N. Huynh, D.T. Hoang, D.N. Nguyen, E. Dutkiewicz, and M. Mueck, "Defeating Smart and Reactive Jammers with Unlimited Power". IEEE on WCNC), DOI: 10.1109/ICC42927.2021.9500391 Jun 2021.

[17] G. Lee, and M. Kim, "Interference-aware Self-optimizing Wi-Fi for high Efficiency Internet of Things in dense Networks". Comput Commun., vols. 89–90, pp. 60–74, Sep. 2016

[18] S.J. Lee, Y.R. Lee, S.E. Jeon, and I.G. Lee, "Machine learning-based jamming attack classification and effective defense technique". Computers and Security Journal, ElSevier, 2023.

[19] Y. Liu, N. QI, Q. Shi, L. Jia, W. Wang, and Z. Huang, "Anti-Reactive-Jamming Wireless System: a Strategy of "Masking". 13th International Symposium on Antennas, Propagation and EM Theory (ISAPE), 2021.

[20] S. Nan, S. Brahma, C.A. Kamhoua, and N.O. Leslie, "Mitigation of Jamming Attacks via Deception". IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications: Track 2: Networking and MAC, 2020.

[21] X Tang, P. Ren, and Z. Han, "Jamming Mitigation via Hierarchical Security Game for IoT Communications". IEEE Access, Journal article, volume 6, 2018.

[22] N. Oukas, M. Boulif, and A. Abbas, "Mitigating Jamming Attacks in IoT RF-Devices through Dynamic Channel Hopping: A Novel Petri-nets Formulation". International Conference on Computer and Applications (ICCA), 2023.

[23] H. Pirayesh, and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey". IEEE Communications Surveys & Tutorials, Volume: 24, Issue: 2, Jan 2021.

[24] A. Pourranjbar, G. Kaddoum, A. Ferdowsi, and W. Saad, "Reinforcement Learning for Deceiving Reactive Jammers in Wireless Networks". IEEE Transactions on Communications, 2021.

[25] M. Reynvoet, O. Gheibi, F. Quin, and D. Weyns, "Detecting and Mitigating Jamming Attacks in IoT Networks Using Self-Adaptation". IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C), 2022.

[26] A.A. Sharah, H.A. Owida, and T.A. Edwan, "Aggressive Jamming Attack in IoT Networks". 4th IEEE MENACOMM, DOI: 10.1109, 2022.

[27] J. Singh, I. Woungang, S.K. Dhurandher, and K. Khalid, "A jamming attack detection technique for opportunistic networks". Science Direct Access, Internet of Things Journal, 2022.

[28] E. Testi, L. Arcangeloni, and A. Giorgetti, "Machine Learning-Based Jamming Detection and Classification in Wireless Networks", WiseML'23: Proceedings of the 2023 ACM Workshop on Wireless Security and Machine Learning, Pages 39–44, June 2023.

[29] K. Thiha, B. Soong, V. Vaiyapuri, and S. Nadarajan, "A new method of defeating reactive jamming: Hardware Design Approach". 14th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2019.

[30] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine Learning-Based Jamming Detection in Wireless IoT Networks", IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS) DOI: 10.1109/APWCS46464, 2019

[31] W. Yin, P. Hu, H. Zhou, G. Xing, and J. Wen, "Jamming attacks and defenses for fast association in IEEE 802.11ah networks". Science Direct Access, Computer Networks Volume 208, 2022.

[32] F. Zahra, Y.S. Bostanci, and M. Soyturk, "Comparative Analysis of Deep Learning Models for Detecting Jamming Attacks in Wi-Fi Network Data", 12th IFIP/IEEE International Conference Evaluation and Modelling in Wired and Wireless Networks (PEMWN), 2023.

[33] L. Zhang, T. Mao, C. Zhang, Z. Xiao, and X. Xia, "Reactive Jamming Detection Based on Hidden Markov Model". IEEE/CIC International Conference on Communications in China (ICCC), 2022.

[34] Z. Chkirbene, R. Hamila, and A. Erbad, "Secure Wireless Sensor Networks for Anti-Jamming Strategy Based on Game Theory". International Wireless Communication and Mobile Computing (IWCMC), 2023.

[35] A. Gouissem, K. Abualsaud, E. Yaacoub, T. Khattab, and M. Guizani, "Accelerated IoT Anti-Jamming: A Game Theoretic Power Allocation Strategy". IEEE Transactions On Wireless Communications, Vol. 21, No. 12, December 2022.

[36] S. Brauer, A. Zubow, S.Z.M. Roshandel, and S. Mashhadi-Soh, "On Practical Selective Jamming of Bluetooth Low Energy Advertising". IEEE Conference on Standards for Communications and Networking (CSCN), 2016.

[37] N. López-Vilos, C. Valencia-Cordero, C. Azurdia-Meza, S. Montejo-Sánchez, and S.B. Mafra, "Performance Analysis of the IEEE 802.15.4 Protocol for Smart Environments under Jamming Attacks". Sensors, Vol 21, No. 12, Jun 2021.

[38] L. Avanco, A.E. Guelfi, E. Pontes, A.A.A. Silva, S.T. Kofuji, and F. Zhou, "An Effective Intrusion Detection Approach for Jamming Attacks on RFID Systems". International EURASIP Workshop on RFID Technology (EURFID), 2015.

[39] K Grover, A Lim, and Q Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," Int. J. Ad Hoc Ubiquitous Comput., vol. 17, no. 4, pp. 197–215, 2014.

[40] S Vadlamani, B Eksioglu, H Medal, and A Nandi, "Jamming attacks on wireless networks: A taxonomic survey," Int. J. Prod. Econ., vol. 172, pp. 76–94, Feb. 2016.

[41] R Di Pietro and G Oligeri, "Jamming mitigation in cognitive radio networks," IEEE Netw., vol. 27, no. 3, pp. 10–15, May/Jun. 2013.