Collaborative Adversarial Modeling for Spectrum Aware IoT Communications

Priyanka Samanta, Elizabeth Kelly, Amina Bashir, Saptarshi Debroy
City University of New York
Emails: *psamanta@gradcenter.cuny.edu*, {*elizabeth.kelly25, amina.bashir80*}*@myhunter.cuny.edu*,
saptarshi.debroy@hunter.cuny.edu

***Abstract*—In order to cater the growing spectrum demands of large scale future 5G Internet of Things (IoT) applications, Dynamic Spectrum Access (DSA) based networks are being proposed as a high-throughput and cost-effective solution. However the lack of understanding of DSA paradigm's inherent security vulnerabilities on IoT networks might become a roadblock towards realizing such spectrum aware 5G vision. In this paper, we make an attempt to understand how such inherent DSA vulnerabilities in particular Spectrum Sensing Data Falsification (SSDF) attacks can be exploited by collaborative group of selfish adversaries and how that can impact the performance of spectrum aware IoT applications. We design a utility based selfish adversarial model mimicking collaborative SSDF attack in a cooperative spectrum sensing scenario where IoT networks use dedicated environmental sensing capability (ESC) for spectrum availability estimation. We model the interactions between the IoT system and collaborative selfish adversaries using a leader-follower game and investigate the existence of equilibrium. Using simulation results, we show the nature of adversarial and system utility components against system variables. We also explore Pareto-optimal adversarial strategy design that maximizes the attacker utility for varied system strategy spaces.**

***Index Terms*—Dynamic spectrum access, Internet of things, collaborative attacks, leader-follower game, selfish adversary.**

I. Introduction

With wider autonomous deployments of potentially large scale Internet of Things (IoT) applications, the access networks will face the burden of hauling large volume of data that these applications produce and consume. Since most of the IoT devices are expected to be connected wirelessly, there will be an unprecedented need for higher capacity wireless networks; where the current operational Industrial, Scientific and Medical (ISM) or licensed bands will fall short. In recent times, dynamic spectrum access (DSA) based secondary (unlicensed) communication has been proposed as a high throughput solution for the growing demands of wireless IoT networks. DSA based solutions are currently being pursued for the growing demands of commercial networks, smart cities with smart vehicular networks and smart grids, and military communications to name a few.

However, the promise of DSA based IoT communications comes at a price due to two broad reasons in particular. First, the dynamic and open philosophy of spectrum sharing amplifies the vulnerabilities of existing IoT applications. Second, new threats may arise due to the inherent DSA vulnerabilities that emerge from dynamic spectrum sensing, and spectrum negotiation. Fig. 1 exemplifies a smart city scenario with DSA based IoT applications with cascading effects triggered from attacks during spectrum sensing. The figure shows a collaborative/organized set of adversaries looking to cripple the IoT operations, choosing to penetrate the network using DSA vulnerabilities. This is particularly true when the underlying DSA functionality of the IoT network uses cooperative spectrum sensing [1] with multi-sensor enabled Environmental Sensing Capability (ESC) [2].

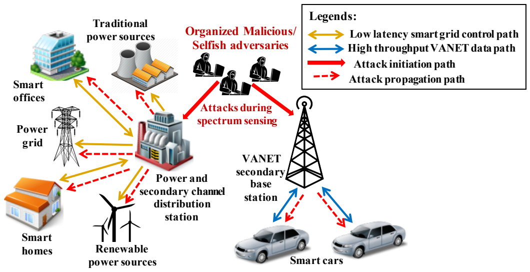

Traditional power sources
Organized Malicious/ Selfish adversaries
Legends:
Low latency smart grid control path
High throughput VANET data path
Attack initiation path
Attack propagation path
Smart offices
Attacks during spectrum sensing
Power grid
VANET secondary base station
Power and secondary channel distribution station
Smart homes
Renewable power sources
Smart cars

Fig. 1: Collaborative attacks by collaborative adversaries on DSA based IoT systems in a Smart City Scenario

Such collaborative adversaries intelligently manipulate sensed spectrum data in order to misguide the Spectrum Access System (SAS) who periodically receives and fuses individual dataset from ESC sensors. As the SAS's ability to perform spectrum availability estimation is critically dependent upon the accurate, local and timely information about spectrum availability, careful and intelligent manipulation by a set of collaborative adversaries working towards a common goal can severely impact the performance of the overlaying IoT network. Such attacks are called Spectrum Sensing Data Falsification Attacks (SSDF). Although research exploration has been made on defense to prevent such attacks, design and analysis of truly intelligent and collaborative attack models and their impact on the IoT network performance are rare. Factors, such as, number of compromised agents, quantization of the spectrum information [3], and overall attack budget can have significant implications on the IoT network; thus warranting careful exploration.

In this paper, we design an intelligent collaborative SSDF attack model and analyze its impact on a DSA based IoT network. We first characterize organized selfish attack strategies, given that the adversaries have some knowledge about the underlying DSA system. In particular, we design a utility based attack model for a given resource budget in a cooperative sensing scenario where collaborative attackers try to inflict maximum damage, yet evade detection. In order to design the attacker utility, we characterize adversarial gain, cost of attack, and attack detection probability based on attack variables. The IoT network or system utility is designed based on secondary usage, successful attack detection probability, and probability of misdetection. The behavioral interaction between the attackers and the system is captured using a leader-follower game where attackers are the follower, selecting strategies in order to maximize their own utility in response to the leader, i.e. system. We analyze the game to prove the non-existence of a Nash Equilibrium (NE) and design Pareto-optimal adversarial strategies based on multiple system strategy-spaces. Finally, using simulations, we show the nature of individual adversarial and IoT network performance metrics with varied attack and system variables. We also validate the existence of Pareto-optimal adversarial strategies through simulation results.

The remainder of the paper is organized as follows. Section II describes the related work. Section III presents our system model. Section IV discusses the steps of our attack model design. Section V presents the leader-follower game design and analysis. Section VI discusses evaluation and results. Section VII concludes the paper.

II. Related Work

There are a number of notable solutions against traditional integrity, confidentiality, and availability attacks in IoT devices, such as [4–7]. Authors in [4] provide a classification of IoT security challenges, e.g., physical, network, software, and encryption attacks. Authors in [5] provide a survey on IoT privacy and security challenges focusing on studying the privacy attributes. In [6], the authors focus on IoT safety measures such as, key management and algorithm, security routing protocol, data fusion technology, and authentication and access control. In [7], authors have surveyed the research status of key technologies used in IoT security including encryption mechanism, communication security, sensor data protection, and cryptographic algorithms. *Most of these works address some specific types of IoT threats based on certain security objectives. In this paper however, we look to investigate the DSA based vulnerabilities on IoT networks.*

Notable works dealing with DSA vulnerabilities in 5G applications include [8–11]. Authors in [8] provide a security analysis on a well established DSA radio developed by Shared Spectrum Company under the DARPA xG program. In [9, 10], the authors propose robust trust models to defend against intelligent SSDF attacks. Authors in [11] show how DSA can cause a new set of challenges when it comes to denial of service (DoS) attacks. *Although these make notable contributions in DSA based application security, very few focus on understanding how the inherent security vulnerabilities of DSA would impact the performance of future 5G IoT networks.*

There are also recent works that deal with DSA based secondary network security and privacy that are applicable for IoT networks [12, 13]. Authors in [12] have focused on PUE attacks in cognitive radio (CR) based IoT networks and proposed an improved energy detection with localization scheme for detecting PUE attacks. Work such as, [13] has proposed trust based defense mechanisms against data falsification attacks. However, most of these works lack of a sophisticated attack model that capture intelligent behavior of collaborative adversaries. *In this paper, we seek to design an intelligent and collaborative SSDF attack on DSA based IoT networks.*

III. System Model and Background

In this paper, we assume a DSA based secondary IoT network that can access the licensed bands in the absence of primary users. We assume the IoT network to use K ESC terminal/nodes to perform cooperative sensing in order to determine the presence of primary in N channels. In a three step cooperative sensing process, the ESC nodes sense the spectrum locally first, take local decision, send the decision to a fusion center (FC), e.g., SAS that makes final decision based on local decisions of multiple such ESCs. The fusion rule used by FC/SAS to decide on each channel's availability based on individual decisions by ESCs on that particular channel can be based on majority voting, K out of N, weighted average, or AND/OR rule.

We assume that FC accumulates quantized PSD values (not raw PSD values) from all K nodes for all N channels and apply the fusion rule. We assume a multi-bit quantized model [13], where quantized thresholds are successively $\Delta, 2\Delta, 3\Delta, \cdots, M\Delta$, $M = 2^B - 1$, $\Delta = (V_{max} - V_{min})/2^B$, and B is the number of bits used to send quantized results after each sensing. Value of Δ is decided based on a centroid ESC node, so that for every other ESC nodes present in the system, for one particular channel, Δ is universal during quantization. If the detected power spectral density (PSD) values belong to a certain interval of quantization, ESC nodes send the corresponding B bit quantized value to the FC. Therefore, periodically FC receives K vectors of N elements with each element being B bits in length.

The collaborative adversaries try to compromise the ESC nodes, more specifically the multi-bit quantized PSD values for each channel emanating from the compromised ESC nodes to exploit the FC fusion rules. The idea is to compromise enough ESC nodes to change the final channel decision by the FC that can significantly affect the secondary IoT communication, yet not getting detected. In our system, we also assume hardware error by ESC nodes (P_{HE}) that work in favor of the collaborative adversaries towards turning the channel decision into their favor. One such example of collaborative attack compromising ESC nodes is depicted in Fig. 2 where compromising only quantized values (here only 1 bit quantization) from two ESCs (ESC1 and ESC5) is sufficient to change the overall decision by FC (which uses a majority voting rule) from available (0) to occupied (1), thus resulting the IoT device not using the channel in spite of the channel being actually available. In this example, the hardware error ESC2 works in favor of the collaborative attackers.

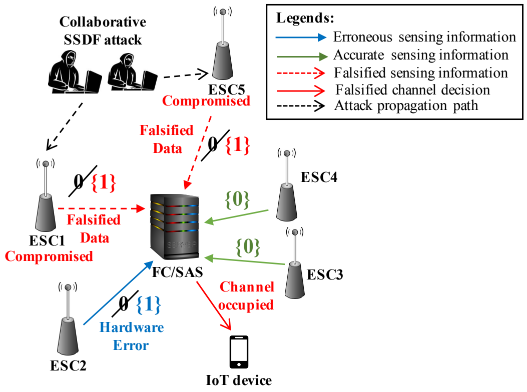


Fig. 2: Compromised ESCs through collaborative SSDF attack cause channel decision change for IoT device exploiting FC/SAS majority voting fusion rule

IV. Collaborative adversarial Model Design

Based on the system model, this paper seeks to design a utility based game theoretic collaborative adversarial model for a secondary IoT network using a cooperative spectrum sensing based DSA environment.

A. Adversarial Gain

As mentioned before, the purpose of the collaborative attackers is underutilization of the channels by the secondary IoT devices, i.e., making sure available channels are considered as occupied by the FC/SAS. With total N channels in the system, we assume that the attackers have a target of attacking N_a channels where $N_a \leq N$ based on attacker objectives and available budget. For a given situation, attackers only have the information about geographic locations of primary transmitters. So when attackers aim to attack any channel, i.e., changing available to occupied, their collaborative strategy will be to attack the channel whose primary is nearer to the region's centroid. Thus, the channels are sorted in descending order according to their sensed PSD values at centroid and the first N_a channels from the list are chosen for attack. In such a collaborative attack model,

$$\textit{Adversarial gain} = \frac{N_{as}}{N_a} \tag{1}$$

where $N_{as} = \sum_{n=1}^{N_a} P_s^n$, i.e., number of channels where attack was successful. Here P_s^n is the attack success probability of channel n and can be computed as

$$P_s^n = \begin{cases} 1 \text{ if } \frac{K_a^n + K_\eta^n}{K} \geq L \\ \quad 0 \text{ otherwise} \end{cases} \tag{2}$$

where L is the FC fusion rule parameter, i.e., the fraction of total votes required for channel occupancy decision. In this model, the attackers have to attack K_a^n number of ESC nodes collaboratively for successfully changing the decision for any n^{th} channel with $K_a^n = K \times L - K_\eta^n$, where K_η^n is the number of honest (non-compromised) ESC nodes whose sensed PSD is higher than the threshold PSD value for primary presence (η^n) including ESC hardware error and/or overlapping signal effects. K_η^n can be expressed as, $K_\eta^n = K \times P_f^n \times P_0^n \times P_{HE\eta}^n + P_\eta^n \times [1 - P_f^n \times P_0^n] \times K$, where P_f^n is the false alarm probability on n^{th} channel, P_0^n is probability of absence of primary in n^{th} channel, P_η^n is the probability that a node with hardware error will cross the threshold η^n, and $P_{HE\eta}^n$ is the probability that the observed PSD will cross the threshold η^n. Thus, Eq. (2) can be rewritten as,

$$P_s^n = \begin{cases} \quad 1 \text{ if } (K_a^n + P_f^n P_0^n P_{HE\eta}^n + P_\eta^n [1 - P_f^n P_0^n]) \geq L \\ \qquad\qquad\qquad 0 \text{ otherwise} \end{cases} \tag{3}$$

B. Cost of attack

Depending on the fusion rule, the attackers have to collaboratively compromise K_a^n ESC nodes in order to sufficiently change the channel's decision. However, to attack the ESC nodes, the attackers incur some cost which is proportional to the number of ESC nodes attacked. Now due to the shadowing and fading characteristics, some ESC nodes will see the lower PSD values than the centroid and some will see higher. At the same time, due to hardware errors, some nodes will observe PSD values different than expected. The attackers will exploit these abnormalities, more specifically exploit ESC nodes that are expected to see higher than usual. This way, the attackers need to compromise less ESC nodes, hence minimizing the cost. If K_{Ta} is the total number of nodes compromised to change decision on N_a channels, then,

$$\textit{Cost of attack} = \frac{K_{Ta}}{K} \tag{4}$$

where $K_{Ta} = P(K_{Ta}) \times K$. Now, the probability for attacking K_a nodes for changing decision on n^{th} channel is given as, $P(K_a^n) = \frac{K_a^n}{K - K_\eta^n}$. Then, using the *inclusion-exclusion identity*, $P(K_{Ta})$ can be easily computed from $P(K_a^n)$.

C. Successful attack detection

Another objective that the attackers is avoiding detection. We assume that the IoT system to have a detection threshold ζ, above which and reported PSD value by the ESC is regarded as an indicator of compromise, and helps the system to detect compromised ESC nodes. More specifically, if the quantized PSD value of an ESC crosses ζ for J out of N number of channels, then the ESC node is identified as compromised and SAS discards that node's reported PSD values for all channels. If we assume κ_d to be the set of successfully detected ESC nodes by the system, then,

$$\textit{Successful attack detection} = \frac{|\kappa_d|}{K_{Ta}} \tag{5}$$

where κ_d is expressed as, $\kappa_d = \{K_{ad}^1 \cap K_{ad}^2 \cdots \cap K_{ad}^n\} \; \forall \; n \in N_a$. Here K_{ad}^n is the number of detected ESC nodes that compromised PSD values on n^{th} channel and can be expressed as $K_{ad}^n = \{P({\kappa_a}^n) \times P_{detection}^n \times k_i\} \; \forall \; k_i \in K \setminus K_\eta^n$, where $P({\kappa_a}^n)$ is the probability of an ESC node to be in the set of successfully detected ESC nodes for channel n, $P_{detection}^n$ the probability of successful detection in channel n.

Based on these three parameters, i.e., *Adversarial gain*, *Cost of attack*, and *Successful attack detection*, we devise an objective function of the collaborative attackers' utility that follows a market-based approach:

$$\begin{aligned} \text{maximize} \quad & U_a = \frac{N_{as}}{N_a} - \frac{K_{Ta}}{K} - \frac{|\kappa_d|}{K_{Ta}} \\ \text{subject to} \quad & 1 \leq N_a \leq N, \; 0 \leq K_{Ta} \leq K, \\ & 0 \leq |\kappa_d| \leq K_{Ta}. \end{aligned} \tag{6}$$

V. Game Formulation

In this section, we first express the IoT network/system utility function and then analyze the effective attacker strategy by designing a *Leader-follower* game model. The system utility has three following components:

Secondary usage: The IoT system's secondary usage is expressed as the utility of any DSA based secondary network in successfully utilizing available channels and that can be expressed as:

$$\textit{Secondary usage} = \frac{N - N_{as}}{N} \tag{7}$$

In order to maximize the secondary usage, the number of successfully attacked channel N_{as} needs to be minimized.

Successful attack detection: This component is the same as in attackers' utility formulation, however, the system will try to increase the attack detection probability by controlling different system parameters. Hence from Eq. (5):

$$\textit{Successful attack detection} = \frac{|\kappa_d|}{K_{Ta}}$$

Misdetection: At the same time, increasing the attack detection probability would also increase the chances of misdetection (when the system is too conservative) which the system would try to avoid. The system strategy can be controlled by choosing J where $1 \leq J \leq N$ with $J = N$ represents highly relaxed system strategy where a ESC node needs to report PSD values greater than ζ for all N channels in order to be regarded as compromised by the system or SAS. Thus, if $|\kappa_{md}|$ is the total number of ESC nodes reporting PSD values above ζ for J or more channels, then

$$\textit{Misdetection} = \frac{|\kappa_{md}|}{K - K_{Ta}} \tag{8}$$

Thus, similar to attacker utility function, the overall system utility is expressed as:

$$\begin{aligned} \text{maximize} \quad & U_s = \frac{N - N_{as}}{N} + \frac{|\kappa_d|}{K_{Ta}} - \frac{|\kappa_{md}|}{K - K_{Ta}} \\ \text{subject to} \quad & 1 \leq N_a \leq N, \; 0 \leq |\kappa_d| \leq K_{Ta}, \\ & 1 \leq J \leq N, 0 \leq |\kappa_{md}| \leq K_{Ta}. \end{aligned} \tag{9}$$

Game Optimization: We design the interactions between the system and the collaborative attackers as a *Leader-follower* game where system leads by deciding on a strategy, i.e., value of J with collaborative attackers following by strategizing with a value of N_a; both trying to maximize their own utility. In a complete information game, J will be a known parameter to the attackers, whereas for partial information game, exact system J will be unknown, however a common knowledge of the range of J is available. We try to find the existence of optimum adversarial strategy for NE. We also explore a

Pareto-optimal adversarial strategies based on multiple system strategy space.

Lemma 1: For an incomplete information game with unknown system strategy J, the optimal attacker strategy is N_a = $\{z|z = n$, where $K_a^n < |K_{ad}^n|\}$ where $z \in \mathbb{Z}$.

proof 1.1: We know from Eq. (6) that the adversarial gain and cost of attack are J independent; but the successful attack detection is J dependent. Thus the attacker should attack only n^{th} channel if and only if ${K_a}^n < |{K_{ad}}^n|$. As $K_{ad}^n = \{P({\kappa_a}^n) \times P_{detection}^n \times k_i\}$ for all $k_i \in \{K\} \setminus K_{\eta}^n$, therefore the term K_{ad}^n is independent of J and hence for any channel n, if ${K_a}^n < |{K_{ad}}^n|$, assuming that the attacker knows ζ^n, the theorem holds for any J set by the system where attacker can guarantee non detection yet success. If the solution space is small then it is possible to calculate ${K_a}^n < |{K_{ad}}^n|$ for the entire game tree and $N_a = \{z|z = countof(n)\}$ is feasible.

Now, if the collaborative adversaries obey this lemma, then they can guarantee zero attack detection. But as ${\kappa_a}^n$ and $P_{detection}^n$ depend on PSD values seen by ESC nodes, for any random distribution of PSD we cannot claim NE. But for any random PSD, $N_a = 1$ is the Pareto optimal solution. This Pareto optimality depends on cost of attack; $N_a = 1$ is the value for which cost of attack will be minimum, independent of any random distribution of PSD. Hence for any system strategy J, there exist an attacker strategy N_a for which adversarial model becomes Pareto optimal.

Lemma 2: For any complete information game with given system strategy J, the optimal attacker strategy $N_a = \{z| \underset{z}{\operatorname{argmin}} |\kappa_d|\}$ where $z \in \mathbb{Z}$.

proof 2.1: For each attacked channel n, the attacker can calculate $K_{ad}^n = \{P({\kappa_a}^n) \times P_{detection}^n \times k_i\}$ for all $k_i \in \{K\} \setminus K_{\eta}^n$. Therefore, if the attacker knows system J, then $|\kappa_d|$ can be truly calculated and thus attacker's strategy should be to minimize $|\kappa_d|$. Thus, the attacker will choose $N_a = z$ that will guarantee the minimum detection $|\kappa_d|$.

Now as κ_a^n depends on the PSD distribution, K_{ad}^n will also depend on the PSD. Hence there cannot exist a NE for a known system strategy J. Again assuming that the attacker knows ζ^n and J both, then the attacker will try to attack at least $J - 1$ channels confidently without worrying about detection. Thus attacker can guarantee non detection yet maximum success. Considering the attacker strategy space and aggressive system strategy J, as N_a is an increasing non-zero integer, $N_a = 1$ will guarantee the best response with minimum detection $|\kappa_d|$ for any known J. Hence for any known system strategy J, there exists an attacker strategy N_a for which adversarial model becomes Pareto optimal.

Lemma 3: For any partial information game range with known ranges of strategy J, if $1 \leq J \leq \frac{N}{2}$, then the optimal attacker strategy $N_a \leq \frac{N}{4}$ and if $\frac{N}{2} + 1 \leq J \leq N$, then the optimal attacker strategy $N_a \leq \frac{N}{2}$.

proof 3.1: If the solution space for N_a is small for small number of N, then according to *Lemma 1*, it is possible to calculate ${K_a}^n < |{K_{ad}}^n|$ for the entire game tree and then $N_a = \{z|z = n$ where ${K_a}^n < |{K_{ad}}^n|\}$ is optimal. But if N is sufficiently large, then it's not possible to calculate ${K_a}^n < |{K_{ad}}^n|$ for the entire game tree and the solution approach has to be an approximation. Given the fact that the attacker knows the range of J, the attacker can approximate N_a to optimize U_a. If J is in *aggressive* range, i.e., $1 \leq J \leq \frac{N}{2}$, then attacker's approach has to be *aggressive* to maximize U_a by trying to maximize the *adversarial gain*, i.e., $\frac{N_{as}}{N_a}$. In such as scenario, the optimal attacker strategy will be $N_a \leq \frac{N}{4}$. In the contrary, if J is *conservative*, i.e., $\frac{N}{2} + 1 \leq J \leq N$, then in order to maximize U_a, attacker's approach should be minimizing *successful attack detection*, i.e., $\frac{|\kappa_d|}{K_{Ta}}$. Hence in this case attacker strategy will be *conservative* in nature, i.e., $N_a \leq \frac{N}{2}$ which is the lower limit of J range.

In this case, no NE exists due to the dependency on PSD, but there exist two Pareto optimal solutions. For $1 \leq J \leq \frac{N}{2}$, if the attacker chooses any strategy $N_a < \frac{N}{4}$, then they may end up minimizing U_a. Considering the best case scenario with upper limit of J ($J = \frac{N}{2}$), the attacker can attack max $N_a = \frac{N}{2}$ channels without getting detected. Now considering the worst case scenario with $J = 1$, the attacker can attack max $N_a = 1$ channels without getting detected. Hence Pareto optimal solution should be the average case, i.e., $N_a = \frac{N}{4}$. Similarly, for the range of $\frac{N}{2} + 1 \leq J \leq N$, the Pareto optimal solution is $N_a = \frac{N}{2}$. Considering the best case scenario with $J = N$, the attacker can attack maximum $N_a = N$ channels without getting detected. And considering the worst case with $J = \frac{N}{2} + 1$, the attacker can attack max $N_a = \frac{N}{2} + 1$ channels without getting detected. Hence Pareto optimal solution should be the average case, i.e., $N_a = \frac{N}{2}$.

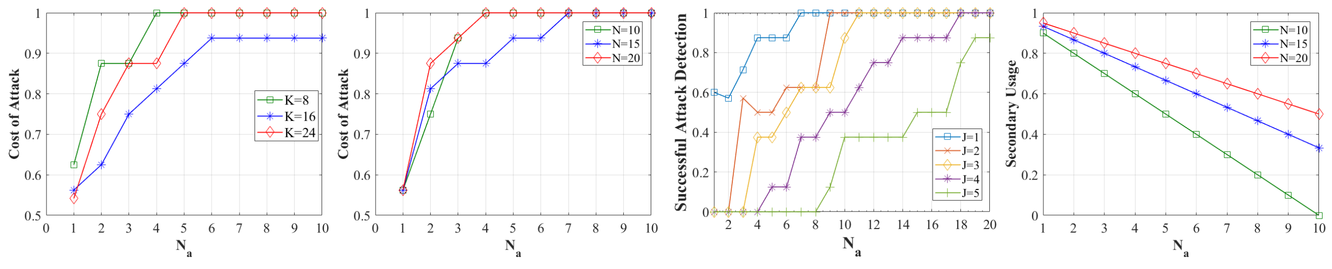
VI. Simulation and Results

We conduct extensive simulation experiments to analyze the impact of coordinated group of selfish adversaries employing our proposed utility based selfish adversarial model on the performance of DSA based IoT applications. In the simulation model, eight ESC nodes are deterministically deployed in a grid pattern with a varying number of channels (10 to 20) in the system with 1 MHz bandwidth each, and the primary detection threshold of -80 dBm to conform with 3.5GHz standard. The sensed PSD values follow a normal distribution with a varying mean (-100 to -60 dBm) and standard deviation of 10 dBm in order to mimic environmental and hardware error effects.

Cost of attack: In Figs, 3(a) and 3(b), we show the nature of cost of attack to compromise ESC nodes against different values of N_a. In Fig. 3(a), we show cost of attack characteristics for different values of K. As expected, for any value of K, cost of attack increases with more channels to be attacked. However, we observe an inflection characteristic for $K = 16$ when the cost of attack is less for any particular N_a than $K = 8$ and $K = 24$. This signifies that there exists an optimal fraction of total number of ESC nodes in the system where irrespective of the channel attack requirement, the cost of attack is minimum. In Fig. 3(b), we show the cost of attack characteristics for varying number of total channels in the system. Similar characteristics are observed where an optimal fraction of total number of channels exists for minimum cost of attack. Thus for collaborative attack objectives that are one-dimensional in nature in terms of minimizing cost of attack, there exist optimal strategies in terms of fraction of total ESC nodes and total number of channels to be attacked.

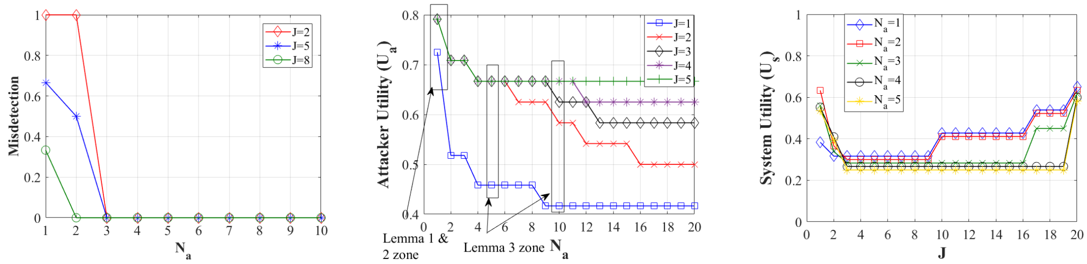
Successful attack detection: In Fig. 3(c), we show the successful attack detection characteristics of compromised ESC nodes vs N_a for different values of system J. It can be observed that as expected, the detection probability increases with N_a. We also observe that for conservative J, even for attacks on a few channels, i.e., 1 or 2, the detection probability is high. However, with more relaxed J, the detection probability is significantly low (less than 20%) for low intensity attacks.

Secondary usage: In Fig. 3(d), we observe that the secondary usage decreases with increasing attack intensity in terms of



(a) (b) (c) (d)

Fig. 3: (a) Cost of attack characteristics for different number of ESC nodes, (b) Cost of attack characteristics for different number of channels, (c) Successful attack detection characteristics for different system strategy J, (d) Secondary usage characteristics for total number of channels in the system



(a) (b) (c)

Fig. 4: (a) Misdetection characteristics for different system strategy J, (b) Attacker utility characteristics for different system strategy J, (c) System utility characteristics for different number of attacked channels N_a

N_a. The system can counter the effect of such decrease by utilizing more available channels in the system provided the attack intensity remains constant.

Misdetection: Fig. 4(a) shows the nature of misdetection of honest ESC nodes for different number of system J. It can be seen that when system J is very conservative, misdetection is rampant for low intensity attacks, i.e., $N_a = 1, 2$. However, for any other range of J, misdetection can be controlled for any attack intensity. This can help the system decide J without worrying too much about misdetection.

Attacker utility: In Fig. 4(b), we show the attacker utility characteristics for different system strategies J. We observe that when system strategy J is not known (from lemma 1), $N_a = 1$ exhibits highest value of U_a. Whereas from lemma 2, when J value is known, then also $N_a = 1$ is Pareto optimal for the collaborative adversaries. If J is in conservative range, i.e., from 1 to 10, then $N_a \leq 5$ exhibits Pareto optimality which is consistent with theoretical findings according to *Lemma 3*. Similarly, for J from 10 to 20, $N_a \leq 10$ shows Pareto optimal strategy that is consistent with the theoretical findings.

IoT system utility: Fig. 4(c) shows system utility characteristics for different values of N_a. It can be observed that when system J is very conservative, the overall system utility is higher than other values of J for any attack intensity. Thus, we can conclude that the secondary IoT system is better off being conservative ($J \leq 2$) than relaxed in order to maximize its own utility.

VII. Conclusion and Future work

In this paper, we made an attempt to understand how inherent DSA vulnerabilities can be exploited by collaborative group of selfish adversaries via intelligent SSDF attacks. Our theoretical and simulation results are consistent in finding Pareto optimal adversarial strategy design in terms of deciding on the number of channels to be attacked at any stage in order to maximize the attacker utility. The results also show that the IoT system is better off being conservative than relaxed in order to maximize its own utility in the event of a collaborative SSDF attack. In future, we will explore other DSA based attacks such as PUE and their effects on secondary IoT networks and also devise effective system strategies in order to counter such intelligent and collaborative adversarial strategies.

References

[1] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical communication*, vol. 4, no. 1, pp. 40–62, 2011.

[2] F. C. Commission *et al.*, "Report and order and second further notice of proposed rulemaking," *Amendment of the Commissions Rules with Regard to Commercial Operations in the*, pp. 3550–3650, 2015.

[3] G. Yang, J. Wang, J. Luo, O. Y. Wen, H. Li, Q. Li, and S. Li, "Cooperative spectrum sensing in heterogeneous cognitive radio networks based on normalized energy detection," *IEEE Transactions on vehicular technology*, vol. 65, no. 3, pp. 1452–1463, 2016.

[4] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *Computers and Communication (ISCC), 2015 IEEE Symposium on*. IEEE, 2015, pp. 180–187.

[5] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the internet of things," in *The Internet of Things*. Springer, 2010, pp. 389–395.

[6] L. Li, "Study on security architecture in the internet of things," in *Measurement, Information and Control (MIC), 2012 International Conference on*, vol. 1. IEEE, 2012, pp. 374–377.

[7] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on*, vol. 3. IEEE, 2012, pp. 648–651.

[8] T. R. Newman, T. C. Clancy, M. McHenry, and J. H. Reed, "Case study: Security analysis of a dynamic spectrum access radio system," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[9] S. Bhattacharjee, S. Debroy, and M. Chatterjee, "Quantifying trust for robust fusion while spectrum sharing in distributed dsa networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 2, pp. 138–154, 2017.

[10] S. Bhattacharjee, S. Debroy, M. Chatterjee, and K. Kwiat, "Utilizing misleading information for cooperative spectrum sensing in cognitive radio networks," in *Communications (ICC), 2013 IEEE International Conference on*. IEEE, 2013, pp. 2612–2616.

[11] G. Jakimoski and K. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks," in *Communications Workshops, 2008. ICC Workshops' 08. IEEE International Conference on*. IEEE, 2008, pp. 524–528.

[12] F. Jin, V. Varadharajan, and U. Tupakula, "Improved detection of primary user emulation attacks in cognitive radio networks," in *Telecommunication Networks and Applications Conference (ITNAC), 2015 International*. IEEE, 2015, pp. 274–279.

[13] M. Jia, X. Wang, Q. Guo, X. Gu, and Z. Yu, "A multi-bit decision cooperative spectrum sensing algorithm in mobile scenarios based on trust valuations in cognitive radio context," in *Wireless Personal Multimedia Communications (WPMC), 2014 International Symposium on*. IEEE, 2014, pp. 335–339.