A Game-Theoretic Framework for Jamming Attacks and Mitigation in Commercial Aircraft Wireless Networks*

David Slater, Patrick Tague, Radha Poovendran
{dmslater, tague, rp3}@u.washington.edu
Network Security Lab (NSL), Department of Electrical Engineering
University of Washington, Seattle, WA 98195, USA

Mingyan Li
Mingyan.Li@boeing.com
Boeing Research & Technology
Bellevue, WA 98008, USA

As wireless personal electronic devices (PEDs) become increasingly ubiquitous, the demand for wireless network services on commercial aircraft is likely to increase. Introduction of services to an aircraft network creates a host of wireless security challenges, whereby a passenger can use a wireless PED to potentially interfere with or jam valid network traffic and future inter-aircraft communications. Aircraft networks will thus require the ability to detect and appropriately respond to jamming attacks. In this work, we investigate the interactions between the aircraft network and jamming PEDs and propose the use of game theory to model jamming attacks and mitigation techniques. We present a game-theoretic framework to model these interactions and delineate tailored response mechanisms to specific threats. We then demonstrate the ability of the network to enforce desired behavior by offering incentives for passenger cooperation and punishments for failing to cooperate.

I. Introduction

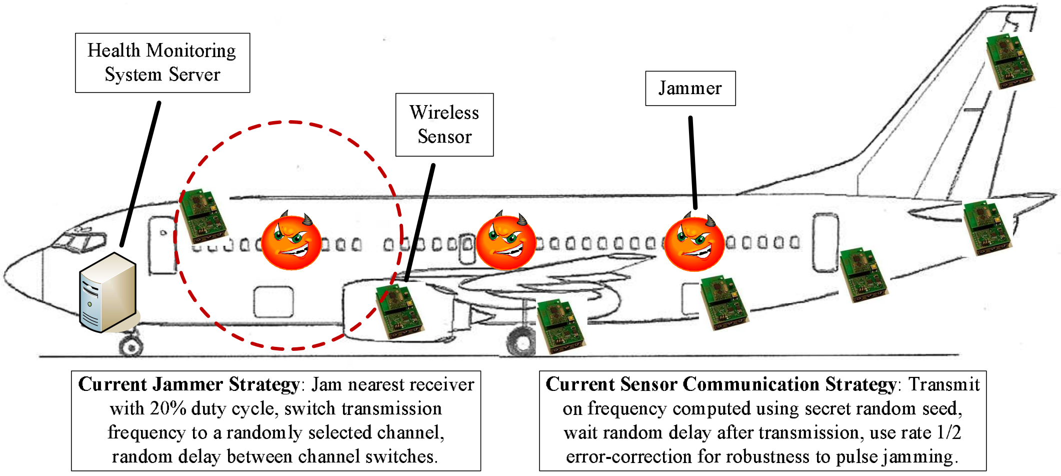
Current trends in networking technology suggest that wireless networked systems will be deployed on next-generation commercial aircrafts, forming essential components of the aircraft's onboard monitoring systems[1,2] as well as providing public Internet access points for airline passengers. Since many wireless personal electronic devices (PEDs) are currently allowed on airplanes (laptops, PDAs, smart phones, etc.) and would be needed to obtain in-flight Internet access, passengers could easily introduce wireless PEDs that intentionally or accidentally interfere with the aircraft's wireless network traffic. This could create security risks to other passengers, and reduce passengers' confidence in the airlines operation, and the aircraft's wireless systems by potentially decreasing the safety margins.[3–5] Vital network components are physically separated from the passenger cabin and cargo by reinforced walls and the cockpit door, and can be virtually separated from passenger wireless access through firewalls and cryptographic protocols. However, the nature of the wireless medium for networked communication introduces critical vulnerabilities into the aircraft's wireless systems, most notably through jamming based denial-of-service (DoS) attacks.[6,7] In such a jamming attack, an adversary injects signals or energy into the communication medium to intentionally interfere with network communication, thereby preventing reception of the intended messages. Such attacks could cripple onboard wireless network functionality and could easily be mounted by permitted wireless PEDs. In order to safely and successfully operate under these conditions, the network must be able to detect, isolate, and eliminate the jamming sources or to mitigate the jamming attack if elimination is impossible (for instance, if the jammer is located in an inaccessible part of the plane such as the cargo hold).

Detection of the jammer may lead to its elimination and possible subsequent prosecution of the offender, depending on the severity of the attack. A naïve strategy such as jamming continuously over a wide frequency band would cause significant disruptions over a short period of time but would also easily be detected, limiting the effectiveness of the approach. Hence, an intelligent jammer who wants to cause significant network disruption may employ sophisticated strategies[8–11] to avoid detection which would otherwise truncate the

*This work is supported in part by the following grants: ARO PECASE, W911NF-05-1-0491, and ARO MURI, W911NF-07-1-0287.

attack duration. Similarly, the aircraft system may choose to modify the communication and networking protocols in order to avoid interference from the jamming transmissions and to improve overall performance in the presence of jamming. Since the network's objective to detect and eliminate jammer activity is clearly divergent from the jammer's objective, we model this interplay using game theory,[12] a powerful tool to analyze the interactions between players with competing goals. In a game, players interact by choosing strategies so as to optimize their own benefit, or payoff, with the knowledge that the other players are selfishly choosing strategies to optimize their own payoffs. In addition, a player may only have partial knowledge of the opponent's profile, consisting of possible strategies and their corresponding payoffs, introducing uncertainly into the model.

The jamming adversary can fit a number of different profiles, depending on its inherent goals, ranging from unintentional interference from a device mistakenly left on by a passenger to targeted high-power jamming by a malicious adversary. Between these extremes are greedy users who attempt to monopolize Internet access by blocking other users and malicious users who seek to deny service to the onboard monitoring systems. Since game-theory rests on the assumption of players demonstrating rational behavior, we constrain our focus to exclude extreme malicious attacks. For a particular profile, an adversary can choose from a large number of strategies by varying the jamming type (random, constant, periodic, reactive, wide-band, narrow-band, etc.)[13] and attack parameters (power, duty cycle, randomization model, jamming schedule, frequency-hopping pattern, etc.). To mitigate jamming attacks, the networked system can similarly choose from a variety of strategies, consisting of the communication protocol used (normal, using anti-jamming techniques[14–18] such as spread spectrum or directional antennas, etc.), the associated parameters, and alerts to flight crew (e.g. alerting crew of a jammer's location), as in the example in Figure 1.



Current Jammer Strategy: Jam nearest receiver with 20% duty cycle, switch transmission frequency to a randomly selected channel, random delay between channel switches.

Current Sensor Communication Strategy: Transmit on frequency computed using secret random seed, wait random delay after transmission, use rate 1/2 error-correction for robustness to pulse jamming.

Figure 1. The interaction between the aircraft health monitoring system and the jamming adversary is illustrated. In the game-theoretic framework, these two parties compete to achieve conflicting performance goals by modifying protocols and parameters.

In this paper, we present a detailed game-theoretic framework to model the interaction between the aircraft networked systems and the jamming adversary interested in denying service to the aircraft systems. This model allows thorough equilibrium and worst-case analysis of the attack and mitigating strategies, which can be used to design optimal response mechanisms, so that the aircraft network can function within desired safety margins even during a worst-case attack. Game theory can be used to quantify the goals and payoffs of both players, allowing the design of protocols that remove all incentives for adversarial jamming. Furthermore, game-theoretic modeling can allow the network to differentiate between adversarial profiles, so that unwanted circumstances such as a false alarm of attack warning due to benign passenger devices can be avoided. To demonstrate the use of the game-theoretic framework, we illustrate an example scenario in which a passenger introduces a wireless PED to jam and effectively monolopize network services. In this study, we consider various attack and mitigation strategies, and analyze the resulting non-cooperative game. Finally, we show how network response strategies can be formulated to ensure optimal network operations.

In Section II we present the network and jamming models and their associated parameters. We present our general game-theoretic framework for jamming attacks and mitigation in Section III. Then in Section IV, we illustrate a specific scenario using our framework and demonstrate the abilty to enforce desired behavior. We conclude in Section V.

II. Network and Jammer Systems

Before addressing the interaction between the aircraft network and the jammers, we first provide an overview of the two systems independently. We introduce the parameters used in the network and jamming models, and describe basic jamming attacks and mitigation tactics.

II.A. Aircraft Wireless Network

We first consider the wireless network on the aircraft system, consisting of several distinct components including next-generation critical inter-aircraft communication systems, sensors for on-board health and system monitoring, and internet access points for passengers and crew. The goal of the network is to provide reliable service to all system components, with an obvious hierarchy in terms of service priority. For example, the network would prioritize critical communication operations over passenger entertainment.

Independently of the access control systems logically separating operational and passenger systems, the aircraft network must be robust to the wide variety of passenger devices brought onto the aircraft,[19,20] due to the resource sharing of the wireless medium. For example, the health monitoring sensor network may operate over a set of frequency bands which is disjoint from those commonly used by PEDs. In order to achieve the desired robustness to the highly variable operation of passenger systems, we consider the operation of a aircraft network that can be dynamically tuned in response to passenger system operation. We let $\mathcal{S}_n$ denote the set of possible operational states of the aircraft network, such that each state $s_n \in \mathcal{S}_n$ completely characterizes the behavior of the system in terms of frequency usage, medium access control, transmission power levels, error correction, etc.

The choice of operational state depends on the presence or absence of interfering or jamming signals. However, to trigger a heightened state of network awareness and choose the appropriate state, the network must be able to reliably detect jamming. We thus assume that collaborative approaches for sensing interference and jamming are employed by the aircraft network using a network of sensors throughout the aircraft,[21] as illustrated in Figure 2. Such a system can characterize the behavior of the jamming attack or localize the source of the interference, potentially alerting flight crew to the location of the jammer.

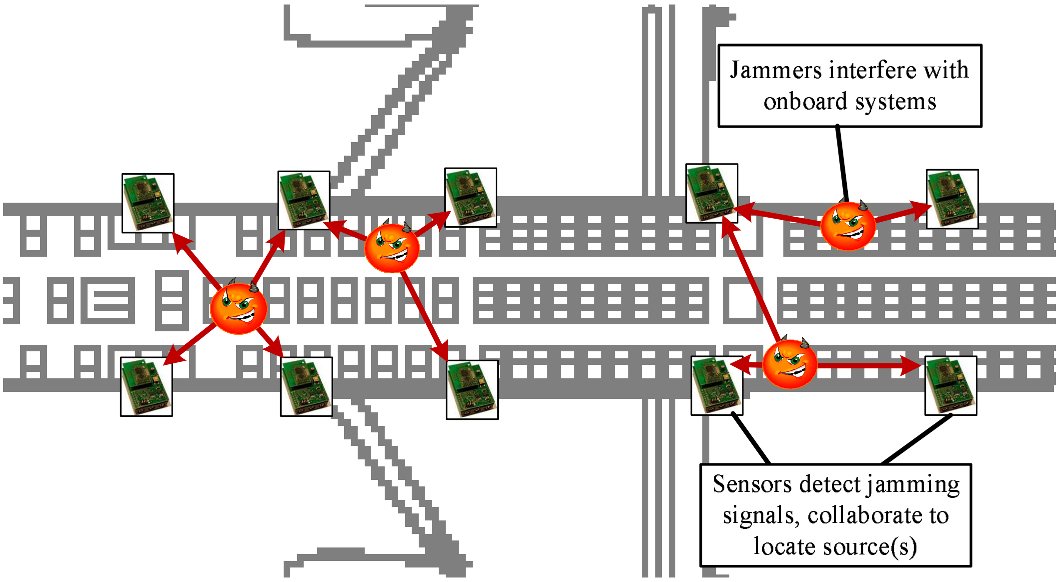

Jammers interfere with onboard systems
Sensors detect jamming signals, collaborate to locate source(s)

Figure 2. The onboard systems may be capable of detecting interfering signals and collaboratively determining the source of the interference.

Using the sensed information about the jammer and interference, the network can choose the appropriate operating state for robustness to jamming. For example, the network can choose an operating state s_n which employs anti-jamming spread spectrum technology,[14] such as direct-sequence spread spectrum (DSSS). Alternatively, the network can selectively employ directional antennas to filter and attenuate interfering signals. Such techniques offer improved reliability of service using secret spreading information or specialized methods, but they require additional overhead in terms of communication bandwidth or hardware complexity.

Hence, there are trade-offs between the reliability of service and the corresponding resource expenditure for different states in $\mathcal{S}_n$. In addition to the resource concerns, however, the operational state of the aircraft network has social influences on the passengers. While safety is the primary concern, it is certainly undesirable to cause unnecessary panic or negative social response through hawkish responses to threat compensation.

II.B. Interfering and Jamming Devices

We next consider the passenger devices which either unintentionally interfere or intentionally jam the communications of the aircraft wireless network. On-board PEDs are in complete control of the passengers and may range from cellular phones to sophisticated high-power jammers. This diversity inherently presents an additional obstacle for the robustness of the aircraft network.

As with the aircraft network, we suppose the jammer operation can be dynamically tuned. We thus let $\mathcal{S}_j$ denote the set of possible operational states of the jammer, such that each state $s_j \in \mathcal{S}_j$ completely characterizes the behavior of the jamming attack. Numerous type of jamming attacks have been proposed, and each has different behavior in terms of resource expenditure, detection, and impact on the target network. For example, jamming devices can transmit constant interfering signals, resulting in high error rates for the target network in trade for a high detection risk. Wideband jamming can be used to reduce the effectiveness of spread spectrum techniques by jamming over a wide range of communication channels, but this increased impact requires significantly more energy than narrorband jamming. Random and periodic jamming techniques[13] allow the jammer to avoid detection by alternating between intervals of active jamming and hibernation. Cross-layer jamming[8,10,11,17] incorporates information from higher layers in the network protocol stack into physical layer jamming, allowing the jammer to reduce resource expenditure by several orders of magnitude, but requiring intimate knowledge of network protocols. Reactive jamming[13] allows the jammer to reduce resource expenditure by only jamming the wireless channel when packet transmissions are detected, though the effectiveness of this technique is limited by network geometry.

Each type of jamming attack has associated parameters, including transmission power, jamming duty cycle, and targeted network components. A certain jamming technique may be more suited to denying service to a wireless access point, while another may be able to accurately target primary communication systems. Finally, the adversary's degree of reluctance towards being detected and subsequently prosecuted will determine to what extent a flight crew alarm could be used as a deterrent.

III. Game-Theoretic Jamming Attacks

The divergent goals of the aircraft wireless network and the jammers lead to the use of game theory for attack modeling and incentive-based jamming mitigation. The goals of the network, in the order of importance, are to ensure passenger safety through reliable inter-aircraft communication, maintain onboard health monitoring and flight crew communication systems, and provide network services to passengers. The jammers' goals could include disabling airline information services (AIS), monopolizing passenger information and entertainment services (PIES), and avoiding detection.

Game theory allows for succinct representation of a diverse array of network and jammer types, goals, and actions and is useful in modeling their interactivity.[12] It further allows the network to provide incentives for desired onboard passenger activity and to effectively enforce those behaviors.

III.A. Game Formulation

To model the interaction between the aircraft network and the jammers, we set up a two-player jamming game. At a given time, the network and the jammers each choose a *strategy* to play and receive a certain *payoff* depending on the chosen strategies. The strategies chosen by the network and jammers correspond to the possible operational states, so each choice is given by a pair $s_{jn} = (s_j, s_n)$ in the set $\mathcal{S} = \mathcal{S}_j \times \mathcal{S}_n$. Each pair s_{jn} has associated costs, risks, benefits, and implications for the network and the jammer. The payoff functions $P_j(s_{jn})$ for the jammer and $P_n(s_{jn})$ for the network combine the benefits and costs associated with the chosen strategy and the effects of the opponents strategy. For example, suppose the jammer chooses the strategy s_j corresponding to no jamming activity and the network chooses the strategy s_n to actively mitigate jamming attacks. In this case, $P_j(s_{jn}) = 0$ because no resources are used and there is no risk of detection, while $P_n(s_{jn}) < 0$ because resources are being used with no benefit.

Since the interaction between the network and jammers is dynamic in time, both players can continually modify their strategies. We thus consider a *repeated game* consisting of a number of *subgames*, each corresponding to the choice of strategies s_j and s_n as above. In a given subgame, the aim of each player is to choose the strategy s_j^* or s_n^* which maximizes the payoff $P_j(s_{jn})$ or $P_n(s_{jn})$. For a particular subgame, a strategy $s^* = (s_j^*, s_n^*)$ is said to be a *Nash Equilibrium* (NE)[12] for that subgame if neither player can increase their payoff by deviating from their present strategy. For example, if $P_j(s^*) = 4$ and $P_n(s^*) = 2$ is a NE for the subgame, then $P_j(s_j, s_n^*) \leq 4$ for all $s_j \in \mathcal{S}_j$ and $P_j(s_j^*, s_n) \leq 2$ for all $s_n \in \mathcal{S}_n$. In other words, the NE corresponds to each player's best response to their opponent's moves. Furthermore, the existence of a NE is guaranteed for any game, possibly involving probabilistic strategies. The interactive nature of the repeated game is illustrated in Figure 3.

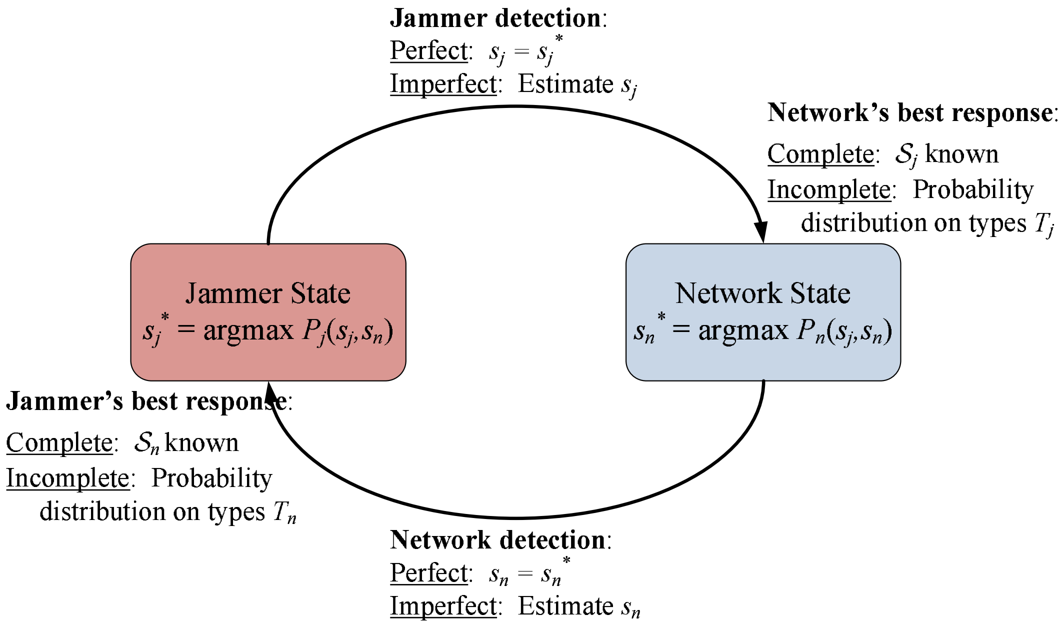

Jammer detection:
Perfect: $s_j = s_j^*$
Imperfect: Estimate s_j
Network's best response:
Complete: $\mathcal{S}_j$ known
Incomplete: Probability distribution on types T_j
Jammer State
$s_j^* = \text{argmax } P_j(s_j, s_n)$
Network State
$s_n^* = \text{argmax } P_n(s_j, s_n)$
Jammer's best response:
Complete: $\mathcal{S}_n$ known
Incomplete: Probability distribution on types T_n
Network detection:
Perfect: $s_n = s_n^*$
Imperfect: Estimate s_n

Figure 3. The interaction between the network and jammers is illustrated as a block diagram, indicating that each of the network's and jammer's strategies is chosen based on the opponent's previously used strategies.

In this repeated jamming game, each player selfishly chooses best-response strategies in an attempt to maximize their payoff over time. From the network's perspective, the goal of the jamming game is to determine if jammers are present, characterize the jamming attack, understand the threat level, and attempt to adequately mitigate the jamming attack. From the jammer's perspective, the goal of the jamming game is to determine the state of the network, degrade the service provided by the network, and avoid detection.

III.B. Effect of Uncertainty in Jamming Games

The outcome of the jamming game depends on the sequence of subgames, each player's knowledge of the opponent's strategies and payoffs, and each player's knowledge of the opponent's chosen strategy. Players are said to have *complete information* about their opponents if the opponent's strategy set and payoffs are known, while they have *incomplete information* if there is uncertainty in the set of strategies and corresponding payoffs. In the context of jamming games, incomplete information may be due to the inability of the network to determine a priori the precise goals of the jammers, the jammers' locations, the capabilities of individual jammers, or even the existence of jammers. On the other hand, the jammer might have limited information about the aircraft specifications, network protocols used, and the threshold for triggering alarms.

Incomplete information can be modeled stochastically by associating a particular *type* with each player, representing the elements of the game that will be unchangable over the duration of the game. For example, players cannot incorporate new strategies or change their perceptions in terms of their payoffs in the middle of the game. Let T_j and T_n represent the sets of possible jammer and network types. By taking into account the populations of potential players (e.g. all potential airlines' passengers, all next-generation commercial aircraft networks), it is possible for each player to derive a probability distribution on their opponent's type, a priori. Players can then update this probability distribution via Bayes Rule, using the additional information retrieved from prior subgames.

Similarly, players are said to have *perfect information* if the opponent's chosen strategy in each subgame is known, while they have *imperfect information* if there is uncertainty in their opponent's chosen subgame strategies. The concepts of perfect and complete information are indicated on the diagram in Figure 3. Since subgame strategies are chosen simultaneously, players are unable to immediately determine their opponents' current strategy, though they can estimate their opponent's prior moves through wireless detection mechanisms. The randomness of the wireless channel coupled with the detection mechanisms of the network and jammer ensure that estimatations of prior moves are imperfect. For example, due to burstiness of ambient noise, a cellular phone signal could be mistaken for that of a high-power jamming device. This information can be interpreted probabilistically in each subgame and updated as more information becomes available. Hence, during each subgame, players update their knowledge of their opponents' types and prior moves to further optimize the payoff.

III.C. Equilibria and Incentive-based Punishments

We model the jamming game as having an *infinite horizon*[12] corresponding to an infinite number of subgames, motivated by the length of a flight being orders of magnitude greater than that of a jamming cycle. Since an infinite summation over the subgame payoffs is likely to diverge, we compare strategies for the entire game via their average payoff per subgame, given by $\lim_{X\to\infty}\sum_{x=1}^{X} P_x/X$, where P_x denotes the payoff of the x^{th} subgame. The implication is that gains from deviating for a finite number of subgames have an insignificant effect on the average payoff, when compared to long-term behaviors. In an infinite horizon game, it is possible to enforce a wide range of behaviors via a *grim trigger strategy*,[22] where at the first sign of deviating behavior, the opposing player will forever switch to the worst-case response to punish the offender, thus nullifying their short-term gain. An example of this would be the network activating an alarm at the first sign of any jamming threat.

By the Folk Theorem,[23] any payoff pair can be enforced as long as it is greater than the worst-case punishment for both players. The worst-case jammer punishment is given by the minimax formulation $\min_{s_n\in\mathcal{S}_n}\max_{s_j\in\mathcal{S}_j} P_j(s_j, s_n)$, and is similarly defined for the network. Nash Equilibria are naturally included in this region, as they are best responses for both players. By threatening a harsh response to any malicious behavior, the network can deter the jamming adversary from mounting aggressive jamming attacks.

Uncertainty from incomplete and imperfect information in the game, where deviations and punishments are probabilistically determined, can restrict the feasible region of the Folk Theorem. Furthermore, randomness in the wireless channel may cause the network to detect a jamming attack when none is present, generating a false alarm. Using the grim trigger strategy, this noise would trigger the worst-case punishment, transitioning the network into a suboptimal state. A resilient punishment strategy can compensate for false alarms by recovering to the original strategy after the supposed offender has been sufficiently punished. Interestingly, by punishing the offending player equivalently to their potential gain for deviation, the feasible region for the Folk Theorem remains unchanged from the grim trigger strategy.

In the case of imperfect information, when knowledge of previous moves is stochastic, players may rely on *brinkmanship* to force a desired solution. Brinkmanship is the act of credibly threatening an opponent with a possibility of devasting response.[24] In the current context, a threat could be that any jamming behavior would probabilistically lead to alarm, due to the escalating interplay between jamming and mitigation strategies. In order to make the threat credible, the network's response can be automated, thus disallowing any sort of rational bargaining between the jammer and the network.

IV. An Example Game

We illustrate the game-theoretic formulation of jamming attacks and mitigation with an example. Here, we take a single jammer type and network type, and show how the network can enforce its optimal payoff.

IV.A. Problem Setup

We focus on the case of complete and perfect information, for ease of presentation. In other words, the network and jammer types and strategies, as well as all moves in previous subgames, are known to both players. The deterministic information thus makes stochastic types and updating unnecessary, directly allowing the use of the Folk Theorem to determine feasible enforcible regions.

We consider the case of a malicious jammer whose goal is to monopolize network resources without being detected. We consider a set $\mathcal{S}_j$ of three strategies j_0, j_1, and j_2, respectively corresponding to no jamming, low-impact jamming, and high-impact jamming. The case of high-impact jamming increases the effectiveness of jamming at the expense of increased risk of detection. We similarly consider a set $\mathcal{S}_n$ of three strategies n_0, n_1, and n_2, respectively corresponding to normal operation, operation with anti-jamming techniques, and activating an alarm. The use of light anti-jamming increases the energy consumption of the network but reduces the effectiveness of the jamming attack, and activating an alarm greatly increases the chance of detecting the jammer but may have negative social impacts on other passengers. For illustration purposes, we suppose the payoff structure of each subgame is given by

	n_0	n_1	n_2
j_0	$(0, 10)$	$(1, 8)$	$(-20, -6)$
j_1	$(10, 2)$	$(2, 5)$	$(-15, -8)$
j_2	$(6, -20)$	$(5, -15)$	$(-10, -10)$,

where each ordered pair indicates the corresponding jammer payoff $P_j(s)$ and network payoff $P_n(s)$.

Let us first examine the subgame NE. First note that the jammer's possible payoffs from playing j_0, {0, 1, -20}, are all respectively lower payoffs than those for playing j_1, {10, 2, -15}. Thus, it can be said that j_1 *strictly dominates* j_0, with the implication that a rational player would never play a strictly dominated strategy. With j_0 removed, the same analysis can be applied to the network side. n_1 now strictly dominates n_0, because from the remaining jammer strategies j_1 and j_2, {5, -15} is strictly greater than {2, -20}. A repeated iteration of strict dominance will remove j_1 and n_1, leaving only (j_2, n_2) as a rational strategy pair. In this state, both players receive -10 as their payoff, but neither can increase their payoff by unilaterally deviating from the current strategy. The state (j_2, n_2) is thus a NE, and this is the only NE for this subgame.

The derivation of the subgame NE allows each player to deduce what strategy is mostly likely to play. Thus, for a game consisting of only one subgame, the only reasonable prediction for an outcome yields a payoff of -10 for both jammer and network. Unfortunately for both players, this is significantly lower than any of the payoffs for strategies (j_0, n_0), (j_0, n_1), (j_1, n_0), or (j_1, n_1). It would thus be desirable for the players to somehow agree on one of these solutions before the series of escalating responses reduces both payoffs.

IV.B. Strategic Enforcement

Since this subgame has an infinite horizon, as seen in Section III.C, it is possible to enforce any strategy as long as it falls within the feasible minimax region. For the jammer, the best responses to the network's strategies are $\{j_1, j_2, j_2\}$ for $\{n_0, n_1, n_2\}$, respectively resulting in payoffs of $\{10, 5, -10\}$. Thus, the worst punitive strategy the network can play is n_2, resulting in a payoff of -10 for the jammer. Likewise, the worst punishment that the jammer can perform is by playing j_2, which results in a payoff of -10 for the network. Thus, the feasible region for equilibria in the repeated game is all strategies that achieve a payoff of at least $(-10, -10)$. The four strategies (j_0, n_0), (j_0, n_1), (j_1, n_0), or (j_1, n_1) would thus become valid solutions.

Since the desired solution for the network is for (j_0, n_0) to be played, we will focus on an equilibrium strategy for that case. Here, the network's strategy is to play n_0 as long as the jammer is playing j_0. If the jammer deviates, then in the next subgame the network will punish the jammer by playing n_2, erasing the benefits of deviating. After this punishment, the network plays n_0 until the jammer deviates again. From the jammer's perspective, it receives an average subgame payoff of 0. By deviating to j_1, it can gain a payoff of 10 for one subgame, but then in the subsequent punishment period, the jammer's best response is j_2, resulting in a subgame payoff of -10. Thus, regardless of which strategy is employed, the average payoff of the jammer is still 0, and the jammer has no incentive to deviate from strategy j_0. The network, on the other hand, has ensured that the jammer has no incentive to deviate from j_0, and can thus enforce it's optimal payoff of 10.

V. Conclusion

In this work we considered wireless vulnerabilities on aircraft introduced by passenger-induced jamming attacks. Due to the ubiquitous nature of wireless PEDs and their increasing prevalence onboard passenger flights, the number of network services available while flying is likely to increase, presenting an array of new security challenges. We presented a general game-theoretic framework which can be used to model a variety of wireless vulnerabilities, network systems, jammer profiles, and mitigation techniques in the presence of uncertain information. This allows us to determine valid network responses and punitive measures to ensure that the offending jammer has no incentive to jam, due to the risk of detection and prosecution. Additionally, it can allow us to fine-tune the countermeasures to minimize the effects of false alarm. We demonstrated the relevance of this approach through an example game. In order to integrate this framework into secure network design, future work will be aimed at identifying and analyzing various network and jammer types and realistically profiling the associated strategies and perceived payoffs.

References

[1] Sampigethaya, K., Poovendran, R., and Bushnell, L., "Secure Operation, Control, and Maintenance of Future e-Enabled Airplanes," *Proc. IEEE*, Vol. 96, No. 12, Dec. 2008, pp. 1992–2007.

[2] RTCA SC-2002, "Guidance on Allowing Transmitting Portable Electronic Devices (T-PEDs) on Aircraft (RTCA/DO-294C)," Dec. 2008.

[3] Olive, M. L., Oishi, R. T., and Arentz, S., "Commercial Aircraft Information Security: an Overview of ARINC Report 811," *Proc. 25th IEEE/AIAA Digital Avionics Systems Conference (DASC'06)*, Oct. 2006, pp. 1–12.

[4] Wargo, C. A. and Dhas, C., "Security Considerations for the e-Enabled Aircraft," *Proc. 2003 IEEE Aerospace Conference*, March 2003, pp. 4–1533–4–1550.

[5] Thanthry, N. and Pendse, R., "Aviation Data Networks: Security Issues and Network Architecture," *Proc. 38th Annual International Carnahan Conference on Security Technology*, Oct. 2004, pp. 77–81.

[6] Anderson, R., *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, Inc., 2001.

[7] Wood, A. D. and Stankovic, J. A., "Denial of Service in Sensor Networks," *IEEE Computer*, Vol. 35, No. 10, Oct. 2002, pp. 54–62.

[8] Bellardo, J. and Savage, S., "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," *Proc. USENIX Security Symposium*, Washington, DC, Aug. 2003, pp. 15–28.

[9] Li, M., Koutsopoulos, I., and Poovendran, R., "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks," *Proc. 26th IEEE International Conference on Computer Communications (INFOCOM'07)*, May 2007, pp. 1307–1315.

[10] Lin, G. and Noubir, G., "On Link Layer Denial of Service in Data Wireless LANs," *Wireless Communications and Mobile Computing*, Vol. 5, No. 3, May 2005, pp. 273–284.

[11] Thuente, D. J. and Acharya, M., "Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks," *Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM'06)*, Washington, DC, Oct. 2006, pp. 1–7.

[12] Fudenberg, D. and Tirole, J., *Game Theory*, MIT Press, 1991.

[13] Xu, W., Ma, K., Trappe, W., and Zhang, Y., "Jamming Sensor Networks: Attack and Defense Strategies," *IEEE Network*, Vol. 20, No. 3, May/June 2006, pp. 41–47.

[14] Fazel, K. and Kaiser, S., *Multi-Carrier and Spread Spectrum Systems*, Wiley, 2003.

[15] Poisel, R. A., *Modern Communication Jamming Principles and Techniques*, Artech House, 2004.

[16] Chan, A., Liu, X., Noubir, G., and Thapa, B., "Control Channel Jamming: Resilience and Identification of Traitors," *Proc. IEEE International Symposium on Information Theory (ISIT'07)*, Nice, France, June 2007.

[17] Tague, P., Li, M., and Poovendran, R., "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," *Proc. 18th Annual IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'07)*, Athens, Greece, Sept. 2007.

[18] Xu, W., Trappe, W., and Zhang, Y., "Channel Surfing: Defending Wireless Sensor Networks from Interference," *Proc. 6th International Conference on Information Processing in Sensor Networks (IPSN'07)*, Cambridge, MA, USA, April 2007, pp. 499–508.

[19] Bird, G., Christensen, M., Lutz, D., and Scandura, P., "Use of Integrated Vehicle Health Management in the Field of Commercial Aviation," *Proc. NASA ISHEM Forum*, Nov. 2005.

[20] Harman, R. M., "Wireless Solutions for Aircraft Condition Based Maintenance Systems," *Proc. 2002 IEEE Aerospace Conference*, March 2002, pp. 6–2877–6–2886.

[21] Woods, R., Ely, J. J., and Vahala, L., "Detecting the use of Intentionally Transmitting Personal Electronic Devices Onboard Commercial Aircraft," *Proc. 2003 IEEE International Symposium on Electromagnetic Compatibility*, Aug. 2003, pp. 263–268.

[22] Green, E. J. and Porter, R. H., "Noncooperative Collusion under Imperfect Price Information," *Econometrica*, Vol. 52, No. 1, Jan. 1984, pp. 87–100.

[23] Rubenstein, A., "Equilibrium in Supergames with the Overtaking Criterion," *Journal of Economic Theory*, Vol. 21, No. 1, Aug. 1979, pp. 1–9.

[24] Dixit, A. K. and Nalebuff, B. J., *Thinking Strategixially: The Competitive Edge in Business, Politics, and Everyday Life*, W. W. Norton & Company, Inc., 1991.