Postprint of: Konorski J., Szott S., Credibility of Threats to Jam Anonymous Traffic Remapping Attacks in Ad Hoc WLANs, IEEE COMMUNICATIONS LETTERS, Vol. 21, Iss. 3 (2017), pp. 624-627, DOI: 10.1109/LCOMM.2016.2639483

Credibility of Threats to Jam Anonymous Traffic Remapping Attacks in Ad Hoc WLANs

Jerzy Konorski and Szymon Szott, *Senior Member, IEEE.*

***Abstract*—In ad hoc networks, selfish stations can pursue a better quality of service (QoS) by performing traffic remapping attacks (TRAs), i.e., by falsely assigning their traffic to a higher-priority class, which can hurt honest stations' QoS. To discourage the attackers, honest stations can announce their dissatisfaction with the perceived QoS. If such a threat fails, a costly data frame jamming defense can be launched. We analyze the arising noncooperative game in which the attackers decide whether to continue a TRA when threatened and honest stations decide whether to start jamming when the TRA is continued. Using a Maynard Smith setting we prove that the threats are credible to a rational attacker, who will then refrain from playing the game and remain honest.**

***Index Terms*—Ad hoc networks, IEEE 802.11, EDCA, QoS, game theory, selfish behavior, traffic remapping**

I. Introduction

QUALITY of service (QoS) provisioning in ad hoc networks often uses a class-based approach [1]: at each station, application-layer traffic is assigned to a traffic class with specific medium access rights. However, selfish stations can pursue a better QoS than they are entitled to by falsely assigning their traffic to a higher class. Such behavior, typically damaging to the other, honest stations, is termed *class hijacking* [2] or the *traffic remapping attack* (TRA) [3].

In [3], a distributed scheme was proposed to discourage TRAs in a single-hop wireless LAN (WLAN) with anonymous stations, where stations' identities cannot be inferred from MAC addresses written into transmitted frames. The scheme has honest stations, whenever dissatisfied with the currently perceived QoS, append DISSATISFACTION primitives to data packets. These signal readiness to detect selfish attackers, e.g., via traffic classification (TC) of sensed frames, and mete out a punishment, e.g., via selective jamming of frames. A detailed discussion of detection methods can be found in [3]. Assuming that the threat of imminent punishment subtracts from selfish stations' QoS satisfaction, a noncooperative game arises, leading to a Nash equilibrium where TRAs are either harmless or counterproductive. A prerequisite for that is the credibility of the DISSATISFACTION threat, which was left out from [3]. In this letter we prove it rigorously.

In our analysis, continuing a TRA when DISSATISFACTION primitives are broadcast instills a separate noncooperative game we refer to as the THREAT/JAM game, in which selfish stations can only suffer from degraded QoS, whereas honest stations cannot, even if they are to fulfill their threats.

S. Szott is with AGH University, Poland. His work is supported by the Polish National Science Centre (decision no. DEC-2011/01/D/ST7/05166).

J. Konorski is with the Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Poland.

Manuscript received October 24, 2016; revised December 12, 2016.

II. Threat/Jam Game

Consider an IEEE 802.11 ad hoc WLAN in which the enhanced distributed channel access (EDCA) function is employed. At least one station is honest and at least one is selfish. Honest stations adhere to standard CoS-to-AC mapping, where CoS refers to the ITU-T Y.1541-defined class of service of the application-layer traffic (e.g., written into IP packet headers according to RFC 4594), and AC refers to the EDCA-defined access category. For clarity, we restrict the used ACs to VO (voice, priority access) and BE (best-effort, non-priority access). Stations whose application-layer traffic should be mapped onto BE (e.g., a file transfer) and VO (e.g., a VoIP call) will be called *natively BE* and *natively VO*, respectively. An honest station can be natively either BE or VO, whereas a selfish one is always natively BE, but when launching a TRA, assigns its traffic to a CoS that maps onto VO, e.g., using packet mangling software.

A. Game Outline

Suppose one or more selfish stations launch a TRA and find it beneficial in terms of attained throughput (which we further assume indicative of QoS). If honest stations perceive it as damaging, a two-phase THREAT/JAM game arises. In the phase-one (THREAT) game, selfish stations continue the TRA, which they can withdraw from at any time (and so terminate the whole game in phase one), while honest stations broadcast a DISSATISFACTION threat at no cost. This threat they can either continue until no TRA is perceived, or fulfill at any time by initiating TC and selective jamming. In the phase-two (JAM) game ensuing in the latter case, honest stations can either surrender (quit TC and selective jamming) or continue until no TRA is perceived, while selfish stations can withdraw from the TRA at any time (in particular, never if honest stations have surrendered). This is a war of attrition [4]: selfish stations perceive TC and selective jamming as damaging (their packets cannot get through), while honest stations perceive it as costly (have to expend extra processing and transmission power). Note that depending on the outcome of the THREAT game, the JAM game may be played or not. Both are multistage games with infinite horizon, each stage played as a one-shot game long enough for stations to detect other stations' behavior and choose their own next-stage behavior.

Faced with continued selective jamming and no packets getting through, applications at selfish stations abandon current network activity (drop a user's session) after t stages of the JAM game with probability $\varphi(t)$, a nondecreasing function of $t = 1, 2, \ldots$ with $\varphi(1) > 0$. This is considered an externality and common knowledge of all stations that has to be accounted for when deciding further course of play.

B. Players, Stage Actions, and Payoffs

Though in reality a multi-player game, THREAT/JAM is modeled below assuming just two players:

- Attacker, denoted i, is a selfish station ready to launch a TRA,
- Defender, denoted j, is an honest station broadcasting DISSATISFACTION primitives.

Due to stations' anonymity, a selfish station launching (not launching) a TRA is indistinguishable from a natively VO (BE) honest station. Also, during the THREAT game it is hard for a dissatisfied honest station to learn the number of similar stations and their determination to engage in the JAM game. Therefore, the number of selfish stations conceptually embodied by Attacker, as well as of dissatisfied honest stations conceptually embodied by Defender, cannot be accurately observed and made part of either player's strategy. A two-player game model reflects this limited knowledge.

In each stage of the THREAT game, players choose between two actions: Attacker can *attack* (continue a TRA) or *withdraw* (quit the TRA and stay honest thereafter), whereas Defender can *threat* (continue to broadcast DISSATISFACTION primitives) or *fulfill* (quit threatening and initiate TC and selective jamming of Attacker's packets). In each stage of the JAM game, Attacker takes actions as above, and Defender chooses between *jam* (continue TC and selective jamming) or *surrender* (quit TC and selective jamming to accept damage caused by the continued TRA). Note that by collecting on-the-fly measurements of own throughput, Defender can easily distinguish *withdraw* from *attack*, whereas by sensing packets on the channel, Attacker can easily distinguish *threat* from *fulfill* and *jam* from *surrender*; hence THREAT/JAM is a perfect information game. Fig. 1 shows some of its possible scenarios.

Players' perceived benefits per stage are referred to as *payoffs*. They are defined in terms of observed station throughput under saturation load. As such, they depend on the number of honest stations that are natively VO and BE, which we assume fixed for the game duration. Relevant payoff levels are:

- $P_{i\mathrm{h}}$ and $P_{i\mathrm{a}}$ – Attacker's throughput while honest and while attacking without Defender's TC and selective jamming, respectively ($P_{i\mathrm{h}} < P_{i\mathrm{a}}$). Under TC and selective jamming, Attacker's throughput is taken to be 0.
- $P_{j|\mathrm{a}}$, $P_{j|\mathrm{h}}$, and $P_{j|-}$ – Defender's throughput while Attacker is attacking, honest, and absent, respectively ($P_{j|\mathrm{a}} < P_{j|\mathrm{h}} < P_{j|-}$).

C. Long-Term Utilities and Subgame Perfect Equilibrium

Perceived benefits from the (possibly indefinite) continuation of play are referred to as *utilities*; these drive the players' successive stage actions. Utilities are taken to be sums of discounted future payoffs, with players' discount factors δ_i and δ_j ($0 \le \delta_i, \delta_j < 1$), assumed to be common knowledge. This assumption is not unrealistic: δ_x can be regarded as the probability of player x staying in session until a next stage and derived from the statistics of application session durations.

It is assumed that the players are rational and their rationality is common knowledge as well. Therefore, each player pursues a *subgame perfect equilibrium* (SPE) and anticipates similar play of the other player [4]. Informally, at an SPE each player's *strategy* (the rule of choice of successive stage actions) maximizes her current utility vis á vis the other player's strategy. At a *mixed-strategy SPE* (MSPE), both players choose their actions at random in each stage.

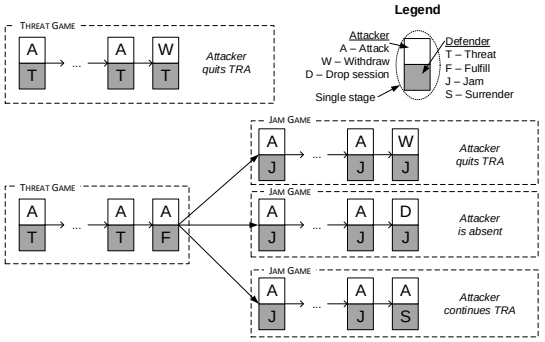

Fig. 1. Possible scenarios of the THREAT/JAM game.

III. PROBLEM STATEMENT AND ANALYSIS

Given that TC and selective jamming are feasible but costly, is the DISSATISFACTION threat credible? That is, are selfish stations convinced that the JAM game, if played, will indeed damage their throughput more than it will honest stations' (hence that the latter indeed will fulfill their threat should the ongoing TRA be continued)? We answer in the affirmative by analyzing the game arising between Defender and Attacker in a slightly adapted Maynard Smith setting [5]. Both players choose their actions at random with probabilities that maximize each player's utility, hence neither has an incentive to use different probabilities. Following [5], this equilibrium postulate is translated into a set of equations from which equilibrium utilities can be deduced. Specifically, we show that MSPE play of the THREAT/JAM game (*i*) terminates after finitely many stages with probability one, (*ii*) yields Attacker an expected utility not exceeding that yielded by honest behavior, and (*iii*) cannot worsen Defender's expected utility compared to the case when no threats are issued or fulfilled.

A. Maynard Smith Setting

Two players, i and j, fight for a reward in stages $t = 1, 2, \ldots$, feasible stage actions being *continue* and *quit*. Denote a player of interest by x ($x = i$ or j) and her opponent by $-x$. Choice of *continue* in stage t brings player x a reward $R_x(t)$ should player $-x$ quit in stage t, or entails a cost of fighting C_x otherwise; *quit* in stage t brings a fine $F_x(t)$[1]. Let

- $p_x(t)$ – probability that player x chooses *quit* in stage t (and *continue* with remaining probability),
- $U_x(t) = \sum_{\tau=0}^{\infty} \delta_x^\tau P_x(t+\tau)$ – player x's MSPE utility from stage t on, where $P_x(t)$ is her MSPE payoff in stage t.

Key to MSPE calculation is the backward induction recurrence

$$U_x(t) = \begin{cases} F_x(t), \text{ if } x \text{ chooses } \textit{quit} \text{ in stage } t, \\ (-C_x + \delta_x U_x(t+1))\,(1 - p_{-x}(t)) + \\ \qquad R_x(t) p_{-x}(t), \text{ otherwise.} \end{cases} \tag{1}$$

[1]The terms "reward" and "fine" are used just as a convention, for $F_x(t) \le R_x(t)$ need not hold; neither do we assume $F_x(t) = 0$ or $C_x \ge 0$.

MSPE stipulates that player $-x$ employs probabilities $p_{-x}(t)$ that in each stage make player x indifferent between *quit* and *continue*. Thus player $-x$'s MSPE probabilities solve

$$\begin{aligned}(-C_x + \delta_x U_x(t+1))\,(1-p_{-x}(t)) + R_x(t)p_{-x}(t) = \\ (-C_x + \delta_x F_x(t+1))\,(1-p_{-x}(t)) + R_x(t)p_{-x}(t) = F_x(t),\end{aligned} \quad (2)$$

where the first equality uses our stipulation recursively, i.e., player x remains indifferent in stage $t+1$. If one of the following two pairs of inequalities hold:

$$-C_x + \delta_x F_x(t+1) < F_x(t) < R_x(t) \quad (3)$$

$$-C_x + \delta_x F_x(t+1) > F_x(t) > R_x(t) \quad (4)$$

then the solution of (2) is nontrivial (i.e., $0 < p_{-x}(t) < 1$) and

$$p_{-x}(t) = \frac{1}{1+\xi_x(t)}, \quad (5)$$

$$\xi_x(t) = \frac{R_x(t) - F_x(t)}{F_x(t) + C_x - \delta_x F_x(t+1)}. \quad (6)$$

Player x's expected MSPE utility from the play is $F_x(1)$. Note that if for all $t = 1, 2, \ldots$, $\xi_x(t)$ is bounded from above (hence $p_{-x}(t) \geq \epsilon$ for some $\epsilon > 0$) then condition (*i*) is true.

B. JAM *Game*

We identify the relevant terms in (1): C_x^{JAM}, $F_x^{\text{JAM}}(t)$, and $R_x^{\text{JAM}}(t)$ in turn for Attacker, i (for whom *continue* corresponds to *attack* and *quit* to *withdraw*), and Defender, j (for whom *continue* corresponds to *jam* and *quit* to *surrender*).

1) Attacker: Choice of *withdraw* in stage t implies that Attacker stays honest from now on, which would bring her a payoff of $P_{i\text{h}}$ in each subsequent stage. We regard it as a reference level. However, the applications at Attacker may drop the current session in stage t with probability $\varphi(t)$ and her payoffs will be 0 henceforth. Hence, relative to the reference level, Attacker's penalty is the expected lost utility:

$$F_i^{\text{JAM}}(t) = -\varphi(t)\sum_{\tau=0}^{\infty} P_{i\text{h}}\delta_i^{\tau} = -\varphi(t)\frac{P_{i\text{h}}}{1-\delta_i}. \quad (7)$$

Choice of *attack* while Defender chooses *jam* causes in stage t loss of all transmitted data compared to potentially achieved throughput when staying honest, i.e., $C_i^{\text{JAM}} = P_{i\text{h}}$.

Choice of *attack* while Defender chooses *surrender* in stage t brings Attacker same penalty as above if her applications drop the current session, otherwise an excess $P_{i\text{a}} - P_{i\text{h}}$ over honest throughput in each subsequent stage:

$$R_i^{\text{JAM}}(t) = \frac{(1-\varphi(t))P_{i\text{a}} - P_{i\text{h}}}{1-\delta_i}. \quad (8)$$

To verify (3) observe that the second inequality holds since $P_{i\text{a}} > P_{i\text{h}}$; the first one, in view of $U_i(t+1) = F_i^{\text{JAM}}(t+1)$ as MSPE stipulates, can be written as

$$\delta_i \frac{1-\varphi(t+1)}{1-\varphi(t)} < 1, \quad (9)$$

which is obviously true. Thus, the MSPE probability of Defender choosing *surrender* in stage t is given by (5), where

$$\xi_x(t) = \xi_i^{\text{JAM}}(t) = \frac{\frac{P_{i\text{a}}}{P_{i\text{h}}} - 1}{1 - \delta_i \frac{1-\varphi(t+1)}{1-\varphi(t)}}. \quad (10)$$

Expected MSPE utility of Attacker equals $F_i^{\text{JAM}}(1)$.

2) Defender: Choice of *surrender* in stage t while Attacker still chooses *attack* (which from now on continues unpunished) brings Defender a payoff of $P_{j|\text{a}}$ in each subsequent stage, a reference level, if applications at Attacker do not drop the current session. Otherwise Attacker does not transmit anymore and, with respect to the reference level, Defender henceforth enjoys excess throughput of $P_{j|-} - P_{j|\text{a}}$. Thus

$$F_j^{\text{JAM}}(t) = \varphi(t)\frac{P_{j|-} - P_{j|\text{a}}}{1-\delta_j}. \quad (11)$$

Choice of *jam* requires extra processing and transmission power; this is a non-negligible throughput-related cost, since both TC and selective jamming must keep pace with Attacker's transmission rate, and the resulting depletion of Defender's battery resources may reflect upon its future throughput. We take $C_j^{\text{JAM}} = \kappa(P_{j|-} - P_{j|\text{a}})$, where $\kappa > 0$ is a constant.

Choice of *jam* while Attacker chooses *withdraw* in stage t brings Defender excess throughput of $P_{j|-} - P_{j|\text{a}}$ in each subsequent stage if applications at Attacker drop the current session, and of $P_{j|\text{h}} - P_{j|\text{a}}$ otherwise. Thus

$$R_j^{\text{JAM}}(t) = \frac{(1-\varphi(t))P_{j|\text{h}} + \varphi(t)P_{j|-} - P_{j|\text{a}}}{1-\delta_j}. \quad (12)$$

It is easy to verify the second inequality of (3), whereas for the first one to hold regardless of κ it suffices that for all t,

$$\delta_j < \frac{\varphi(t)}{\varphi(t+1)}. \quad (13)$$

(Note that the opposite of (13) would mean that *jam* is Defender's dominating action in some stages; this would also be true if $\varphi(1) = 0$, which we have assumed away. However, the assumed positive-valued $\varphi(\cdot)$ prevents indefinite jamming.)

Given (13), the MSPE probability of Attacker choosing *withdraw* in stage t is given by (5), where

$$\xi_x(t) = \xi_j^{\text{JAM}}(t) = \frac{\left(1-\varphi(t)\right)\frac{P_{j|\text{h}} - P_{j|\text{a}}}{P_{j|-} - P_{j|\text{a}}}}{(1-\delta_j)\kappa + \varphi(t) - \delta_j\varphi(t+1)}. \quad (14)$$

Expected MSPE utility of Defender equals $F_j^{\text{JAM}}(1)$.

C. THREAT *Game*

For Defender, *continue* now corresponds to *threat* and *quit* to *fulfill*; Attacker's actions are same as above.

1) Attacker: Choice of *withdraw* in stage t implies that Attacker is honest from now on, which brings her $P_{i\text{h}}$ in each subsequent stage. This is a reference level that Attacker can count on when staying honest all along. Hence, relative to the reference level, $F_i^{\text{THREAT}}(t) = 0$.

Choice of *attack* in stage t while Defender still chooses *threat* brings $P_{i\text{a}}$; compared with the reference level $P_{i\text{h}}$, this produces a negative cost of fighting: $C_i^{\text{THREAT}} = -(P_{i\text{a}} - P_{i\text{h}})$.

Choice of *attack* in stage t while Defender chooses *fulfill* initiates the JAM game, in which Attacker's expected MSPE utility is given by (7). Since both $R_i^{\text{THREAT}}(t) = F_i^{\text{JAM}}(1)$ and $C_i^{\text{THREAT}}(t)$ are negative, (4) holds and the MSPE probability of Defender choosing *fulfill* in stage t is given by (5), where

$$\xi_x(t) = \xi_i^{\text{THREAT}} = \frac{\varphi(1)}{(1-\delta_i)\left(\frac{P_{i\text{a}}}{P_{i\text{h}}} - 1\right)}. \quad (15)$$

Expected MPSE utility of Attacker is $F_i^{\text{THREAT}}(1) = 0$.

2) Defender: Choice of *fulfill* in stage t initiates the JAM game, bringing $R_j^{\text{THREAT}}(t) = F_j^{\text{JAM}}(1)$, cf. (11).

Choice of *threat* in stage t while Attacker chooses *attack* is costless (DISSATISFACTION primitives require little processing and no extra transmission power), hence $C_j^{\text{THREAT}} = 0$.

Choice of *threat* in stage t while Attacker chooses *withdraw* brings Defender $P_{j|\text{h}}$ consistently in subsequent stages; compared with the reference level $P_{j|\text{a}}$ that Defender could count on if Attacker continued to choose *attack*, this produces

$$R_j^{\text{THREAT}}(t) = \frac{P_{j|\text{h}} - P_{j|\text{a}}}{1 - \delta_j}. \tag{16}$$

Verifying (3) one immediately sees that the first inequality holds, whereas the second one amounts to

$$\varphi(1) < \frac{P_{j|\text{h}} - P_{j|\text{a}}}{P_{j|\text{-}} - P_{j|\text{a}}}. \tag{17}$$

If (17) is true, the MSPE probability of Attacker choosing *withdraw* in stage t is given by (5), where

$$\xi_x(t) = \xi_j^{\text{THREAT}} = \frac{\frac{P_{j|\text{h}} - P_{j|\text{a}}}{P_{j|\text{-}} - P_{j|\text{a}}} - \varphi(1)}{(1 - \delta_j)\varphi(1)}. \tag{18}$$

(If (17) is not true, Defender initiates the JAM game already in stage 1 and Attacker incurs a negative utility.) Expected MSPE utility of Defender is $R_j^{\text{THREAT}}(1) = F_j^{\text{JAM}}(1)$.

D. Inference of Payoffs

MPSE play of the THREAT/JAM game requires that the players' payoffs be common knowledge. This is possible even with anonymous stations. Firstly, let there be m stations transmitting VO traffic (including natively VO honest stations and Attacker when launching a TRA) and n stations transmitting BE traffic (including natively BE honest stations and Attacker when not launching a TRA). Given m and n, one can calculate the throughputs $S_{\text{VO}}(m, n)$ and $S_{\text{BE}}(m, n)$ of each of the m and n stations, respectively, from an EDCA performance model [6]. Furthermore, let $S^T_{\text{VO}}(m, n) = mS_{\text{VO}}(m, n)$ and $S^T_{\text{BE}}(m, n) = nS_{\text{BE}}(m, n)$ be the total VO and BE throughput; note that unlike S, S^T is observable to all stations in a single-hop WLAN. The Attacker toggles between BE and VO, so during the game will have observed both $S^T_{\text{VO}}(m + 1, n)$ and $S_{\text{VO}}(m + 1, n)$, whence calculates m, as well as both $S^T_{\text{BE}}(m, n + 1)$ and $S_{\text{BE}}(m, n + 1)$, whence calculates n. A natively VO Defender will have observed both $S^T_{\text{VO}}(m + 1, n)$ and $S_{\text{VO}}(m + 1, n)$, whence calculates m; moreover infers n from $S^T_{\text{VO}}(m, n+1)$ (cf. Fig. 2). Similarly, a natively BE Defender will have observed both $S^T_{\text{BE}}(m + 1, n)$ and $S_{\text{BE}}(m + 1, n)$, whence calculates n; moreover infers m from $S^T_{\text{BE}}(m, n + 1)$ (cf. Fig. 2). Finally, Attacker knows whether Defender is natively VO or BE from the AC field next to the DISSATISFACTION primitive (which only honest stations have incentives to append [3]); putting AC = VO or AC = BE accordingly, it infers $P_{j|\text{-}} = S_{\text{AC}}(m, n)$, $P_{j|\text{h}} = S_{\text{AC}}(m, n + 1)$, and $P_{j|\text{a}} = S_{\text{AC}}(m + 1, n)$. Meanwhile, Defender infers $P_{i\text{a}} = S_{\text{VO}}(m + 1, n)$ and $P_{i\text{h}} = S_{\text{BE}}(m, n + 1)$.

Based on [6], condition (17) is found not too restrictive; for $m \le 5$ and $n \le 10$ its right-hand side never falls below 0.6 and 0.75 for a natively BE and VO Defender, respectively.

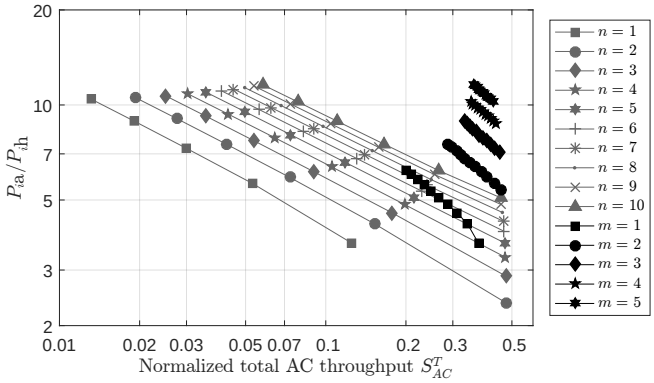

Fig. 2. Inference of m and n by Defender. Grey curves are for natively BE Defender: knowing $n = 0 \ldots 10$, locates points corresponding to $m = 0 \ldots 5$. Black curves are for natively VO Defender: knowing $m = 0 \ldots 5$, locates points corresponding to $n = 0 \ldots 10$. Each dot shows the value of $P_{i\text{a}}/P_{i\text{h}}$ (critical for MSPE probability), which appears fairly insensitive to small errors in throughput observation.

IV. CONCLUSION

Using a game-theoretic Maynard Smith setting we have demonstrated that threats of TC and jamming expressed by DISSATISFACTION primitives are credible and so can prevent TRAs in IEEE 802.11 ad hoc WLANs. Specifically, for condition (*i*), we have shown that all the ξ's are bounded from above (cf. the last sentence of Section III.A) which implies that the probabilities of terminating each phase of the game by each player remain bounded away from zero over time; as a consequence, the game duration will be finite with probability one. Conditions (*ii*) and (*iii*) follow from Attacker's and Defender's equilibrium utilities, as derived in Sections III.B and III.C (cf. (7) and (11) at $t = 1$, and the last sentences of parts 1) and 2) of Section III.C). Since Attacker never has a positive utility, it cannot be better off by attacking when threatened, or by continuing to attack when jammed; similarly, since Defender never has a negative utility, it cannot be worse off by jamming when Attacker continues the attack despite the threat. This implies that a rational Defender will never refrain from playing the THREAT/JAM game, whereas a rational Attacker will serve herself best by not playing, i.e., will stick to honest behavior.

REFERENCES

[1] S. Mangold, S. Choi, G. R. Hiertz, O. Klein, and B. Walke, "Analysis of IEEE 802.11e for QoS support in Wireless LANs," *IEEE Wireless Communications*, vol. 10, no. 6, pp. 40–50, 2003.

[2] R. Haywood, S. Mukherjee, and X.-H. Peng, "Investigation of H.264 Video Streaming over an IEEE 802.11e EDCA Wireless Testbed," in *Proc. of ICC*, 2009.

[3] J. Konorski and S. Szott, "Discouraging traffic remapping attacks in local ad hoc networks," *IEEE Transactions on Wireless Communications*, vol. 13, pp. 3752–3767, 2014.

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

[5] J. Maynard Smith, "The theory of games and the evolution of animal conflicts," *Journal of Theoretical Biology*, vol. 47, no. 1, pp. 209–221, 1974.

[6] S. Szott, M. Natkaniec, and A. R. Pach, "An IEEE 802.11 EDCA model with support for analysing networks with misbehaving nodes," *EURASIP Journal on Wireless Communications and Networking*, 2010.