MAC Games for Distributed Wireless Network Security with Incomplete Information of Selfish and Malicious User Types

Yalin Evren Sagduyu, Randall Berry and Anthony Ephremides

***Abstract*— We consider game theoretic models of wireless medium access control (MAC) in which each transmitter makes individual decisions regarding their power level or transmission probability. This allows for scalable distributed operation; however, it can also enable users to pursue malicious objectives such as jamming other nodes to deny them service. We study games with two types of players: selfish and malicious transmitters. Each type is characterized by a utility function depending on throughput reward and energy cost. Furthermore, we focus on the setting where the transmitters have incomplete information regarding other transmitters' types, modeled as probabilistic beliefs. We first analyze a power-controlled MAC game in which the nodes select powers for continuous transmissions and then extend this to a random access MAC in which nodes choose transmission probabilities. For each case, the Bayesian Nash equilibrium strategies are derived for different degrees of uncertainty, and the resulting equilibrium throughput of selfish nodes is characterized. We identify conditions in which the throughput improves with increasing type uncertainty and introduce Bayesian learning mechanisms to update the type beliefs in repeated games. For unknown types and costs, we also specify the equilibrium cut-off thresholds for monotonic transmission decisions. The analysis provides insights into the optimal defense mechanisms against denial of service attacks at the MAC layer in wireless networks.**

***Index Terms*— Bayesian games; distributed operation; incomplete information; malicious users; MAC; power control; random access; security; selfish users.**

I. Introduction

In wireless networks, centralized access control does not scale with the number of nodes. A promising alternative is *distributed* control in which nodes independently select their transmission strategies to optimize individual performance objectives. Such systems are naturally modeled as non-cooperative games, e.g., [1]-[3] consider *power control* games and [4]-[6] consider *random access* games for single-receiver access control. We consider models for both of these situations as well.

Non-cooperative nodes may pursue not only *selfish* but also *malicious* objectives such as interfering with the packet transmissions of other nodes. In this context, the channel jamming effects of malicious transmitters have been evaluated in terms of the worst-case throughput performance for ALOHA systems in [7] and have been incorporated into a zero-sum game of balancing the mutual information over Gaussian channels in [8]. For both models of power control and random access, jamming games have been formulated for users with *known* selfish or malicious types reflected in their utilities [9]-[11]. The possible misbehavior of transmitters has been studied in [12]-[13] for intrusion detection and in [14] for packet forwarding without MAC interactions.

In this paper, we strip off all the complexities introduced by multihop operation and analyze the fundamental interactions of selfish and malicious nodes at the MAC layer. This problem has been studied in [9]-[10] under power control and random access for the case of *known* types of selfish and malicious nodes (with known utility functions). However, the *Nash equilibrium* strategies strongly depend on the (selfish or malicious) user types. In practice, malicious nodes would likely conceal their intent, i.e., nodes would have *incomplete information* regarding the types of other nodes. Here, we study the effects of such incomplete information.

Our goal is to develop a framework for *denial of service attacks* as *dynamic non-cooperative games* among selfish nodes transmitting to a common receiver and malicious nodes jamming their transmissions. Although our primary focus is on the case of *two* transmitters, we also extend the analysis to an *arbitrary* number of selfish and malicious transmitters. The node types are possibly hidden and represented by *probabilistic beliefs* at individual nodes. The performance objectives incorporate (*i*) *throughput* rewards (based on Signal-to-Interference-plus-Noise-Ratio (SINR) for power control or success probability for random access), (*ii*) transmission *energy* costs, and (*iii*) malicious *jamming* interests.

Malicious nodes do not have any incentive of jamming each other's transmissions and they become less aggressive in their attack decisions, if they are uncertain about whether the opponent nodes are selfish. This suggests a *distributed security* paradigm that allows random malicious node behavior (without external detection) and relies on individual nodes to hide their types as an inherent *defense* mechanism to mitigate the malicious operation. We evaluate the *Bayesian Nash equilibrium* strategies and present the conditions in which the *type uncertainty* may be beneficial for selfish nodes to improve their throughput properties.

For random access, we also derive the equilibrium set of thresholds for the *monotonic* transmission decisions under the incomplete information on types and cost parameters. A similar problem has been considered in [15] for selfish nodes with known types only. Instead, we formulate the uncertainty of node types and (energy) costs *jointly*.

In addition to *one-stage Bayesian games*, we extended the results to consider *dynamic repeated games*. The usual

Y. E. Sagduyu and R. Berry are with the Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208, USA. y-sagduyu@northwestern.edu, rberry@ece.northwestern.edu

A. Ephremides is with the Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA. etony@umd.edu

approach to intrusion detection is based on externally detecting malicious behavior, e.g., by hypothesis testing, if the transmission strategies of selfish and malicious nodes are fixed and known [16]. Instead, we introduce a distributed solution to the *network security* problem at the MAC layer in which nodes learn each other's types according to a *Bayesian learning* mechanism and play the *best-response* strategies against their type beliefs that evolve dynamically over time.

The paper is organized as follows. Section II introduces the game model for power-controlled MAC with two users. The interactions of possibly selfish or malicious users are presented in Sections III and IV for two different SINR-based throughput reward functions. This is followed in Section V by the analysis of Bayesian learning mechanisms for selfish and malicious user types with unknown belief distributions. We outline the generalization to an arbitrary number of users in Section VI. The game model is extended in Section VII to consider probabilistic transmission decisions for random access. Finally, we draw conclusions and present thoughts for future work in Section VIII.

II. Two-user Power-Controlled MAC Game

Consider a *one-stage game* between *two* transmitters of *two* possible (*selfish* or *malicious*) types. Define $P_i \geq 0$ and $E_i \geq 0$ as the transmission power and the corresponding energy cost (per unit power) of node $i = 1, 2$, respectively. Assume a synchronous slotted system, in which each packet transmission takes one time slot. Each node $i = 1, 2$ independently chooses the power P_i for transmitting to a common receiver in order to maximize the individual expected utility $u_i(P_1, P_2)$. The SINR value achievable by selfish node i is

$$\gamma_i = \frac{h_i P_i}{\frac{1}{L}\sum_{j \neq i} h_j P_j + \sigma^2}, \tag{1}$$

where h_i is the channel gain for node i, L is the processing gain and σ^2 is the channel noise. The (throughput) reward for a selfish node i is $f_i(\gamma_i)$, which is an increasing function of the SINR value γ_i. We consider *two* different *reward functions* for selfish nodes:

$$f_i(\gamma_i) = \gamma_i, \;\; f_i(\gamma_i) = \log(1 + \gamma_i), \tag{2}$$

namely, the SINR value γ_i and the Shannon rate from transmitter i to the receiver for the SINR value γ_i.

Any *selfish* node i also incurs the energy cost $E_i P_i$ proportional to power P_i and maximizes the expected utility

$$u_i(P_1, P_2) = f_i(\gamma_i) - E_i P_i. \tag{3}$$

Any *malicious* node $i = 1, 2$ incurs as cost the throughput reward $f_j(\gamma_j)$ of selfish opponent $j \neq i$ as well as the energy cost $E_i P_i$ and so maximizes the expected utility

$$u_i(P_1, P_2) = \begin{cases} -f_j(\gamma_j) - E_i P_i, \\ \text{if the opponent node } j \text{ is selfish}, \\ -E_i P_i, \\ \text{if the opponent node } j \text{ is malicious}, \end{cases} \tag{4}$$

for $j = 1, 2$, $j \neq i$, i.e., malicious nodes do not have any incentive of interfering with each other's transmissions. Note that without energy costs, a game between one malicious node and one selfish node will be a zero-sum game of throughput balancing.[1] However, we end up with a non-zero-sum game for the case of non-zero energy costs.

Let ϕ_i denote the probabilistic belief of node i that the other node $j \neq i$ is selfish. The parameters L, σ^2, h_i, E_i and ϕ_i, $i = 1, 2$, are known to all nodes. This models the case when the system is monitored and nodes are notified with the long-term statistics of attack possibilities. We will consider the effects of uncertainty on type belief distributions and energy costs in Sections V and VII.

III. Interactions of Selfish and Malicious Transmitters for Reward Function $f_i(\gamma_i) = \gamma_i$

We next present results for two transmitters with reward function $f_i(\gamma_i) = \gamma_i$, under different assumptions on the type uncertainty. In general, the Nash equilibrium strategies P_i^* for any node i satisfy

$$u_i(P_i^*, P_{-i}^*) \geq u_i(P_i, P_{-i}^*), \quad i = 1, 2, \tag{5}$$

for any strategy P_i, $i = 1, 2$, where P_{-i} is the strategy of the node(s) other than node i, such that no node can unilaterally improve its individual performance beyond the Nash equilibrium.

A. Known Types of Two Transmitters

Theorem 1: For *two selfish transmitters*, the *unique Nash equilibrium* strategies are[2]:

$$P_i = \frac{L}{h_i}\Big(\frac{h_j}{E_j} - \sigma^2\Big), \; j \neq i, \;\; \text{if } h_i \geq \sigma^2 E_i, \; i = 1, 2, \tag{6}$$

$$P_i = 0, \;\; \text{if } h_i < \sigma^2 E_i, \; i = 1, 2, \tag{7}$$

$$P_i = 0, \; P_j \to \infty, \;\; \text{if } h_i < \sigma^2 E_i, \; h_j > \sigma^2 E_j, \; j \neq i. \tag{8}$$

Proof: The individual optimization problem for any transmitter $i = 1, 2$ is given by

$$\max_{P_i \geq 0} \; u_i(P_i, P_{-i}), \quad \text{for } P_{-i} \geq 0. \tag{9}$$

For each user, define the Lagrangian

$$L_i(P_1, P_2) = u_i(P_1, P_2) + \lambda_i P_i, \quad i = 1, 2, \tag{10}$$

where $\lambda_i \geq 0$ is a Lagrange multiplier corresponding to the inequality constraint in (9). The Karush-Kuhn-Tucker (KKT) conditions for the optimal solutions of (9) are given by

$$\frac{\partial L_i(P_1, P_2)}{\partial P_i} = 0, \; P_i \geq 0, \; \lambda_i \geq 0, \; \lambda_i P_i = 0, \; i = 1, 2. \tag{11}$$

These necessary conditions are also sufficient for optimality, since the utility $u_i(P_1, P_2)$ and inequality constraint $P_i \geq 0$ are continuously differentiable and concave functions of P_i. The equilibrium strategies (6)-(8) follow from applying the KKT conditions (11) separately to each objective function

[1] We could also define the malicious utility by using a reward function $\mathcal{K} - f_j(\gamma_j)$ to be maximized (for a constant $\mathcal{K}$). However, this would not change the equilibrium strategies of selfish or malicious nodes.

[2] Similar utility functions have been considered in [1]-[3] for selfish nodes with throughput and energy efficiency objectives.

$u_i(P_1, P_2)$, $i = 1, 2$, with constraint $P_i \geq 0$, where the utilities $u_i(P_1, P_2)$, $i = 1, 2$, are given by (3). ■

For a power-controlled MAC, the performance measure of interest is the SINR value achievable by selfish nodes. The SINR value achievable by selfish node $i = 1, 2$ in Nash equilibrium is given by

$$\gamma_i = \begin{cases} \frac{E_i P_i}{}, & \text{if } h_j > \sigma^2 E_j, \\ \frac{h_i P_i}{\sigma^2}, & \text{otherwise}, \end{cases} \quad j = 1, 2, \; j \neq i. \qquad (12)$$

Theorem 2: For *selfish* transmitter 1 and *malicious* transmitter 2, the *unique Nash equilibrium* strategies are

$$P_1 = \frac{L}{h_2} \frac{E_2 h_1}{(E_1)^2}, \; P_2 = \frac{L}{h_2}\Big(\frac{h_1}{E_1} - \sigma^2\Big), \text{ if } h_1 \geq \sigma^2 E_1, \quad (13)$$

$$P_1 = 0, \; P_2 = 0, \text{ if } h_1 < \sigma^2 E_1. \quad (14)$$

Proof: The equilibrium strategies (13)-(14) follow from applying the KKT conditions (11) separately to each objective function $u_i(P_1, P_2)$, $i = 1, 2$, with constraint $P_i \geq 0$, where the utilities $u_1(P_1, P_2)$ and $u_2(P_1, P_2)$ are given by (3) and (4), respectively. ■

The equilibrium SINR of selfish node 1 is given by (12) with P_1 from (13)-(14). The malicious attack of node 2 is more successful in reducing the SINR of selfish node 1 compared to the alternative selfish behavior of node 2 (under the assumption of $h_i \geq \sigma^2 E_i$, $i = 1, 2$, for the non-zero transmission powers), if and only if $\frac{h_2}{E_2} > \sigma^2 + \frac{E_2}{h_2}\big(\frac{h_1}{E_1}\big)^2$, i.e., if h_1 is small and E_1 is large. Otherwise, we observe the *windfall of malice*, i.e., the malicious attack fails compared to the selfish operation (as noted before for the separate problem of routing [17]). If both transmitters are malicious, they do not receive any reward from interfering with each other and the Nash equilibrium strategies are $P_1 = 0$ and $P_2 = 0$.

The system parameters may not be perfectly known or may be random. Then, any jamming node randomly chooses to pursue either selfish or malicious objective functions. Therefore, each node would face an opponent of random identity with the degree of uncertainty depending on the distributions of system parameters.

B. Selfish Transmitter 1 (Known Type) and Transmitter 2 of Unknown Type

Assume now that selfish node 1 believes that node 2 is selfish with probability ϕ_1 (known to node 2). Define $P_{2,S}$ and $P_{2,M}$ as the power, $E_{2,S}$ and $E_{2,M}$ as the energy cost, and $h_{2,S}$ and $h_{2,M}$ as the channel gain for selfish and malicious node 2, respectively.

Theorem 3: For selfish transmitter 1 and transmitter 2 of unknown type, the *Bayesian Nash equilibrium* strategies for $\phi_1 \in (0, 1)$ are

$$P_1 = \frac{L}{h_1}\Big(\frac{h_{2,S}}{E_{2,S}} - \sigma^2\Big), \qquad (15)$$

$$P_{2,S} = \frac{L}{h_{2,S}}\left[\frac{h_1\phi_1}{\Big(E_1 - \frac{(1-\phi_1)h_1}{\frac{h_{2,M}}{L}P_{2,M} + \sigma^2}\Big)} - \sigma^2\right]^+, \qquad (16)$$

$$P_{2,M} = \left[\sqrt{\frac{Lh_1P_1}{h_{2,M}E_{2,M}}} - \frac{L\sigma^2}{h_{2,M}}\right]^+, \qquad (17)$$

if $h_{2,S} \geq \sigma^2 E_{2,S}$, where $[x]^+ = \max(x, 0)$. Otherwise,

$$P_1 = \Big(\Big[E_1 - \frac{\phi_1 h_1}{\sigma^2}\Big]^+\Big)^{-2} \; \frac{E_{2,M} L h_1}{h_{2,M}} \; (1 - \phi_1)^2, \qquad (18)$$

$P_{2,S} = 0$ and $P_{2,M}$ is given by (17) with P_1 from (18).

Proof: The equilibrium strategies (16)-(18) follow from applying the KKT conditions separately to the objective functions $u_{2,S}(P_1, P_{2,S})$ of selfish node 2 and $u_{2,M}(P_1, P_{2,M})$ of malicious node 2 with constraints $P_1 \geq 0$, $P_{2,S} \geq 0$ and $P_{2,M} \geq 0$, where the utilities $u_{2,S}$ and $u_{2,M}$ are given by (3) and (4), respectively. Then, the equilibrium strategy (15) follows from applying the KKT conditions (11) to the expected objective function $\bar{u}_1(P_1, P_{2,S}, P_{2,M}) = \phi_1 u_1(P_1, P_{2,S}) + (1 - \phi_1) u_1(P_1, P_{2,M})$ of selfish node 1, where the utility u_1 is given by (3). ■

Assume $h_{2,S} \geq \sigma^2 E_{2,S}$ for the case of non-zero transmission power of selfish node 2. Selfish node 1 can individually detect the type of node 2, unless $P_{2,S} = P_{2,M}$ in (16)-(17). If node 1 detects the other node as malicious such that $\phi_1 = 0$, the power P_1 is changed to (13), whereas the power of node 2 is still given by (17).

Consider the case when node 2 is *selfish*. In Nash equilibrium, P_1 is the same as in the case of two selfish nodes with known types (independent of ϕ_1). So, selfish node 2 cannot learn, whether node 1 detects the type of node 2, or not, and continues to operate with the same value of ϕ_1 as before. The uncertainty of the opponent's type is beneficial for selfish node 2 (i.e., selfish node 2 can increase $\gamma_{2,S}$ by hiding its type compared to the case with the known types), if $\frac{h_1}{E_1} > \Big(\frac{h_{2,M}}{L}P_{2,M} + \sigma^2\Big)$, where $P_{2,M}$ follows from (17), i.e., if h_1 is large and E_1 is small. Otherwise, selfish node 2 should reveal its type.

On the other hand, the uncertainty on the opponent's type is beneficial for selfish node 1, if $\frac{h_1}{E_1} < \Big(\frac{h_{2,M}}{L}P_{2,M} + \sigma^2\Big)$, i.e., if h_1 is small and E_1 is large.

Next, consider the case when node 2 is *malicious*. Then, the power $P_{2,M}$ does not depend on ϕ_1. The attack of node 2 is more successful (in reducing the SINR value γ_1) by hiding its type (compared to the case of known types of selfish node 1 and malicious node 2), if and only if $\frac{E_{2,M}}{h_{2,M}}\big(\frac{h_1}{E_1}\big)^2 > \frac{h_{2,S}}{E_{2,S}} - \sigma^2$ (i.e., if h_1 is large and E_1 is small). As a result, selfish and malicious nodes choose between revealing and concealing their identities depending on the system parameters.

The equilibrium SINR value achievable by selfish nodes is depicted in Figure 1 as function of the type belief probability ϕ_1, where the expected SINR γ_1 of selfish node 1 is averaged over the type of node 2 under the assumption that the type belief distribution ϕ_1 is equal to the true distribution $\tilde{\phi}$ that node 2 is selfish. In Figure 2, we illustrate the case when the type belief distribution ϕ_1 deviates from the true distribution $\tilde{\phi}$. Note that assuming the true distribution $\tilde{\phi}$ for the type belief ϕ_1 does not necessarily optimize the equilibrium SINR value γ_1 of selfish node 1, i.e., the uncertainty on type belief distributions may possibly improve the equilibrium SINR γ_1.

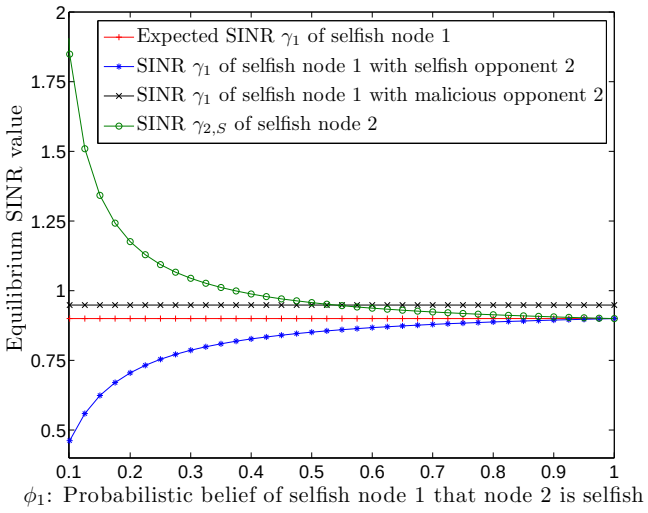

Fig. 1. The equilibrium SINR values of selfish nodes as function of type belief probability ϕ_1 for $h_i = 1$, $E_i = 1$, $i = 1, 2$, $L = 1$ and $\sigma^2 = 0.1$.

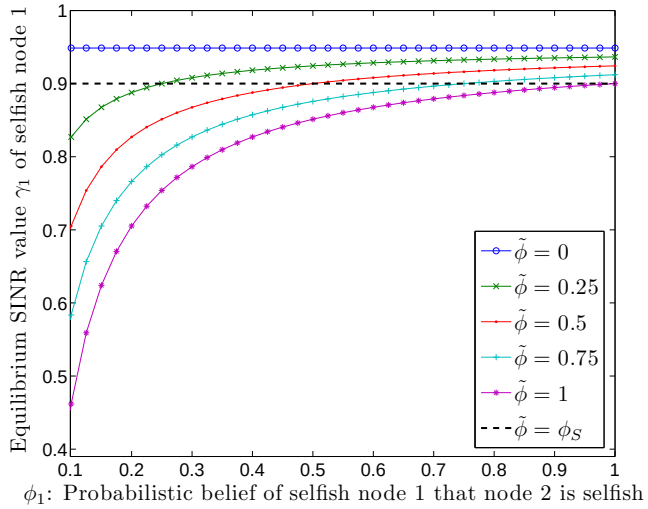

Fig. 2. The equilibrium SINR value of selfish node 1 as function of type belief probability ϕ_1 for different values of true distribution $\tilde{\phi}$ that node 2 is selfish and for $h_i = 1$, $E_i = 1$, $i = 1, 2$, $L = 1$ and $\sigma^2 = 0.1$.

C. Malicious Transmitter 1 (Known Type) and Transmitter 2 of Unknown Type

Now assume that malicious node 1 believes that node 2 is selfish with probability ϕ_1 (known to node 2).

Theorem 4: For $\phi_1 \in (0, 1)$, the *Bayesian Nash equilibrium* strategies are

$$P_1 = \frac{L}{h_1}\Big(\frac{h_{2,S}}{E_{2,S}} - \sigma^2\Big), \tag{19}$$

$$P_{2,S} = \frac{L}{h_1}\frac{E_1 h_{2,S}}{(E_{2,S})^2}\frac{1}{\phi_1}, \tag{20}$$

$$P_{2,M} = 0, \tag{21}$$

if $h_{2,S} \geq \sigma^2 E_{2,S}$. Otherwise, $P_1 = 0$, $P_{2,S} = 0$, $P_{2,M} = 0$.

Proof: The equilibrium strategies (20)-(21) follow from applying the KKT conditions (11) separately to the objective functions $u_{2,S}(P_1, P_{2,S})$ of selfish node 2 and $u_{2,M}(P_1, P_{2,M})$ of malicious node 2, with constraints $P_1 \geq 0$, $P_{2,S} \geq 0$ and $P_{2,M} \geq 0$, where $u_{2,S}$ and $u_{2,M}$ are given by (3) and (4), respectively. The equilibrium strategy (19) follows from applying the KKT conditions (11) to the expected objective function $\bar{u}_1(P_1, P_{2,S}, P_{2,M}) = \phi_1 u_1(P_1, P_{2,S}) + (1-\phi_1)u_1(P_1, P_{2,M})$ of malicious node 1 with $u_1(P_1, P_{2,M}) = 0$ and $u_1(P_1, P_{2,S})$ from (4). ■

After playing one stage of the game, malicious node 1 would immediately learn the opponent's type by observing the interference power (through the SINR feedback), since $P_{2,S} \neq P_{2,M}$. For $h_{2,S} > \sigma^2 E_{2,S}$, the equilibrium SINR of selfish node 2 is given by

$$\gamma_{2,S} = \frac{E_1 h_{2,S} L}{E_{2,S} h_1}\frac{1}{\phi_1}, \tag{22}$$

which increases, as ϕ_1 decreases, i.e., a malicious attack becomes less successful (in reducing the equilibrium SINR $\gamma_{2,S}$ of the possibly selfish node 2), as the uncertainty on the opponent's type increases. Therefore, node 2 should hide its type to increase $\gamma_{2,S}$, if it is selfish.

D. Transmitters 1 and 2 of Unknown Types

Nodes 1 and 2 have *unknown* selfish or malicious types. For each selfish and malicious node, define E_S and E_M as the energy cost, h_S and h_M as the channel gain, ϕ_S and ϕ_M as the probabilistic belief that the opponent is selfish. These parameters are known to both nodes. In this paper, symmetric strategies are considered for identical nodes with common type belief distributions, costs and system parameters. Then, each node assumes that all nodes of the same type choose the same transmission strategy. Define P_S and P_M as the transmission power of selfish and malicious node, respectively.

Theorem 5: For $\phi_S \in (0, 1)$ and $\phi_M \in (0, 1)$, the symmetric *Bayesian Nash equilibrium* strategies P_S and P_M of selfish and malicious transmitters are

$$P_S = [P_S^*]^+, \tag{23}$$

$$P_M = \frac{L}{h_M}\Big[\sqrt{P_S}\sqrt{\frac{\phi_M h_S h_M}{L E_M}} - \sigma^2\Big]^+, \tag{24}$$

respectively, where P_S^* is the solution to

$$\frac{\phi_S h_S \sigma^2}{\big(\frac{h_S}{L}P_S^* + \sigma^2\big)^2} + \frac{(1-\phi_S)\sqrt{h_S L E_M}}{\sqrt{P_S^*}\sqrt{\phi_M h_M}} = E_S. \tag{25}$$

Proof: Define $u_{i,j}$ as the utility of selfish node $i = S$ or malicious node $i = M$ with a selfish opponent $j = S$ or malicious opponent $j = M$. The equilibrium strategies (23)-(25) follow from applying the KKT conditions (11) separately to the objective functions $\bar{u}_S = \phi_S u_{S,S}(P_S, P_S) + (1-\phi_S)\, u_{S,M}(P_S, P_M)$ of each selfish node and $\bar{u}_M = \phi_M\, u_{M,S}(P_S, P_M) + (1-\phi_M)\, u_{M,M}(P_M, P_M)$ of each malicious node, with constraint $P_S \geq 0$ and $P_M \geq 0$, where the utilities $u_{S,S}$ and $u_{S,M}$ are given by (3), and the utilities $u_{M,S}$ and $u_{M,M}$ are given by (4). ■

Consider a selfish node with a malicious opponent. The equilibrium SINR of the selfish node is given by

$$\gamma_S = \begin{cases} \frac{\sqrt{P_S}\sqrt{h_S L E_M}}{\sqrt{\phi_M h_M}}, & \text{if } P_S > \frac{L E_M \sigma^4}{\phi_M h_S h_M}, \\ \frac{h_S P_S}{\sigma^2}, & \text{otherwise}, \end{cases} \tag{26}$$

which decreases with ϕ_S for fixed ϕ_M, with ϕ_M for fixed ϕ_S and with $\phi_S = \phi_M$. The expected SINR value γ_S (averaged over the distribution of the opponent's type) decreases with $\phi_S = \phi_M$, as shown in Figure 3, under the assumption that the type belief distributions are both equal to the true distribution $\tilde{\phi}$ that any given node is selfish. In Figure 4, we evaluate the effect of the mismatch between the type belief distribution $\phi_S = \phi_M$ and true distribution $\tilde{\phi}$ on the equilibrium SINR γ_S of any selfish node. The results show that assuming type beliefs other than the true distribution may possibly improve the equilibrium SINR value γ_S.

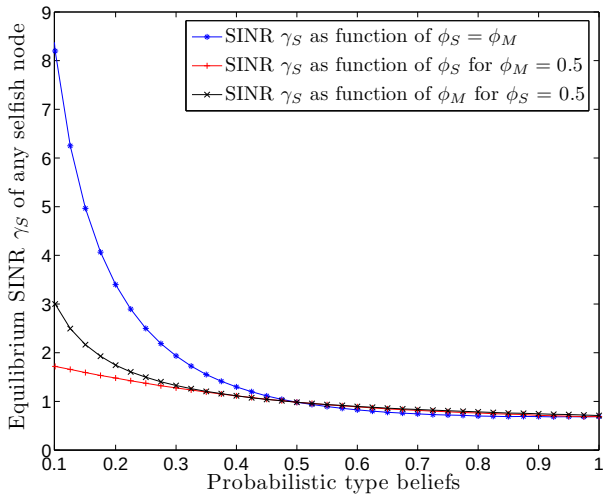

Fig. 3. The equilibrium SINR γ_S of any selfish node as function of type belief probabilities for $h_i = 1$, $E_i = 1$, $i = 1, 2$, $L = 1$ and $\sigma^2 = 0.1$.

Hence, the type uncertainty is beneficial for the selfish node and it should hide its type to increase γ_S, whereas the success of any malicious attack increases with ϕ_S and ϕ_M.

IV. Interactions of Selfish and Malicious Transmitters for Reward Function $f_i(\gamma_i) = \log(1 + \gamma_i)$

The analysis for reward function $f_i(\gamma_i) = \log(1 + \gamma_i)$ is similar to the previous analysis for reward function $f_i(\gamma_i) = \gamma_i$. Here, we outline the equilibrium strategies in Theorems 6-10. The proofs of Theorems 6-10 follow from the same arguments as in Theorems 1-5, where the reward function $f_i(\gamma_i) = \gamma_i$ is replaced by $f_i(\gamma_i) = \log(1 + \gamma_i)$.

A. Known Types of Two Transmitters

Theorem 6: For *two selfish transmitters*, the *unique* Nash equilibrium strategies are

$$P_i = \frac{\frac{h_i L}{E_i} - \frac{h_j}{E_j} - \sigma^2(L-1)}{h_i\Big(L - \frac{1}{L}\Big)}, \quad j \neq i, \ i = 1, 2, \tag{27}$$

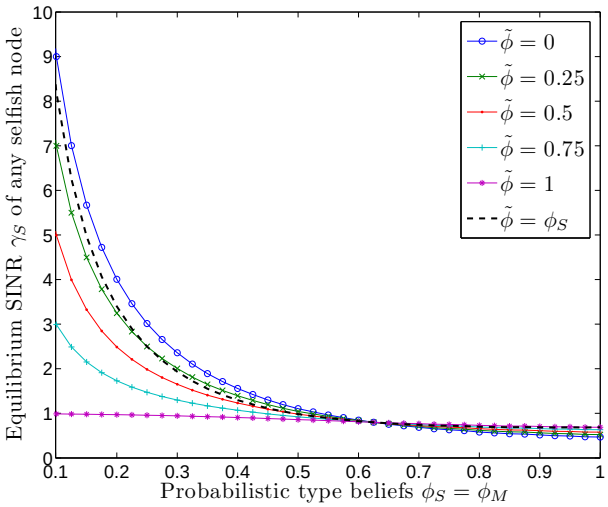

Fig. 4. The equilibrium SINR γ_S of any selfish node as function of type belief probabilities for different values of true distribution $\tilde{\phi}$ that a node is selfish and for $h_i = 1$, $E_i = 1$, $i = 1, 2$, $L = 1$ and $\sigma^2 = 0.1$.

if $\frac{h_i L}{E_i} - \frac{h_j}{E_j} \geq \sigma^2(L-1)$, $i = 1, 2$,

$$P_i = 0, \quad P_j = \Big[\frac{1}{E_j} - \frac{\sigma^2}{h_j}\Big]^+, \quad j \neq i, \tag{28}$$

if $\frac{h_i L}{E_i} - \frac{h_j}{E_j} < \sigma^2(L-1)$ and $\frac{h_j L}{E_j} - \frac{h_i}{E_i} > \sigma^2(L-1)$, $j \neq i$.

The same utility function has been considered in [3] for selfish nodes. The equilibrium SINR of a selfish node i is

$$\gamma_i = \begin{cases} \frac{(L^2-1)h_i P_i}{\frac{h_j L}{E_j} - \frac{h_i}{E_i} + \sigma^2 L(L-1)}, & \text{if } \frac{h_i L}{E_i} - \frac{h_j}{E_j} \geq \sigma^2(L-1), \\ \frac{h_i P_i}{\sigma^2}, & \text{otherwise.} \end{cases} \tag{29}$$

Theorem 7: For *selfish* transmitter 1 and *malicious* transmitter 2, the *unique* Nash equilibrium strategies are

$$P_1 = \frac{L E_2 h_1}{E_1(E_1 h_2 + L E_2 h_1)}, \tag{30}$$

$$P_2 = \frac{L}{h_2}\Big(h_1\Big(\frac{1}{E_1} - P_1\Big) - \sigma^2\Big), \tag{31}$$

if $\frac{\sigma^2 E_1}{h_1} + \frac{L E_2 h_1}{E_1 h_2 + L E_2 h_1} \leq 1$. Otherwise,

$$P_1 = \Big[\frac{1}{E_1} - \frac{\sigma^2}{h_1}\Big]^+, \quad P_2 = 0. \tag{32}$$

The equilibrium SINR of selfish node 1 is

$$\gamma_1 = \begin{cases} \frac{L E_2 h_1}{E_1 h_2}, & \text{if } \frac{\sigma^2 E_1}{h_1} + \frac{L E_2 h_1}{E_1 h_2 + L E_2 h_1} \leq 1, \\ \big[\frac{h_1}{\sigma^2 E_1} - 1\big]^+, & \text{otherwise.} \end{cases} \tag{33}$$

The malicious attack of node 2 is more successful in reducing γ_1 compared to the alternative selfish behavior, if the SINR value γ_1 given in (33) is smaller than the SINR value γ_i given in (29) for $i = 1$. This condition strongly depends on the underlying system parameters.

For two malicious nodes, the Nash equilibrium strategies are given by $P_1 = 0$ and $P_2 = 0$.

B. Selfish Transmitter 1 (Known Type) and Transmitter 2 of Unknown Type

Theorem 8: For $\phi_1 \in (0,1)$, the *Bayesian Nash equilibrium* strategies are

$$P_1 = [P_1^*]^+, \quad P_{2,S} = [P_{2,S}^*]^+, \quad P_{2,M} = [P_{2,M}^*]^+, \quad (34)$$

where P_1^*, $P_{2,S}^*$ and $P_{2,M}^*$ are solutions to

$$\frac{h_1 P_1^*}{L} + h_{2,S} P_{2,S}^* + \sigma^2 = \frac{h_{2,S}}{E_{2,S}}, \quad (35)$$

$$\frac{h_{2,M} h_1 P_1^*}{L} = E_{2,M}\Big(\frac{h_{2,M} P_{2,M}^*}{L} + \sigma^2\Big) \times \Big(\frac{h_{2,M} P_{2,M}^*}{L} + h_1 P_1^* + \sigma^2\Big), \quad (36)$$

$$\frac{\phi_1 h_1 \Big(\frac{h_{2,S} P_{2,S}^*}{L} + \sigma^2\Big)}{\frac{h_{2,S} P_{2,S}^*}{L} + h_1 P_1^* \sigma^2} + \frac{(1-\phi_1) h_1 \Big(\frac{h_{2,M} P_{2,M}^*}{L} + \sigma^2\Big)}{\frac{h_{2,M} P_{2,M}^*}{L} + h_1 P_1^* + \sigma^2} = E_1. \quad (37)$$

In Nash equilibrium, the type uncertainty is better for selfish node 1 (i.e., selfish node hides its type), if h_1 is small and E_1 is large, or it is better for malicious node 2, otherwise.

C. Malicious Transmitter 1 (Known Type) and Transmitter 2 of Unknown Type

Theorem 9: For $\phi_1 \in (0,1)$, the *Bayesian Nash equilibrium* strategies $P_1 \geq 0$, $P_{2,S} \geq 0$ and $P_{2,M} \geq 0$ are

$$P_1 = \frac{L}{h_1}\Big[\frac{h_{2,S}}{E_{2,S}} - h_{2,S} P_{2,S} - \sigma^2\Big]^+, \quad (38)$$

$$P_{2,S} = \frac{E_1 h_{2,S} L}{E_{2,S}(L E_1 h_{2,S} + \phi_1 E_{2,S} h_1)}, \quad (39)$$

$$P_{2,M} = 0. \quad (40)$$

As ϕ_1 decreases, P_1 decreases and $P_{2,S}$ increases from the equilibrium strategies (38)-(39). Consequently, the equilibrium SINR $\gamma_{2,S}$ of selfish node 2 increases, as ϕ_1 decreases, i.e., the type uncertainty is beneficial for the selfish node of unknown type.

D. Transmitters 1 and 2 of Unknown Types

Theorem 10: For $\phi_S \in (0,1)$ and $\phi_M \in (0,1)$, the symmetric *Bayesian Nash equilibrium* strategies are

$$P_S = [P_S^*]^+, \quad P_M = [P_M^*]^+, \quad (41)$$

where P_S^* and P_M^* are solutions to

$$\frac{P_S^*}{\Big(\frac{h_M P_M^*}{L} + \sigma^2\Big)\Big(\frac{h_M P_M^*}{L} + h_S P_S^* + \sigma^2\Big)} = \frac{L E_M}{\phi_M h_M h_S}, \quad (42)$$

$$\frac{\phi_S h_S \sigma^2}{\Big(\frac{h_S P_S^*}{L} + \sigma^2\Big)\Big(\frac{h_S P_S^*}{L} + h_S P_S^* \sigma^2\Big)} + \frac{(1-\phi_S) h_S}{\frac{h_M P_M^*}{L} + h_S P_S^* + \sigma^2} = E_S. \quad (43)$$

For $h_S = h_M = 1$, $E_S = E_M = 1$, $L = 1$ and $\sigma^2 = 0$, the equilibrium transmission powers from (41)-(43) are given by $P_S = \frac{(1-\phi_S)^2}{1-\phi_S+\phi_M}$ and $P_M = \frac{(1-\phi_S)\phi_M}{1-\phi_S+\phi_M}$ for selfish and malicious nodes, respectively. If the opponent is malicious, the equilibrium SINR value of selfish node is given by $\gamma_S = \frac{1-\phi_S}{\phi_M}$, which decreases with both ϕ_S and ϕ_M, i.e., any selfish node prefers type uncertainty and should hide its type to increase the SINR value γ_S.

V. Bayesian Learning of Selfish and Malicious User Types in Power-Controlled MAC

Next, we deviate from the previous focus of fixed and known type belief distributions and extend the analysis to the dynamic situation in which nodes learn each other's types based on the outcomes of the power-controlled MAC game at each time slot. Consider the reward function $f(\gamma_S) = \gamma_S$ for unknown types of two transmitters.

For simplicity, assume $h_S = h_M = 1$, $E_S = E_M = 1$, $L = 1$ and $\sigma^2 = 0$. Selfish and malicious nodes play the Nash equilibrium strategies $P_S(\phi_S, \phi_M) = \frac{(1-\phi_S)^2}{\phi_M}$ and $P_M(\phi_S, \phi_M) = 1 - \phi_S$ from (23)-(25). Selfish and malicious nodes update ϕ_S and ϕ_M, respectively, based on the opponent's power (which can be observed through the SINR feedback sent from the receiver back to the transmitters).

Nodes assume that the belief of the opponent with the opposite type is *uniformly* distributed over $[0,1]$, whereas nodes of the same type have the same belief distribution and update their beliefs according to the same rule. Define $P_o^{(k)}$ as the opponent's power and $\phi_S^{(k)}$ as the value of ϕ_S at the kth iteration. *Selfish* and *malicious* nodes update their beliefs ϕ_S and ϕ_M, respectively, on the opponent's type according to the Bayes' rule:

$$\phi_S^{(k+1)} = \frac{\phi_S^{(k)}\, a_S^{(k)}(P_o^{(k)})}{\phi_S^{(k)}\, a_S^{(k)}(P_o^{(k)}) + (1-\phi_S^{(k)})\, b_S^{(k)}(P_o^{(k)})}, \quad (44)$$

$$\phi_M^{(k+1)} = \frac{\phi_M^{(k)}\, a_M^{(k)}(P_o^{(k)})}{\phi_M^{(k)}\, a_M^{(k)}(P_o^{(k)}) + (1-\phi_M^{(k)})\, b_M^{(k)}(P_o^{(k)})}, \quad (45)$$

where $a_i^{(k)}(P_o^{(k)}) = P(P_o^{(k)} |$ the opponent of node i is selfish$)$ and $b_i^{(k)}(P_o^{(k)}) = P(P_o^{(k)} |$ the opponent of node i is malicious$)$ for $i \in \{S, M\}$ can be computed as

$$a_S^{(k)}(P_o^{(k)}) = \begin{cases} 0, & P_o^{(k)} < (1-\phi_S^{(k)})^2, \\ 1, & P_o^{(k)} \geq (1-\phi_S^{(k)})^2, \end{cases} \quad (46)$$

$$b_S^{(k)}(P_o^{(k)}) = b_M^{(k)}(P_o^{(k)}) = \begin{cases} 0, & P_o^{(k)} > 1, \\ 1, & P_o^{(k)} \leq 1, \end{cases} \quad (47)$$

$$a_M^{(k)}(P_o^{(k)}) = \begin{cases} \frac{1}{3\left(P_o^{(k)}\right)^2}, & P_o^{(k)} > 1, \\ \frac{1}{3\sqrt{P_o^{(k)}}}, & P_o^{(k)} \leq 1. \end{cases} \quad (48)$$

A selfish node eventually detects the type of the selfish opponent with power $P_o^{(k)}$, whenever $P_o^{(k)} > 1$ is observed, or it detects the type of the malicious opponent, whenever $P_o^{(k)} < (1-\phi_S^{(k)})^2$ is observed. From (44)-(45), we have $\phi_S^{(k+1)} = \phi_S^{(0)}$, until the type of the opponent is detected. The

number of iterations to detect the opponent as a selfish or malicious node is a *geometric* random variable with success probability $(1-\phi_S^{(0)})^2$.

On the other hand, a malicious node eventually detects the type of selfish opponent, whenever $P_o^{(k)} > 1$ is observed or whenever the selfish node detects the type of malicious opponent at the previous iteration (and updated its transmission power accordingly). Then, the expected number of iterations to detect the opponent as a selfish node can be computed as $p + \frac{1}{1-p}\left[\frac{1}{1-(1-p)^2} - (1-(1-p)^2)\right]$, where $p = (1-\phi_S^{(0)})^2$, and the average detection time grows with $\phi_S^{(0)}$.

However, a malicious node cannot detect the type of a malicious opponent with probability one at a particular iteration, but the probability $\phi_M^{(k)}$ asymptotically approaches 0 according to the Bayesian update mechanism (45), as the number of time iterations k increases. Figure 5 shows the updates of the malicious node's type belief probability $\phi_M^{(k)}$ averaged over the distribution of the opponent's power $P_o^{(k)}$. Note that the probability $\phi_M^{(k)}$ converges with smaller rate, if the malicious node selects a larger value for the initial type belief probability $\phi_M^{(0)}$ that the opponent is selfish.

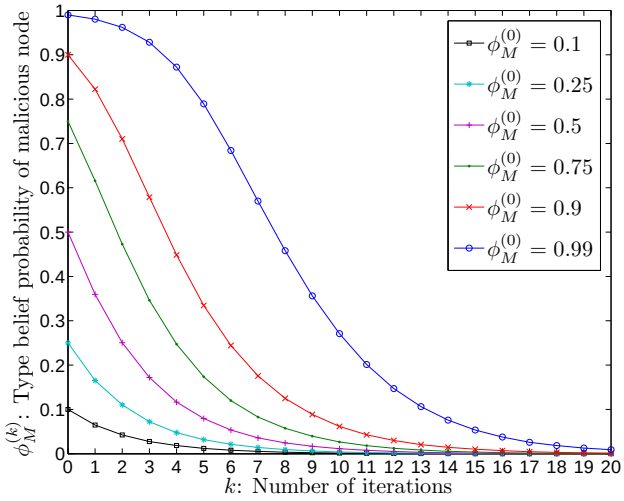

Fig. 5. The type belief probability $\phi_M^{(k)}$ of a malicious node with a malicious opponent for $f(\gamma_S) = \gamma_S$, $h_S = h_M = 1$, $E_S = E_M = 1$, $L = 1$ and $\sigma^2 = 0$.

VI. Power-Controlled MAC Game for Arbitrary Number of Selfish and Malicious Transmitters

Let n and n_s denote the total number of nodes and the number of selfish nodes, respectively, where $n \leq n_{\max}$ and $n_{\max}$ is the maximum possible number of nodes in the system. Let $\eta_S(n, n_s)$ and $\eta_M(n, n_s)$ denote the joint probability mass function of n and n_s, as believed by a selfish and malicious node, respectively. Consider common parameters (known by all nodes), as defined in Section III-D, and assume symmetric strategies P_S or P_M depending on whether the node is selfish or malicious. For the common reward function $f_i(\gamma) = f(\gamma)$ of any selfish node i, the utilities of selfish and malicious nodes are given by

$$u_S(P_S, P_M) = \sum_{n=1}^{n_{\max}} \sum_{n_s=1}^{n} \eta_S(n, n_s)\, f\left(\frac{h_S P_S}{\psi(n_s)}\right) - P_S E_S, \quad (49)$$

$$u_M(P_S, P_M) = -\sum_{n=1}^{n_{\max}} \sum_{n_s=0}^{n-1} \eta_M(n, n_s)\; n_s\; f\left(\frac{h_S P_S}{\psi(n_s)}\right) - P_M E_M, \quad (50)$$

respectively, where $\psi(\tilde{n}) = \frac{1}{L}\Big((\tilde{n}-1)h_S P_S + (n-\tilde{n})h_M P_M\Big) + \sigma^2$. Any malicious node minimizes the sum of throughput rewards of all n_s possibly selfish nodes subject to the additional objective of minimizing the energy cost.

Theorem 11: The symmetric Bayesian Nash equilibrium strategies P_S and P_M of selfish and malicious transmitters are

$$P_S = [P_S^*]^+, \quad P_M = [P_M^*]^+, \quad (51)$$

where P_M^* and P_S^* are solutions to

$$\frac{E_S}{h_S} = \sum_{n=1}^{n_{\max}} \sum_{n_s=1}^{n} \eta_S(n, n_s)\left(\frac{\frac{1}{L}(n-n_s)h_M P_M^* + \sigma^2}{\psi(n_s)(\psi(n_s)+\zeta)}\right), \quad (52)$$

$$\frac{E_M L}{h_S h_M} = \sum_{n=1}^{n_{\max}} \sum_{n_s=0}^{n-1} \eta_M(n, n_s)\left(\frac{n_s(n-n_s)P_S^*}{\psi(n_s)(\psi(n_s)+\zeta)}\right) \quad (53)$$

for *perfect* information of type beliefs, where $\psi(\tilde{n}) = \frac{1}{L}\Big((\tilde{n}-1)h_S P_S^* + (n-\tilde{n})h_M P_M^*\Big) + \sigma^2$, $\zeta = 0$ for $f(\gamma_S) = \gamma_S$ and $\zeta = h_S P_S$ for $f(\gamma_S) = \log(1+\gamma_S)$.

Proof: The equilibrium strategies (51)-(53) follow from applying the KKT conditions (generalized to arbitrary number of nodes) separately to the objective functions $u_S(P_S, P_M)$ of selfish nodes and $u_M(P_S, P_M)$ of malicious nodes, with constraints $P_S \geq 0$ and $P_M \geq 0$, where the utilities u_S and u_M are given by (49)-(50), respectively. ■

The equilibrium SINR of any selfish node is given by $\gamma_S = \frac{h_S P_S}{\psi(n_s)}$. Assume $E_S h_M = E_M h_S$ and $L = 1$. For both reward functions $f(\gamma_S) = \gamma_S$ and $f(\gamma_S) = \log(1+\gamma_S)$, the equilibrium value of γ_S for given n decreases first with the small values of n_s, then reaches the minimum for the intermediate values n_s, and finally increases with the large values of n_s. There exists a critical value for the number of malicious nodes beyond which γ_S increases again, i.e., a malicious attack is more successful, if it is accompanied with the selfish behavior of other nodes. The total throughput reward $n_s\gamma_S$ increases monotonically with the number of selfish nodes n_s, as shown in Figure 6.

VII. Random Access Games for Selfish and Malicious Transmitters of Unknown Types

The results for power control game with incomplete type information generalize to other MAC models. Next, consider *random access* games, where nodes choose between transmitting and waiting. Assume a synchronous slotted system with *collision channels* such that more than one simultaneous transmission fails. The primary focus is again on the case

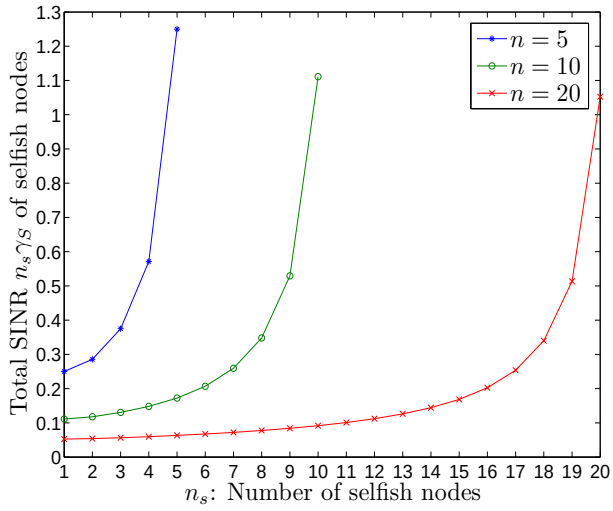

Fig. 6. The total SINR $n_s\gamma_S$ of selfish nodes in Nash equilibrium as function of n_s for $E_S h_M = E_M h_S$ and $L = 1$.

of two transmitters. Define $p_i \in [0,1]$ as transmission probability and $E_i \in (0,1)$ as energy cost (per transmission) of node $i = 1, 2$. Any *selfish* node i receives unit *throughput* reward for successful transmission. The expected utility of selfish node i is given by

$$u_i(p_1, p_2) = p_i\left[-E_i + 1 - p_j\right] + (1 - p_i)\left[0\right],\ j \neq i, \quad (54)$$

for $i = 1, 2$. Any *malicious* node i incurs a unit cost, if the opponent is selfish *and* successfully transmits at the given time slot. The expected utility of malicious node i is given by

$$u_i(p_1, p_2) = \begin{cases} p_i\left[-E_i\right] + (1 - p_i)\left[-p_j\right], \\ \text{if the opponent node } j \text{ is selfish}, \\ p_i\left[-E_i\right] + (1 - p_i)\left[0\right], \\ \text{if the opponent node } j \text{ is malicious}, \end{cases} \quad (55)$$

for $j \neq i$, $i = 1, 2$.

Theorem 12: The symmetric *Bayesian Nash equilibrium* strategies p_S and p_M of selfish and malicious transmitters are

$$p_S = 1,\ p_M = 0,\ \text{if } \phi_S < 1 - E_S,\ \phi_M < E_M, \quad (56)$$

$$p_S = \frac{1 - E_S}{\phi_S},\ p_M = 0,$$

$$\text{if } \phi_S > 1 - E_S,\ E_M\phi_S > \phi_M(1 - E_S), \quad (57)$$

$$p_S = \frac{E_M}{\phi_M},\ p_M = \frac{1 - E_S - E_M\frac{\phi_S}{\phi_M}}{1 - \phi_S},$$

$$\text{if } \phi_S < E_S + E_M\frac{\phi_S}{\phi_M} < 1,\ \phi_M > E_M. \quad (58)$$

Proof: (*a*) The expected utility of a given selfish node $u_S(p_S, p_M) = p_S(-E_S + \phi_S(1 - p_S) + (1 - \phi_S)(1 - p_M))$ is maximized by transmitting, i.e., $p_S = 1$, if $(1 - \phi_S)(1 - p_M) > E_S$. Given $p_S = 1$, the expected utility of a malicious node $u_M(p_S, p_M) = p_M(-E_M) + (1 - p_M)(-\phi_M p_S)$ is maximized by waiting, i.e., $p_M = 0$, if $\phi_M < E_M$, or by transmitting, if $\phi_M > E_M$. However, $u_S(p_S, 1)$ is not maximized by $p_S = 1$ (therefore the strategy pair $p_S = 1$ and $p_M = 1$ does not yield a Nash equilibrium), whereas $u_S(p_S, 0)$ is maximized by $p_S = 1$, if $1 - \phi_S > E_S$ such that the Nash equilibrium strategy (56) follows.

The utility of a selfish node $u_S(p_S, p_M)$ is maximized by waiting, i.e., $p_S = 0$, if $(1-\phi_S)(1-p_M) < E_S$. Given $p_S = 0$, the utility of a malicious node $u_M(p_S, p_M)$ is maximized by waiting only, i.e., $p_M = 0$. However, $u_S(p_S, 0)$ cannot be maximized by $p_S = 0$, and therefore the strategy $p_S = 0$ does not yield a Nash equilibrium.

(*b*) Given $p_M = 0$, the utility of a selfish node $u_S(p_S, p_M)$ is maximized by transmitting, i.e., $p_S = 1$, if $1 - E_S - \phi_S > 0$. This corresponds to Nash equilibrium strategy (56). The strategy $p_S = 1$ cannot yield Nash equilibrium, since it violates the condition $E_S < 1$. The utility $u_S(p_S, p_M)$ is indifferent to p_S, if $p_S = \frac{1-E_S}{\phi_S}$. Given $p_S = \frac{1-E_S}{\phi_S}$, the utility of a malicious node $u_M(p_S, p_M)$ is maximized by waiting, i.e., $p_M = 0$, if $E_M\phi_S > \phi_M(1 - E_S)$ such that the Nash equilibrium strategy (57) follows. For $p_S = \frac{1-E_S}{\phi_S}$, $p_M = 1$ cannot yield any Nash equilibrium, since $u_S(p_S, 1)$ is maximized only by $p_S = 0$ provided that $E_S > \phi_S$ and $u_M(0, p_M)$ cannot be maximized by $p_M = 1$.

(*c*) Consider mixed strategies such that selfish and malicious nodes are indifferent to p_S and p_M, respectively, to maximize u_S and u_M. From $u_S(1, p_M) = u_S(0, p_M)$ and $u_M(p_S, 1) = u_M(p_S, 0)$, we obtain the equilibrium strategy (58) subject to $0 \leq p_S \leq 1$ and $0 \leq p_M \leq 1$. ■

If the type belief distributions $\phi_S = \phi_M$ are equal to the true probability that a node is selfish, the resulting throughput rates are $\lambda_S = 1 - \phi_S$, $\lambda_S = \frac{E_S(1-E_S)}{\phi_S}$ and $\lambda_S = E_M\left(1 + \frac{E_S}{\phi_S}\right)$ for the strategies (56)-(58), respectively.

Consider a selfish node with malicious opponent. The throughput rates are $\lambda_S = 1$, $\lambda_S = \frac{1-E_S}{\phi_S}$ and $\lambda_S = \frac{E_M}{\phi_M}\left(\frac{E_S + E_M\frac{\phi_S}{\phi_M} - \phi_S}{1-\phi_S}\right)$ for the strategies (56)-(58), respectively. If the types are known, the equilibrium strategies are $p_S = E_M$ and $p_M = 1 - E_S$ with throughput $\lambda_S = E_M E_S$. Then, the strategy (56) achieves higher throughput. It is beneficial for the selfish node to hide its type such that the strategy (57) is more throughput-efficient, if $E_S(1 + E_M\phi_S) < 1$, which holds for small energy costs, and the strategy (58) is more throughput-efficient, if $E_S(1 - \phi_M(1 - \phi_S)) > \phi_S(1 - \frac{E_M}{\phi_M})$, which holds for large energy costs.

Selfish and malicious nodes can further choose ϕ_S and ϕ_M, respectively, to maximize and minimize the throughput λ_S of a selfish node. The resulting equilibrium probabilities are $\phi_M^* = 1$ and $\phi_S^* = 0$, if $E_S + E_M < 1$, with throughput $\lambda_S = E_S E_M$, or $\phi_S^* = \frac{1-E_S}{E_M}$, if $E_S + E_M > 1$, with throughput $\lambda_S = E_M$. Hence, the equilibrium throughput λ_S can be improved, if $E_S + E_M < 1$, compared to the case of known types with equilibrium throughput $\lambda_S = E_S E_M$.[3]

[3]The receiver can identify the type of any node (i.e., whether the received packet carries real data or constitutes to a jamming signal), if it is the only one transmitting at the given time slot. Then, we can consider a *Markov game* formulation such that the strategy of a node depends on its type and the state of the game that is updated, whenever the type of any node is detected by the receiver.

A. Unknown Type Belief Distributions and Energy Costs

Assume that node i does not know the exact values of type belief probability ϕ_j and energy cost E_j of the opponent node j, but knows their distributions. The uncertainties on node types and energy costs are *jointly* formulated as probabilistic beliefs. Define μ_i as the subjective belief (namely the probability distribution) of node $i = 1, 2$ about the parameters ϕ_j and E_j of the opponent $j \neq i$. Consider the symmetric game model such that any selfish node has belief μ_S and any malicious node has belief μ_M.

Theorem 13: The *Nash equilibrium* strategy of a *selfish* or *malicious* node is to transmit, respectively, if and only if

$$\theta_S = \frac{E_S}{1-\phi_S} < \theta_S^* = 1 - \mu_S(\theta_M < \theta_M^*), \quad \text{or} \tag{59}$$

$$\theta_M = \frac{E_M}{\phi_M} < \theta_M^* = \mu_M(\theta_S < \theta_S^*). \tag{60}$$

Proof: Each node assumes that the opponent node of the same type would make the same decision to transmit or to wait. Any selfish node transmits, if $u_S(1, p_M) > u_S(0, p_M)$, where u_S is given by (54), i.e., if $E_S < (1-\phi_S)(1-p_M)$, or waits, if $E_S > (1-\phi_S)(1-p_M)$. In the case of equality, the selfish node either transmits or waits. This leads to monotonic transmission decision of selfish node such that $\theta_S = \frac{E_S}{1-\phi_S} < \theta_S^*$, where $\theta_S^* = 1 - p_M$. Selfish node does not know the transmission probability p_M of malicious node but has subjective belief distribution for p_M, if the transmission decision of any malicious node also satisfies the monotonicity property in terms of type belief and cost parameters.

Any malicious node transmits, if $u_M(p_S, 1) > u_M(p_S, 0)$, where u_M is given by (55), i.e., if $E_M < \phi_M p_S$, or waits, if $E_M > \phi_M p_S$. In the case of equality, the malicious node either transmits or waits. This also leads to monotonic transmission decisions of malicious node such that $\theta_M = \frac{E_M}{\phi_M} < \theta_M^*$, where $\theta_M^* = p_S$. Malicious node does not know the transmission probability p_S of selfish node but has subjective belief distribution for p_S, since the transmission decisions of selfish node are also monotonic in terms of type belief and cost parameters. The threshold parameters are $\theta_S^* = 1 - p_M^*$ with $p_M^* = \mu_S(\theta_M < \theta_M^*)$ and $\theta_M^* = p_S^*$ with $p_S^* = \mu_M(\theta_S < \theta_S^*)$ such that the monotonic transmission decisions (59)-(60) follow in Nash equilibrium. ■

If the opponent's beliefs on type probabilities ϕ_S and ϕ_M and costs E_S and E_M are *independent* and *uniformly* distributed over $[0, 1]$ for each selfish and malicious node, the parameters $\theta_S = \frac{E_S}{1-\phi_S}$ and $\theta_M = \frac{E_M}{\phi_M}$ follow a uniform ratio distribution

$$P(\theta_i = \theta) = \begin{cases} \frac{1}{2}, & 0 < \theta < 1, \\ \frac{1}{2\theta^2}, & \theta \geq 1, \\ 0, & \text{otherwise}, \end{cases} \qquad i \in \{S, M\}. \tag{61}$$

From (59)-(60), there exist *unique* equilibrium thresholds $\theta_S^* = \frac{4}{5}$ and $\theta_M^* = \frac{2}{5}$. A selfish node with malicious opponent achieves equilibrium throughput $\lambda_S = \frac{8}{25}$, which is greater than the throughput $\lambda_S = \frac{1}{4}$ averaged over cost distributions for known types. Hence, the type uncertainty is beneficial for selfish nodes to increase the equilibrium throughput λ_S.

B. Arbitrary Number of Selfish and Malicious Users

Consider the probabilistic belief distributions $\eta_S(n, n_s)$ and $\eta_M(n, n_s)$ of selfish and malicious nodes to represent the total number of nodes n and the number of selfish nodes n_s (as defined in Section VI for power control). Assume a *symmetric* game model with transmission probability p_S and p_M for any selfish and malicious node, respectively. Any malicious node wishes to minimize the sum of selfish throughput rewards and incurs a unit cost for each successfully transmitting selfish node. The expected utility of a selfish node is

$$u_S(p_S, p_M) = \sum_{n=1}^{n_{\max}} \sum_{n_s=1}^{n} \eta_S(n, n_s) \Big(p_S \left[-E_S \right. \\ \left. + (1-p_S)^{n_s - 1} (1-p_M)^{n-n_s} \right] + (1-p_S) \left[0 \right] \Big) \tag{62}$$

and the expected utility of a malicious node is

$$u_M(p_S, p_M) = \sum_{n=1}^{n_{\max}} \sum_{n_s=0}^{n-1} \eta_M(n, n_s) \Big(p_M \left[-E_M \right] \\ + (1-p_M) [-n_s p_S (1-p_S)^{n_s - 1} (1-p_M)^{n-n_s-1}] \Big). \tag{63}$$

Theorem 14: For *perfect* information of $\eta_S(n, n_s)$ and $\eta_M(n, n_s)$, the symmetric *Bayesian Nash equilibrium* strategies p_S and p_M of selfish and malicious transmitters are

$$p_S = \min\left([p_S^*]^+, 1 \right), \quad p_M = \min\left([p_M^*]^+, 1 \right), \tag{64}$$

where p_S^* and p_S^* are solutions to

$$E_S = \sum_{n=1}^{n_{\max}} \sum_{n_s=1}^{n} \eta_S(n, n_s) \\ \times [(1 - n_S p_S)(1-p_S)^{n_s - 2} (1-p_M)^{n-n_s}], \tag{65}$$

$$E_M = \sum_{n=1}^{n_{\max}} \sum_{n_s=0}^{n-1} \eta_M(n, n_s)\, n_s\, (n - n_s) \\ \times p_S (1-p_S)^{n_s - 1}\, (1-p_M)^{n-n_s-1}. \tag{66}$$

Proof: The equilibrium strategies p_S and p_M from (64)-(66) follow from applying the KKT conditions separately to the objective functions $u_S(p_S, p_M)$ of any selfish node and $u_M(p_S, p_M)$ of any malicious node with constraints $0 \leq p_S \leq 1$ and $0 \leq p_M \leq 1$, where $u_S(p_S, p_M)$ and $u_M(p_S, p_M)$ are given by (62)-(63), respectively. ■

The throughput of any selfish node in Nash equilibrium is given by $\lambda_S = p_S(1-p_S)^{n_s-1}(1-p_M)^{n-n_s}$. Figure 7 evaluates λ_S as function of n, where $n_s = 1$, and shows that λ_S decreases as the number of malicious nodes increases (except for small values of energy costs E_S and E_M and total number of nodes n).

Assume *partial information* on the probabilistic belief of the opponent on the values of n and n_s. Let $n(i)$ and $n_s(i)$ denote the total number of nodes and the number of selfish nodes believed by any selfish node $i = S$ or by any malicious node $i = M$. Let $\mathcal{P}_i(n, n_s)$ denote the probability distribution function that selfish or malicious node $i \in \{S, M\}$ believes to represent the belief of node $j \in \{S, M\}$, $j \neq i$, on the values of n and n_s.

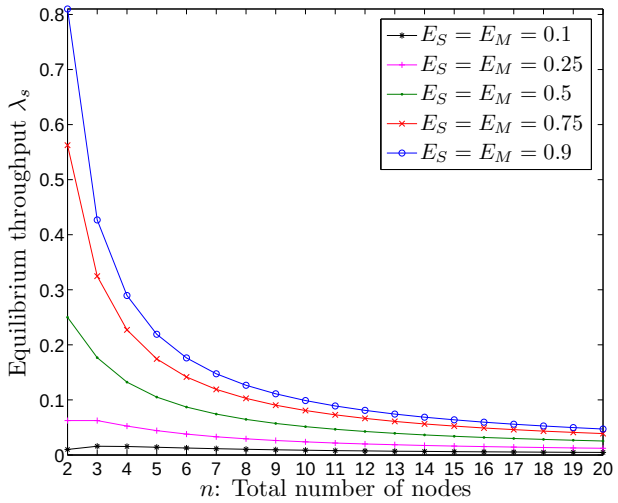

Fig. 7. The throughput λ_S achievable by one selfish node in Nash equilibrium as function of n for $n_s = 1$.

Each node assumes that any other node of the same type would make the same transmission decision. Any selfish node transmits (i.e., $p_S = 1$), if $u_S(1, p_M) > u_S(0, p_M)$ in Eq. (62), i.e., if $(1 - p_M)^{n-1} > E_S$ and $n_s = 1$. On the other hand, any malicious node transmits (i.e., $p_S = 1$), if $u_M(p_S, 1) \geq u_M(p_S, 0)$ in Eq. (63), i.e., if $n_s p_S (1 - p_S)^{n_s - 1} > E_M$. For *incomplete* information on node types, the transmission decisions in Nash equilibrium satisfy the following monotonicity properties:

Any *selfish* node transmits, if and only if

$$n(S) < n^*(S), \quad n_s(S) = 1, \tag{67}$$

and any *malicious* node transmits, if and only if

$$n^*_{s,1}(M) < n_s(M) < n^*_{s,2}(M), \tag{68}$$

provided that the non-negative cut-off thresholds $n^*(S)$ and $n^*_{s,2}(M)$ are the largest solutions and the non-negative cut-off threshold $n^*_{s,1}(M)$ is the smallest solution to

$$\left(1 - \varphi_M\right)^{n^*(S)-1} \geq E_S, \tag{69}$$

$$n^*_{s,i}(M)\, \varphi_S \left(1 - \varphi_S\right)^{n^*_{s,i}(M)} \geq E_M, \quad i = 1, 2, \tag{70}$$

where

$$\varphi_S = \sum_{1 \leq n < n^*(S)} \mathcal{P}_M(n, 1), \tag{71}$$

$$\varphi_M = \sum_{n^*_{s,2}(M) \leq n} \quad \sum_{n^*_{s,1}(M) < n_s < n^*_{s,2}(M)} \mathcal{P}_S(n, n_s). \tag{72}$$

VIII. Conclusions

We presented game-theoretic models to establish a security paradigm at the MAC layer of wireless networks. For selfish and malicious users of unknown types, we considered different MAC models based on power control and random access, and derived the Nash equilibrium strategies depending on the degree of type uncertainty. The performance is measured in terms of throughput rewards, transmission energy costs and malicious attack incentives. The analysis showed under what conditions the type identities should be concealed or revealed to improve the individual performance as a selfish user or to reduce the system performance as a malicious user.

We also extended the results to incorporate different degrees of uncertainty in type distributions and cost parameters, and presented Bayesian learning mechanisms for the type belief updates. The analysis provides new insights into using the type uncertainty as an inherent defense mechanism against the denial of service attacks in wireless networks.

Future work should generalize the game model to multi-hop wireless networks. This would extend the denial of service attack possibilities to the network layer operations and require cross-layer design with the attack and defense mechanisms that have been established for the MAC layer.

References

[1] H. Ji and C. Huang, "Non-cooperative Uplink Power Control in Cellular Radio Systems," *Wireless Networks*, vol. 4, no. 3, pp. 233-240, Mar. 1998.

[2] C. Saraydar, N. B. Mandayam, and D. J. Goodman, "Efficient Power Control via Pricing in Wireless Data Networks," *IEEE Trans. Commun.*, vol. 50, no. 2, pp. 291-303, Feb. 2002.

[3] T. Alpcan, T. Basar, R. Srikant, and E. Altman, "CDMA Uplink Power Control as a Noncooperative Game," *Wireless Networks*, vol. 8, no. 6, pp. 659-670, Nov. 2002.

[4] A. B. MacKenzie and S. B. Wicker, "Game Theory and the Design of Self-Configuring, Adaptive Wireless Networks," *IEEE Commun. Mag.*, vol. 39, no. 11, pp. 126-131, Nov. 2001.

[5] Y. Jin and G. Kesidis, "Equilibria of a Non-cooperative Game for Heterogeneous Users of an Aloha Network," *IEEE Communications Letters*, vol. 6, no. 7, pp. 282-284, July 2002.

[6] J.-W Lee, M. Chiang, and R. A. Calderbank, "Utility-Optimal Random-Access Control," *IEEE Trans. Wireless Commun.*, vol. 6, no. 7, pp. 2741-2751, July 2007.

[7] J. Zander, "Jamming in Slotted ALOHA Multihop Packet Radio Networks," *IEEE Trans. Commun.*, vol. 39, no. 10, pp. 1525-1531, Oct. 1991.

[8] A. Kashyap, T. Basar, and R. Srikant, "Correlated Jamming on MIMO Gaussian Fading Channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119-2123, Sept. 2004.

[9] Y. E. Sagduyu and A. Ephremides, "SINR-Based MAC Games for Selfish and Malicious Users," *Proc. Information Theory and Applications Workshop*, San Diego, CA, Jan. 2007.

[10] Y. E. Sagduyu and A. Ephremides, "A Game-Theoretic Analysis of Denial of Service Attacks in Wireless Random Access," *Proc. WiOpt07*, Limassol, Cyprus, Apr. 2007.

[11] E. Altman, K. Avratchenkov, and A. Garnaev, "A Jamming Game in Wireless Networks with Transmission Cost," *Proc. Net-Coop*, Avignon, France, June 2007.

[12] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks," *Proc. GameNets*, Pisa, Italy, Oct. 2006.

[13] S. Radosavac, A. A. Cardenas, J. S. Baras, and G. V. Moustakides, "Detecting IEEE 802.11 MAC Layer Misbehavior in Ad Hoc Networks: Robust Strategies Against Individual and Colluding Attackers," *Journal of Computer Security*, vol. 15, no. 1, pp. 103-128, Jan. 2007.

[14] G. Theodorakopoulos and J. Baras, "Game Theoretic Modeling of Malicious Users in Collaborative Networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1317-1327, Sept. 2008.

[15] H. Inaltekin and S. B. Wicker, "Random Access Games: Selfish Nodes with Incomplete Information," *Proc. IEEE MILCOM*, Orlando, FL, Oct. 2007.

[16] Mingyan Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attack and Network Defense Policies in Wireless Sensor Networks," *Proc. IEEE INFOCOM*, Anchorage, AK, May 2007.

[17] M. Babaioff, R. Kleinberg, and C. H. Papadimitriou, "Congestion Games with Malicious Players," *Proc. ACM Conf. Electronic Commerce*, San Diego, CA, June 2007.