Abstract—Engineers have numerous low-power wireless sensor devices in the current network setup for the Internet of Things, such as ZigBee, LoRaWAN, ANT, or Bluetooth. These low-power wireless sensors are the best candidates to transfer and collect data. But they are all vulnerable to the physical jamming attack since it is not costly for the attackers to run low power jammer sources in these networks. Having multiple gateways and providing alternative connections to sensors would help these networks to mitigate successful jamming. In this paper, we propose an analytical model to solve the problem of gateway selection and association based on a Stackelberg game, where the jammer is the follower. We first formulate the payoffs of both sensor network and attacker and then establish and prove the conditions leading to NASH equilibrium. With numerical investigation, we also present how our model can capture the performance of sensor networks under jamming with a varying number of gateways. Our results show that compared to the single gateway scenario, the network's throughput will improve by 26% and 60% when we deploy two and four gateways in the presence of a single jammer.

Index Terms—Internet of Things (IoT), wireless sensor networks, jamming attack, Stackelberg game

I. INTRODUCTION

Having passed through all the rises and downs, the wireless sensor network (WSN) technology is now in its plateau of productivity with enormous applications in the Internet of things (IoT) era [1]. The WSNs are typically consist of a number of low cost sensors with small, if any, infrastructure support. This “light-weight” feature is the winning bid of WSNs to be adopted in many use-cases such as tracking and monitoring, among others [2].

One of the challenges of WSNs is to maintain the “battery-powered” sensors at the lowest possible expense while prolonging the network life time. Many advances in electronics such as energy-harvesting and RFID circuits have been emerged to respond to this demand. On the other hand, communication protocols, such as BLE, Zigbee, 6TiSCH, and LPWAN (Sigfox, LoRa, NB-IoT, LTE-M etc.), have been introduced for radio energy conservation. However, signaling at low power (whispering), limited resources, and distributed nature make WSNs also vulnerable to security threads, such as flooding, Denial-of-Service (DoS), jamming, and Sybil attacks [3]. In particular, due to low power operation of sensors, jamming attacks to WSNs are inexpensive using commodity hardwares [4].

In jamming attacks, the malicious device (jammer) disturbs the communication link(s) by sending interfering signals. Jamming techniques can take different forms varying in the implementation complexity, energy efficiency, and stealthiness [5]. In active jamming, the jammer sends its interfering signals, regardless of whether any legitimate user is transmitting on the channel or not. On the other hand, in reactive jamming, the jammer first senses the channel to detect/predict when legitimate signals are being transmitted, and then, it may jam the channel.

The authors in [6], [7] studied an OFDM-based downlink scenario in which a jammer allocates its (interfering) power over different subcarriers in a manner that the number of affected devices is maximized. On the other hand, as a countermeasure, the IoT controller can also tune its power allocation across subcarriers to relieve the IoT devices as much as possible. As both the jammer and the controller play with the same resource, i.e., the power across subcarriers, the problem of finding the best strategy is modeled as a Colonel Blotto game. In [8], the jammer first learns the transmission power among a pair of WSN’s users and adjusts its own power for the maximum damage. The problem of finding the optimum power is approached by modeling the problem as a Stackelberg game, and finding its equilibrium. A cognitive radio network under the attack of a smart jammer with inaccurate observation on the power of the secondary user (SU) transmissions has been studied in [9]. Again, this is the transmit power that the jammer/SU may change for the attack/countermeasure and the problem is formulated as a Stackelberg game. In [10], authors highlight the importance of an intelligent defense against jamming attacks by considering a jamming attack on the WSNs which targets both the disruption of the communication and depletion of the sensor’s energy. The attacker and the defender (sensor) are modeled as the players in an asymmetric Bayesian game. The optimal and heuristic strategies, for the attacker and the defender, are derived which determine how much energy to assign to each transmission.

In general, large scale WSNs may have more than one gateway, following a hierarchical architecture: a tier of sensor nodes, and a tier of gateway nodes [11]. To the best of our knowledge, the problem of jamming attacks has not yet been considered in multi-gateway WSNs. Aside from power control, the multi-gateway networks possess a new degree of freedom to combat the jamming attack through suitable (i.e., jamming-aware) sensors-to-gateways association. Thus, the focus of our work in this paper is on the problem of finding the optimal association strategy which maximizes the average packet delivery
rate (PDR) under jamming attacks. The jammer can operate simultaneously in multiple channels, reactively and selectively. In particular, the jammer, in deciding to jam which sensors, is capable of sensing multiple uplink (sensor-to-gateway) channels, predicting the outcome of each choice on the WSN’s PDR, and select the most adversarial action (jamming those channels (sensors) with the worst effect). Our contribution is summarized as follows.

- We propose a general (agnostic to PHY/MAC protocols) probabilistic model to abstract the operation of multi-gateway WSNs in jamming-poisoned environments. Our proposed model considers the locality of the jammers which act based on their measurements.
- We formulate the problem of finding the best strategy for the sensor-to-gateway association under the smart jamming attack as finding the equilibrium point of a Stackelberg game.
- We derive the equilibrium point of the proposed game, which is the solution of a bilevel integer non-linear programming (BINLP). We further reduce the BINLP to an integer linear programming (ILP) which can be fed to general-purpose ILP solvers (e.g., intlinprog, CPLEX, and Gurobi).

We believe that our model can facilitate the analysis of long-term strategic interactions against jammers. This model would be the first step towards a deeper analysis of the learning approach, where we need to obtain more information about an unknown attacker. The rest of the paper is organized as follows. In Section II, the system model is presented and the problem is formulated as a Stackelberg game. In Section III, we derive an ILP to solve the game and find the WSN’s best association strategy. Simulation results are provided in Section IV. Finally, Section V concludes this paper.

II. SYSTEM MODEL AND GAME FORMULATION

In this section, first we present the system model, and the constraints and the objectives of the WSN and the jammer. We then formulate the WSN’s association problem in the presence of a smart jammer as a Stackelberg game.

A. System Model

Figure 1 presents our system model and Table 1 summarizes the notations used throughout the paper. We consider a WSN consisting of $M$ gateway nodes (GN) and $N$ sensor nodes (SN). The GNs are responsible to collect data from SNs, possibly process, and transmit the (extracted) information to a remote controlling entity. Each SN $n \in \mathcal{N} = \{1, 2, \ldots, N\}$ requires to be associated to one GN $m \in \mathcal{M} = \{1, 2, \ldots, M\}$, to which it directly sends its packets. The problem of finding the optimal SN-to-GN association, which maximizes the average packet delivery rate (PDR), can be formulated as:

\[
\text{P1} : \quad \max_{x} \sum_{m=1}^{M} \sum_{n=1}^{N} p_{n,m} x_{n,m}
\]

subject to

\[
\sum_{m=1}^{M} x_{n,m} \leq 1, \quad n \in \mathcal{N} \tag{1-1}
\]

\[
\sum_{n=1}^{N} x_{n,m} \leq \chi_{m}, \quad m \in \mathcal{M} \tag{1-2}
\]

\[
\sum_{m=1}^{M} c_{m} y_{m} \leq \Gamma \tag{1-3}
\]

\[
x_{n,m} \leq y_{m}, \quad m \in \mathcal{M}, \ n \in \mathcal{N} \tag{1-4}
\]

\[
y_{m}, x_{n,m} \in \{0, 1\} \tag{1-5}
\]

where $x = [x_{1,1}, x_{1,2}, \ldots, x_{N,M}]$, $x_{n,m} \in \{0, 1\}$ is a binary variable indicating whether the SN $n$ is associated to GN $m$ ($x_{n,m} = 1$) or not ($x_{n,m} = 0$), $p_{n,m}$ is the probability of successful packet transmission from the SN $n$ to GN $m$, $\chi_{m}$ is the maximum number of SNs that can associate to GN $m$. The problem P1 also considers operational expenditure by including a cost of $c_{m}$ for turning GN $m$ on and the parameter $\Gamma$ as the maximum average operational cost for all gateways. Moreover, $y_{m} \in \{0, 1\}$ shows the on-off state of the GN $m$. By tuning $\Gamma$, the number of GNs which are on can be controlled.

In P1, constraint set (1-1) ensures that each SN is at most associated to one GN. The constraint (1-2) ensures that the number of associated SNs to GN $m$ is less than $\chi_{m}$. Moreover, (1-3) guarantees that the gateways’ average operational cost is less than $\Gamma$ and (1-4) enforces that association with GN $m$ is only possible when GN $m$ is on. It is assumed that GNs have wired/wireless connection to an IoT controller which is responsible for solving the WSN-side problem and sending the result back to the GNs.

In addition to the WSN, a smart jammer node (JN) is also present. The JN operates reactively; it first overhears ongoing links, then selects a set of sensors as the victims, and finally attempts to disrupt the victims’ links by sending the interfering signals. We assume the JN can detect the signal of SN $n$ by

\[\chi_{m}\] depends on the underlying channel bandwidth and multiple access technique (e.g., FDMA, TDMA, and OFDMA) used by GNs to serve their associated SNs.


B. Stackelberg Game Formulation

Although P1 and P2 look like separated problems, they are coupled with the coupling parameters of \( p_{n,m} \) and \( w_n \) in P1 and P2, respectively. Specifically, for the \( p_{n,m} \), we can write

\[
p_{n,m} = a_n v_n + b_{n,m}
\]

where \( p_{n,m} \) is the WSN-measured (true) probability, SPKT\((n,m)\) denotes the event of successful delivery of a packet sent by SN \( n \) to GN \( m \). Let \( a_n = (\tilde{p}_{n,m}^{(1)} - p_{n,m}^{(0)} - p_{m,n}^{(0)}) \leq 0 \), \( b_{n,m} = p_{n,m}^{(0)} \) and \( p_{n,m} = Pr(\text{SPKT}(n,m)|\text{SN} \text{ is not jammed}) \), and \( p_{n,m} = Pr(\text{SPKT}(n,m)|\text{SN} \text{ is jammed}) \). On the other hand,

\[
w_n = \sum_{m=1}^{M} (\tilde{p}_{n,m}^{(1)} - \tilde{p}_{n,m}^{(0)}) x_{n,m},
\]

where \( \tilde{p}_{n,m}^{(0)} \) and \( \tilde{p}_{n,m}^{(1)} \) are the jammer-measured probability of SPKT\((n,m)\) when \( v_n = 0 \) and \( v_n = 1 \), respectively.

Remark 1: Equation (5) is general enough to model different scenarios based on the jammer’s learning power. For instance, the jammer may simply assume that non-jammed transmissions are always successful and jammed ones are always failed (in this case \( w_n \) reduces to \( -\sum_{m=1}^{M} x_{n,m} \)). On the other hand, a much more complex jammer may measure the WSN’s signaling (e.g., ACK/NACK) and data transmissions for a long enough time to precisely learn \( \tilde{p}_{n,m} = p_n p_{m,n} \tilde{p}_m \) and \( \tilde{p}_{n,m} = p_n p_{m,n} \tilde{p}_m \) where \( \tilde{p}_m \) is the probability that the jammer detects the ACK signals sent by GN \( m \).

Remark 2: The parameter \( p_{n,m} \) and \( \tilde{p}_{n,m} \) models the locality of the JN. Some SNs may be hidden to the JN (\( p_n \approx 0 \)) and some may be in its complete detection scope (\( p_n \approx 1 \)). In general, \( p_n \) depends on the state of the wireless channel between the JN and the SN \( n \), the sensitivity of JN’s receiver, and the transmission power of the SN \( n \).

The coupling among the P1 and P2 lays the foundation for casting the problem as a Stackelberg game. In game theory, the Stackelberg model is a strategic game in which two types of players pursue a hierarchy of actions: one player is the leader, and the other is the follower. The leader, as the name suggests, takes its action first. The follower observes the move and chooses the action that maximizes its payoff (i.e., the best response strategy). With a prior knowledge about the follower’s reaction, the leader can opt its own optimum strategy. This leader’s optimal strategy, in combination with the corresponding follower’s best response, is a Stackelberg (Nash) Equilibrium (SE) of the game. In our model, the jammer selects its victims based on the sensors’ contributions in WSN’s average PDR (estimated by the jammer). Therefore, we can model the WSN’s association and gateway scheduling problem in the presence of a smart jammer as a Stackelberg game, \( G^A \).

Definition 1: The Stackelberg Association game \( G^A \) is defined as a triplet \( (P, S, U) \). \( P \) is the set of players including
WSN and jammer, where WSN is the leader and jammer is the follower. \( S \) is the set of strategies, where the strategy of the leader is the association and gateway scheduling scheme and the strategy of the follower is the set of victims. Finally \( U \) is the set of payoff functions, where \( P_1 \) and \( P_2 \) represent the utility functions of the leader and the follower, respectively.

In the following section we analyze game \( G^A \) and obtain Nash equilibria of this game.

III. OPTIMAL ASSOCIATION AND GATEWAY SCHEDULING

In order to analyze game \( G^A \), for a given strategy of the WSN, we derive the best response strategy of the jammer. Then, based on the knowledge of jammer’s strategy, we formulate the optimal strategy of the WSN which identifies a Stackelberg equilibrium (SE) of the game. For a given WSN’s strategy \( x = [x_{1,1}, x_{1,2}, \cdots, x_{N,M}] \), the jammer’s best response is obtained by solving P2 while treating \( x \) as known parameters. The following lemma presents how we can compute the jammer’s best response strategy.

**Lemma 1:** In game \( G^A \), let \( x \) denote a given strategy of the WSN. Then the best response of the jammer is

\[
v_n = \begin{cases} 0 & w_n + \lambda \rho_n > 0 \\ 1 & w_n + \lambda \rho_n \leq 0 \end{cases}
\]

*Proof:* Plugging the given \( x \) into P1 makes all \( w_n, n \in N \), constant and the objective function becomes a linear function of \( v \). As a result, the optimum choice for the binary variable \( v_n \) is 0 when its coefficient, \( w_n + \lambda \rho_n \), is positive and 1, otherwise.

Assuming that the WSN knows the jammer’s best response strategy, given in (6), it can compute its optimal strategy, by solving the following optimization problem.

**ILP – SE :**

\[
\begin{align*}
\text{max } & \sum_{m=1}^{M} \sum_{n=1}^{N} (a_{n,m}v_n + b_{n,m})x_{n,m} \\
\text{subject to } & \sum_{m=1}^{M} x_{n,m} \leq 1, \quad n \in N \quad (7-1) \\
& \sum_{n=1}^{N} x_{n,m} \leq \chi_m, \quad m \in M \quad (7-2) \\
& \sum_{m=1}^{M} c_{m}y_{m} \leq \Gamma \quad (7-3) \\
& x_{n,m} \leq y_{m}, \quad m \in M, \quad n \in N \quad (7-4) \\
& v_{n} = \Pi (-w_n - \lambda \rho_n), \quad n \in N \quad (7-5) \\
& y_{m}, x_{n,m}, v_{n} \in \{0,1\}, \quad m \in M, \quad n \in N \quad (7-6)
\end{align*}
\]

where \( \Pi(\cdot) \) is the unit step function. The problem SE is an integer non-linear optimization problem. But in view of the following lemma, an integer linear programming (ILP) also exists which simplifies finding the WSN’s optimal solution using commercial ILP solvers.

**Lemma 2:** The optimal strategy of WSN is the solution of the ILP-SE problem.

\[
\text{ILP – SE :} \quad \text{max}_{x} \sum_{m=1}^{M} \sum_{n=1}^{N} a_{n,m}z_{n,m} + b_{n,m}x_{n,m}
\]

subject to

\[
\begin{align*}
& \sum_{m=1}^{M} x_{n,m} \leq 1, \quad n \in N \quad (7-1) \\
& \sum_{n=1}^{N} x_{n,m} \leq \chi_m, \quad m \in M \quad (7-2) \\
& \sum_{m=1}^{M} c_{m}y_{m} \leq \Gamma \quad (7-3) \\
& x_{n,m} \leq y_{m}, \quad m \in M, \quad n \in N \\
& v_{n} = \sum_{m=1}^{M} (z_{n,m} - \tilde{z}_{n,m})x_{n,m}, \quad n \in N \quad (7-5)
\end{align*}
\]

where \( z = [z_{1,1}, z_{1,2}, \cdots, z_{N,M}] \).

*Proof:* We can derive ILP-SE from SE taking the following two steps.

Step 1: We replace the non-linear condition (7-5) in SE by

\[
v_{n} \geq -\lambda \rho_n - \sum_{m=1}^{M} (\tilde{z}_{n,m} - \tilde{z}_{n,m})x_{n,m} \quad (9)
\]

The reason is that for the case in which RHS of (9) is positive, both (6) and (7-5) yield \( v_{n} = 1 \) noting that \( v_{n} \in \{0,1\} \). On the other hand, for the case in which RHS of (9) is negative, (7-5) results in \( v_{n} = 0 \), but (6) lets \( v_{n} \) be free \((v_n \text{ can be either 0 or 1})\). However, note that the objective function in SE favors \( v_{n} = 0 \) as \( a_{n,m} \leq 0 \). So again in this case replacing (7-5) by (9) makes no difference.

Step 2: The nonlinear terms in the objective function of SE, in the form of \( v_{n}x_{n,m} \), can be replaced by \( z_{n,m} \) with the following linear conditions:

\[
\begin{align*}
& z_{n,m} \leq (x_{n,m} + v_{n})/2 \quad (10) \\
& z_{n,m} \geq v_{n} + x_{n,m} - 1 \quad (11) \\
& z_{n,m} \in \{0,1\} \quad (12)
\end{align*}
\]

This replacement can also be easily verified by observing that conditions (10), (11), and (12) enforce \( z_{n,m} = v_{n}x_{n,m} \) in all cases where \((v_n, x_{n,m}) = (0,0), (v_n, x_{n,m}) = (0,1), (v_n, x_{n,m}) = (1,0), \) and \((v_n, x_{n,m}) = (1,1)\).

Using Lemma 1 and 2 we can now compute the Nash equilibrium of game \( G^A \) by the following theorem.

**Theorem 1:** The strategy pair \((x^*, v^*)\) is the Stackelberg Equilibrium of the game \( G^A \), where

\[
(x^*, z^*) = \arg \{\text{ILP-SE}\}
\]

and \( v_{n}x_{n,m} = z_{n,m}, n \in N, \) and \( m \in M \).

Note that the jammer needs to know \( w_n, n \in N \) to play its best response, \( v^* \). In practice, the smart jammer may perform learning, measurements and/or eavesdropping the signaling channels in order to obtain such information. On the other hand, to calculate \( x^* \), the WSN also may conduct machine learning methods to detect and identify the strategy of the jammer [12], [13]. Moreover, ILP-SE provides an achievable
Similarly, we can compute \( \pi_{\text{result}} \) based on (14), for the link between the SN \( n \) and the jammer where \( d_{n,m} \) is proportional to \( p_{n,m}^{(0)} \), and (c) the orange links between SNs and GNs under jamming (the width of the edge between SN \( n \) and GN \( m \) is proportional to \( p_{n,m}^{(0)} \)). For the sake of clarity just a few number of links are depicted.

upper bound on the WSN’s performance considering different association and gateway scheduling schemes. Therefore, ILP-SE may serve as an analytical tool for analyzing and designing multi-gateway WSNs in jamming environments.

IV. SIMULATIONS

We now present simulation results that illustrate the performance of multi-gateway WSNs against smart jammers. We consider a Rayleigh flat fading channel model for wireless links. For the successful packet transmission over such a link (with no jamming), we can write

\[
Pr(\text{success}) = 1 - p_{\text{out}}(R) = \exp \left( -\frac{(2^R - 1)}{\text{SNR}} \right)
\]

where SNR is the signal to noise ratio, \( R \) represents the bit rate, \( p_{\text{out}}(R) = Pr\{ R > \log(1 + |h|^2\text{SNR}) \} \) is the outage probability, and \( h \sim CN(0,1) \) is a zero-mean unit-variance complex Gaussian variable which models the Rayleigh fading [14]. On the other hand, in wireless links, the SNR can be modeled as being proportional to \( d^{-\alpha} \) (i.e., \( \text{SNR} \propto d^{-\alpha} \)), where \( d \) is the distance between the transmitter and the receiver, and \( \alpha \) is the path-loss exponent [14]. Assume that \( Pr(\text{success}) = p_{0}^{(0)} \) over a link with the length of \( d_0 \). As a result, based on (14), for the link between the SN \( n \) and GN \( m \), we have

\[
p_{n,m}^{(0)} = \left( p_{0}^{(0)} \right) \left( \frac{d_{n,m}}{d_0} \right)^{\alpha}
\]

where \( d_{n,m} \) is the distance between SN \( n \) and GN \( m \). Similarly, we can compute \( p_{n,m}^{(1)} \) over the link by,

\[
p_{n,m}^{(1)} = \left( p_{0}^{(1)} \right) \left( \frac{r_{n,m}}{r_0} \right)^{\alpha}, \quad p_{n} = p_{0} \left( \frac{D_{n}}{D_0} \right)^{\alpha}
\]

where \( p_{0}^{(1)} \) is the probability of successful packet transmission from a reference point when its signal is jammed and its distance to the destination over that to the jammer is \( r_0 \). Moreover, \( r_{n,m} \) is \( d_{n,m} \) divided by the distance between SN \( n \) and the jammer. In Equation (16), \( p_{0}^{(1)} \) is the probability that the jammer detects the transmission of a sensor located at its \( D_0 \) distance, and \( D_n \) denotes the distance between the SN \( n \) and the jammer, and we have assumed that jammer can detect the transmission of SN \( n \), if its SNR at the jammer location is large enough. In our simulation, the jammer and the SNs are randomly dispersed within the unit square. Unless otherwise specified, we also assume \( \alpha = 4 \), \( p_{0}^{(0)} = 0.7 \), \( d_0 = 0.5 \), \( p_{0}^{(1)} = 0.1 \), \( r_0 = 1 \), \( p_0 = 0.5 \), \( D_0 = 0.5 \), \( \Omega = 1 \), \( \Gamma = 2 \), \( c_m = 1 \) and \( \chi_m = 10 \), \( m \in M \). Fig. 2 depicts an instance of the randomly generated system model with 3 GNs and 30 SNs.

In our simulations, we have used Matlab’s mixed-integer linear programming (intlinprog) solver to find the solution for the ILP problems. Fig. 3 shows the performance, in terms of average packet delivery rate (PDR), of the WSN with 2 GNs (\( M = 2 \)) and different number of SNs with respect to the jammer’s power (the horizontal axis indicates \( 1 - \lambda \) ). Each data point represents the average performance achieved at the Stackelberg equilibrium (i.e., the solution of ILP-SE problem). The results are reported in the form of the average over 100 experiments (iterations). It is observed that PDR decreases as the jammer’s power increases. Specifically, in the low power region of the jammer, PDR approaches to its maximum value of 20 as the maximum number of associated SNs to each GN is 10 (\( \chi_1 = \chi_2 = 10 \)). Moreover, it is observed that as the number of SNs increases the effect of the jammer on the WSN’s performance decreases. In particular, the performance of the WSN changes by 27%, 14%, and 10% when the number of SNs are 20, 40, and 60, respectively. The reason is that as the number of SNs grows the WSN has more options and can select those which their transmitted signals are less polluted by the JN.

Fig. 4 compares the performance of the WSNs with different number of gateways for the same operation cost that allows switching on two gateways (\( \Gamma = 2 \), \( c_m = 1 \), \( m \in M \)). As the benchmark, the performance of a single gateway system
interactions with the jammer is depicted. As it is evident, the best response strategy may not converge (and in the case of convergence, it will converge to the Stackelberg equilibrium).

V. CONCLUSION

Low-power sensor networks are all vulnerable to jamming attacks. In this paper, we have studied the interaction between jammer and wireless sensor networks with several gateways. Using a game-theoretic model, we have derived the optimal strategies of attackers and sensor networks in a Stackelberg setting. Our simulation results show that how increasing the number of gateways can mitigate the jamming attack. In other words, we have shown how we can decrease the impact of jamming attacks by deploying more gateways. A particularly interesting result is that with only three extra gateways, we can increase the network’s throughput by 60% under same jamming attack. The proposed model is the first step towards a deeper understanding of learning in such security scenarios where the attackers and defenders have sequential interactions. For future work, we intend to evaluate such attacks and countermeasures with various learning approaches.

REFERENCES

[1] M. Kocakulak and I. Butun, “An overview of wireless sensor networks towards internet of things,” in IEEE 7th annual computing and communication workshop and conference (CCWC), pp. 1–6, 2017.
[2] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” Computer Networks, vol. 52, no. 12, pp. 2292–2320, 2008.
[3] I. Butun, P. Osterberg, and H. Song, “Security of the internet of things: Vulnerabilities, attacks, and countermeasures,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, 2019.
[4] E. Aras, N. Small, G. S. Ramachandran, S. Delbrueel, W. Joosen, and D. Hughes, “Selective jamming of lorawan using commodity hardware,” in Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services, 2017.
[5] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, “Denial of service attacks in wireless networks: The case of jammers,” IEEE Communications surveys & tutorials, vol. 13, no. 2, pp. 245–257, 2010.
[6] N. Namvar, W. Saad, N. Bahadori, and B. Kelley, “Jamming in the internet of things: A game-theoretic perspective,” in 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6, IEEE, 2016.
[7] A. Gouissem, K. Abualsaud, E. Yaacoub, T. Khattab, and M. Guizani, “Game theory for anti-jamming strategy in multi-channel slow fading iot networks,” IEEE Internet of Things Journal, pp. 1–1, 2021.
[8] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, “Copying with a smart jammer in wireless networks: A stackelberg game approach,” IEEE Transactions on Wireless Communications, vol. 12, no. 8, 2013.
[9] L. Xiao, T. Chen, J. Liu, and H. Dai, “Anti-jamming transmission stackelberg game with observation errors,” IEEE Communications Letters, vol. 19, no. 6, pp. 949–952, 2015.
[10] F. Chiarotti, C. Pelli, N. Laurenti, A. Zanella, and M. Zorzi, “A game-theoretic analysis of energy-depleting jamming attacks with a learning counterstrategy,” ACM Transactions on Sensor Networks (TOSN), vol. 16, no. 1, pp. 1–25, 2019.
[11] A. A. Abbasi and M. Younis, “A survey on clustering algorithms for wireless sensor networks,” Computer communications, vol. 30, no. 14–15, pp. 2826–2841, 2007.
[12] F. Slimini, B. Scheers, Z. Chtourou, and V. Le Nir, “Jamming mitigation in cognitive radio networks using a modified q-learning algorithm,” in International Conference on Military Communications and Information Systems (ICMCIS), pp. 1–7, 2015.
[13] Y. Wu, B. Wang, and K. R. Liu, “Optimal defense against jamming attacks in cognitive radio networks using the markov decision process approach,” in IEEE Global Telecommunications Conference GLOBE-COM 2010, pp. 1–5, 2010.
[14] A. Goldsmith, Wireless communications. Cambridge university press, 2005.