Bayesian-Based Game Theoretic Model to Guarantee Cooperativeness in Hybrid RF/FSO Mesh Networks

Osama Awwad[*], Ala Al-Fuqaha[*], Bilal Khan[†], Driss Benhaddou[+], Mohsen Guizani[*], Ammar Rayes[┼]
[*]Computer Science Department, Western Michigan University
{oaawwad, alfuqaha, mguizani }@cs.wmich.edu
[†]John Jay College, City University of New York.
bkhan@jjay.cuny.edu
[+]Engineering Technology Department, University of Houston
dbenhaddou@uh.edu
[┼]Advanced Support Technology Group, Cisco Systems, Inc.
rayes@cisco.com

***Abstract*—**In this paper we describe an effective new technique by which to guarantee cooperativeness in Hybrid Radio-Frequency/Free Space Optics (RF/FSO) networks. Our approach is based on a novel Bayesian game-theoretic model, and uses a pricing scheme in which each destination node pays some amount of virtual money to the source node in order to acquire a reliable connection. We describe both single-stage and multi-stage solutions for the game in terms of its Nash and Perfect Bayesian Equilibriums. Pure strategies are found when the required conditions are met; otherwise the game is played as a mixed-strategy. Our numerical results quantify the inherent tradeoffs involved in changing the game's parameters vis-a-vis the equilibrium player strategies and game's outcomes.

***Index Terms*— Hybrid RF/FSO, QoS, Reliable Routing, Game Theory, Nash Equilibrium, Bayesian Game.**

I. INTRODUCTION

Most wireless networks are deployed strictly in the radio frequency (RF) domain, since RF channels provide natural support for radial broadcast operations. However, the downside of RF channels is that they introduce many limiting externalities that make providing scalable quality of service (QoS) support difficult, if not intractable. These well-known technical challenges include bandwidth scarcity, lack of security, high interference, and high bit error rates.

Faced with such daunting obstacles to QoS, several researchers have recently proposed the use of Free Space Optics (FSO) for wireless communications [2-6]. First, FSO has the potential to support higher link data rates compared to present RF technology. Furthermore, because FSO uses directed optical transmissions in which channel beam-width is adjustable, inter-FSO communication interference can be limited. Finally, the avoidance of radial broadcasting also provides some degree of security against eavesdropping. The benefits of FSO do not come without a price, most notable of which is the need to maintain line of sight (LOS) between the transmitter and the receiver during the course of communication. Moreover, FSO link availability can be degraded by adverse weather conditions like fog, rain, snow, and haze. Finally, when link endpoints are mobile, maintaining stable LOS requires potentially sophisticated tracking technology.

Clearly, a hybrid approach that uses both RF and FSO is needed to overcome the shortcomings of each medium, which we have just described. The cost and structure of RF and FSO channels in a hybrid RF/FSO networks will depend on the channel conditions and the desired QoS, respectively. But deciding to use a hybrid model brings with it, its own set of unique problems, stemming in large part from the fact that nodes can choose between two *different* channels types—each with its own transmission characteristics. Given this, steps must be taken to prevent a relay node in a multi-hop connection from being tempted to behave selfishly by forwarding other nodes' packets using the less reliable channel type, thereby avoiding the individual opportunity cost that would be incurred by a "fairer" choice of allocating a high quality link. We address this problem of selfish behavior by formulating node decisions within a hybrid RF/FSO network in a Bayesian game-theoretic model that is designed specifically to guarantee optimal cooperativeness—this model, its formal analysis, and the experimental verification of its properties are the principal contributions of this paper.

We note that the application of game theory to resolving conflicts of interest between nodes in wireless networks is not new. In [10], for example, the authors recast the routing problem for ad hoc networks in terms of a pricing model, in which the destination node gives some amount of virtual money as payment to the source node for each packet of information that is delivered. While the authors of [10] were able to demonstrate a polynomial time modification of Dijkstra's algorithm that can compute a Nash equilibrium path, their model may not be realistic in some scenarios since it does not distinguish between selfish and cooperative nodes in the network. Most prior work that applies game theory to wireless networks assumes complete information among nodes, which is to say, all knowledge about all other players is

978-1-4244-4148-8/09/$25.00 ©2009

available to all players. In practice, this would not be the case since nodes have private information and might not reveal their strategies for strategic reasons. Relatively few investigations have considered these subtle issues; here we will mention briefly, just two. In [11], the authors provided an incomplete-knowledge game theoretic model for an Intrusion Detection System and analyzed the interactions between attacking and defending nodes; static and dynamic games were developed to capture incomplete information regarding the maliciousness of neighboring nodes. In [12], the authors provided a theoretical model to analyze routing behavior in MANETs based on a dynamic multi-stage Bayesian game which incorporates both uncertainty and history, and in which posterior beliefs are updated after each stage.

The rest of this paper is organized as follows. In Section II, we define the *Selfishness Problem* for hybrid RF/FSO networks. In Section III, we describe the system model as a Bayesian static game and provide an analysis. In Section VI, we analyze a repeated multi-stage game extension of the static game. In Section V, we describe our experimental results and interpret the observed outcomes. Finally, in Section VI, we present overall conclusions and the future trajectory of our research efforts.

II. PROBLEM DEFINITION

In wireless mesh networks, if nodes are permitted to be governed by unmitigated self-interest, they may choose to forward packets on low quality links (thereby incurring a lower opportunity cost) rather than inhabiting a cooperative modality in which they forward traffic onto a high-quality links which a connection might fairly deserve. How can this be addressed? We presume here that every source node (be it selfish or cooperative) is *rational*. Specifically, a selfish node would not forward data on to low quality links all the time, if it knew that such poor citizenship would result in strong retribution by the network elements. On the other hand, detecting bad behavior on the part of the source node requires that destination nodes (that are the recipients of traffic) monitor the level of service they are receiving. Unfortunately, from the perspective of a destination node's costs, monitoring is an expensive activity since it requires significant power-consumption in hardware and software-level auditing. Thus, the source node faces a decision regarding the extent of its cooperativeness versus selfishness; simultaneously, the destination node faces a decision regarding the extent to which it monitors the service it is receiving from the source. These competing interests and the decisions that stem from them must be cast in Bayesian game-theoretic terms in order to find the Nash equilibrium point that guarantees the optimal extent of cooperativeness by the source node, and the optimal monitoring rate of the destination node. Our game-theoretic formulation is based on a pricing model wherein each destination node pays some amount of "virtual money" (based on its budget) to the source node, in order to ensure a reliable connection. To be concrete, we consider virtual money to be implemented as a finite set of tokens that are available to the network economy. The money is used by the source node to "buy" links connecting it to the destination. We assume that the source node controls the intermediate nodes by instructing them establish pair-wise links between them, based on QoS parameters it selects. We follow the authors in [10] who implemented this by making the source node offer a payment to every node along the path for every packet it forwards towards the destination. The costs of the individual intermediate links are a function of their physical channel attributes, e.g. the length of the RF links, and weather conditions affecting FSO links, etc.

In such a system, we anticipate two kinds of source nodes will arise:

- *Cooperative* source nodes that route over the highest reliability channel that can be purchased for the money offered by the destination.
- *Selfish* source nodes that seek to maximize their own profit by routing over less reliable links (that what could have been purchased for the price offered by the destination).

In hybrid RF/FSO networks, the *Selfishness Problem* arises because the source can exhibit selfishness in several distinct ways:

1) It can transmit over RF channel instead of the FSO channel although the FSO channel is cheaper, or vice versa (depending on the channel conditions).
2) It can change the FSO beam width.
3) It can reduce transmission power of FSO or RF channels.

III. SINGLE-STAGE BAYESIAN GAME STRUCTURE

We begin by describing a single stage of our two-player Bayesian game. Then, in the next section we will extend the model to repeated solutions for a multi-stage game model.

Formally, a hybrid RF/FSO network is modeled as directed graph *G(V, E)* where *V* being the set of nodes, and *E* representing the FSO and RF links. There is a link $e^F = (v_i^F, v_j^F) \in E$ and $e^R = (v_i^R, v_j^R) \in E$, where e^F is the FSO link and e^R is the RF link. Each link in *E* has the following parameters associated with it:

- A link cost parameter C, which represents the communication set up cost.
- A reliability parameter $R\ (0 \le R \le 1)$ which represents channel availability and stability. Based on this value, the source offers the highest reliability ($\overline{R} \le R$) it can provide for the payment G it receives from the destination. If the source is selfish, however, it might cheat and offers a low reliability ($R < \overline{R}$).
- A monitoring cost C_m which represents how much it will cost the destination to monitor this link

The single-stage game can be modeled such that the destination node has some uncertainty about the source node's type:

$$G = (N, I, < A_i, u_i, \theta_i, \gamma_i >_{i \in I}, \rho)$$

- N: Natural player

978-1-4244-4148-8/09/$25.00 ©2009

- I: Set of *2* players. Player *1* is the source node. Player 2 is the destination node.
- A_i: Action space for player *i*. $A_1 = \{\overline{R}, \underline{R}\}$ $A_{2=}\{\text{Monitor, Not Monitor}\}$
- u_i: Payoff function for player *i*.
- θ_i: Type profile space for player *i*. Player *1* has private information about its type denoted by $\theta_1 = \{\text{Selfish, Cooperative}\}$. Player 2 is a singleton $\theta_2 = \{\text{destination}\}$which is common knowledge.
- $\gamma_i \subseteq A_i x\, \theta_i$Defines the available actions for player *i* of some type in θ_i.
- ρ: Defines the probability with which Nature draws the type profile of player 1 being cooperative. ρ is a common prior. Practically, initial belief value should be specified according to the network environment.
- *p:* Defines the probability with which selfish source plays $\overline{R}$.
- *q:* Defines the probability with which destination plays monitor.

The strategies of our non-zero sum game are presented in the following matrices; we see that the cooperative player adopts a pure strategy, while the selfish source and destination adopt mixed strategies whenever no pure game exists.

Cooperative Player $[\rho]$

	M[q]	NM$[1-q]$
$\overline{R}$	α_1, β_1	α_1, β_2

Non-cooperative player $[1-\rho]$

	M[q]	NM$[1-q]$
$\overline{R}$[p]	α_1, β_1	α_1, β_2
$\underline{R}[1-p]$	α_2, β_3	α_3, β_4

Where:
$\alpha_1 = G - \bar{R}C$
$\beta_1 = \overline{R}W - G - Cm$
$\beta_2 = \overline{R}W - G$
$\alpha_2 = G - \underline{R}\,(C) - (\overline{R} - \underline{R})H$
$\beta_3 = \underline{R}W - G - Cm + (\overline{R} - \underline{R})H$
$\alpha_3 = G - \underline{R}\,C$
$\beta_4 = \underline{R}W - G$
W: Destination gain of creating connection
G: Virtual currency gain the source receives from destination
H: Cheating penalty

To calculate the expected value of the game for each player, we split the non-cooperative player's payoff matrix into A and B for the source player and destination player respectively.

$A = \begin{bmatrix} \alpha_1 & \alpha_1 \\ \alpha_2 & \alpha_3 \end{bmatrix}$ is the selfish source node's payoff matrix, while the destination payoff matrix if source is selfish is given by: $B = \begin{bmatrix} \beta_1 & \beta_2 \\ \beta_3 & \beta_4 \end{bmatrix}$. Combining, we see that the expected payoff to each player is given by:

$$U_{\{src=cooperative\}} = \alpha_1$$

$$U_{\{src=selfish\}} = \sum_{i=1}^{2}\sum_{j=1}^{2} p_i q_j a_{ij}$$

$$U_{dst} = (1-\rho)\sum_{i=1}^{2}\sum_{j=1}^{2} p_i q_j b_{ij} + \rho(q_1\beta_1 + q_2\beta_2)$$

Where:
$q_1 = q \; and \; q2 = 1 - q$
$p_1 = p \; and \; p2 = 1 - p$

Bayesian Nash Equilibrium

Our game has pure strategy Nash equilibrium if any of the following conditions is satisfied:

1) When $C_m > (\overline{R} - \underline{R})H$, destination node plays not monitor (NM), selfish source node plays $\underline{R}$, and cooperative plays $\overline{R}$.
2) When $U_{dst}(\text{Not Monitor}) > U_{dst}(\text{Monitor})$ in pure strategy. This happens when $\rho > \frac{-Cm}{-Cm+(\overline{R}-\underline{R})H} + 1$. In this configuration, destination plays *NM*, selfish source best response is to play $\underline{R}$.

If neither of the conditions (1) or (2) met, we need to adopt a mixed-strategy, in which the selfish source node and destination node choose a probability distribution over possible actions. To calculate the mixed Bayesian Nash Equilibrium point (*p,q*), we used the payoff-equating method. The basis of the payoff-equating method is that "when a player uses a mixed strategy in equilibrium, he must be getting the same payoff from each of the pure strategies used in the mixed strategy" [1]. Such a point guarantees that none of the players will have an incentive to deviate from the equilibrium point. Thus, we proceed by considering that the destination's expected payoffs from the pure strategies of *Monitor* and *Not Monitor* must be identical at mixed-strategy equilibrium:

$$U_{dst}(M) = U_{dst}(NM)$$

From which it follows that:

$$\rho\beta_1 + (1-\rho)(p\beta_1 + (1-p)\beta_3) = \rho\beta_2 + (1-\rho)(p\beta_2 + (1-p)\beta_4)$$

978-1-4244-4148-8/09/$25.00 ©2009

$$p = \frac{\rho(\beta_1 - \beta_2 - \beta_3 + \beta_4) + (\beta_3 - \beta_4)}{\rho(\beta_1 - \beta_2 - \beta_3 + \beta_4) - (\beta_1 - \beta_2 - \beta_3 + \beta_4)}$$

Likewise, at mixed-strategy equilibrium, the selfish source's payoffs must be equal (for cooperating versus acting selfishly):

$$U_{\{src\}}(\overline{R}) = U_{\{src\}}(\underline{R})$$

From which it follows that:

$$q\alpha_1 + (1-q)\alpha_1 = q\alpha_2 + (1-q)\alpha_3$$

$$q = \frac{\alpha_3 - \alpha_1}{\alpha_3 - \alpha_2}$$

In the next section, we extend our proposed solution to handle multiple-stage game.

IV. MULTI-STAGE GAME

We would like to model the multi-stage game as infinite repeated game. Unfortunately the concept of subgame perfectness is not applicable in dynamic games with incomplete information, since the subgames must contain complete information set—an assumption that fails to hold in Bayesian Games. To deal with this difficulty, Kreps & Wilson introduced the approach of Perfect Bayesian Equilibrium (PBE) [8, 9] that refines the equilibrium concept in order to eliminate implausible equilibrium in dynamic games. PBE operates by starting with a prior belief common to all players and makes the moves at decision nodes based on a singleton information set. In *2*x*2* games, PBE can be any or all of the following [7]:

- *Pooling Equilibrium*: When the types of player *1* play same strategy. In this case no updating is possible for player *2*.
- *Separating Equilibrium*: When the types of player *1* play different strategies that makes the updating process for player *2* perfect.
- *Semi-separating Equilibrium*: One type of Player *1* plays a pure strategy while the other type plays a mixed strategy that makes the update process for Player *2* imperfect.

We refer the reader to [7, 8, 9] for more details on PBE. In what follows, we apply PBE to analyze the multi-stage extension of our game.

Multi-stage Game Structure

Our game is modeled as a semi-separating equilibrium where source player θ_1 mixes $\{\overline{R}, \underline{R}\}$ if selfish, while on the other hand, the cooperative player plays pure strategy $\overline{R}$ exclusively. We let the first stage be *k=1*and the last stage be *T* where *T* can be ∞.

We'll refer to the action of source player *i* against destination player *j* in stage *k* as a binary value $a_i^j(k)$. $a_i^j(k) = 0$ if the source action is $\overline{R}$ and equals *1* if the source action is $\underline{R}$. Every destination node *j* will store a history profile $h_i^j(k)$ to be able to condition the source players' stage-game action choices in later periods upon actions taken earlier. $h_i^j(k) = (a_i^j(1), a_i^j(2), \ldots, a_i^j(T))$

The strategy for source player at each stage *k* is:

$$\sigma_1(k) = \begin{cases} \overline{R} & if\ cooperative \\ \underline{R} \quad if\ selfish\ and\ \rho > \dfrac{-Cm}{-Cm + (\overline{R} - \underline{R})H} + 1 & \\ p_k^*(\underline{R}) + (1 - p_k^*)(\overline{R}), & otherwise \end{cases}$$

The best response of the destination player is at each stage *k*:

$$\sigma_2(k) = \begin{cases} \text{Not Monitor} & if\ \rho > \dfrac{-Cm}{-Cm + (\overline{R} - \underline{R})H} + 1 \\ q_k^*\text{M} + (1 - q_k^*)\text{NM} & \text{, otherwise} \end{cases}$$

In the first stage (*k=1*), the nature draws the type of the player using prior probability $\rho_i^j(1)$, provided based on the environment nature. After the first stage, the belief of node *i* about node *j* being cooperative is updated at each stage *k+1* according to Bayes' rule where:

$$\rho_i^j(k+1) = \begin{cases} \dfrac{P_k(\overline{R}|\varphi_2)\mathrm{P_k}(\varphi_2)}{P_k(\overline{R}|\varphi_1)\mathrm{P}(\varphi_1) + P_k(\overline{R}|\varphi_2)\mathrm{P}(\varphi_2)}, & if\ observed\ action\ is\ \overline{R} \\ \varepsilon & ,\ if\ observed\ action\ is\ \underline{R} \end{cases}$$

Where

- φ_1: Selfish source player
- φ_2: Cooperative source player
- $\rho_i^j(k+1)$*:* The probability with which Nature draws the type profile of player 1 being cooperative in stage *k+1*.
- $P_k(\overline{R}|\varphi_2)$*:* The probability of observing $\overline{\mathrm{R}}$ at stage *k* given that the source type is cooperative (φ_2)
- $\mathrm{P_k}(\overline{\mathrm{R}}|\varphi_1)$: The probability of observing $\overline{\mathrm{R}}$ at stage *k* given that the source type is selfish (φ_1)
- $\mathrm{P_k}(\varphi_2)$: The probability of the source type being cooperative at stage *k* which equals $\rho_i^j(k)$:
- $\mathrm{P_k}(\varphi_1)$: The probability of the source type being selfish at stage *k* which equals $1 - \rho_i^j(k)$*:*
- ε: Variable used to set ρ_i^j if $\underline{\mathrm{R}}$ is observed. The value of this variable depends on the network condition and how strict the destination is.

978-1-4244-4148-8/09/$25.00 ©2009

Observing $\underline{R}$ doesn't mean that the source type is selfish all of the time. This might happen because of a technical mistake from a cooperative node, due to a weather condition, or any possible error in the network. Therefore, sitting the value of ε is a design issue that destination and source nodes need to agree on based on the network environment. Further, we emphasize that all game theory parameters must be specified in the service level agreement (SLA). For example, the cheating penalty as we see in the numerical result section is a critical factor in the game that destination node can use to reduce channel monitoring. However, both the source and destination nodes must define the value of this parameter. Not surprisingly, we expect that in negotiating the SLA, the source node will try to minimize cheating penalty while the destination node will try to maximize the cheating penalty. Figure 1 demonstrates a flow chart of our repeated multi-stage game.

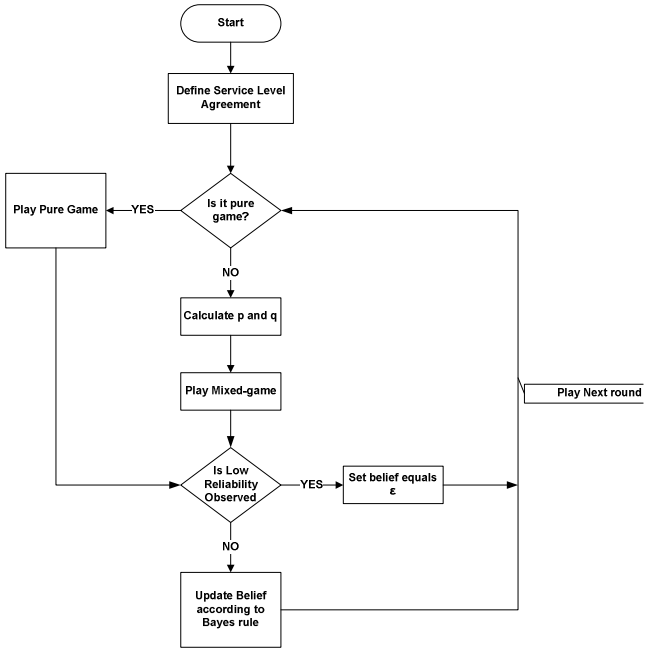

Figure 1: Flow chart of the repeated multi-stage game

We assume in our game model that:

- The route between source and destination node is given.
- The service level on each link of the path between source and destination nodes is agreed upon. Any deviation that involves providing less reliable channel is considered cheating by the destination.
- The behavior of each node is not uniform against all other nodes. For example, node *i* can be a cooperative node when it communicates with node *j*, while behaving in a selfish way when it communicates with node *k*.

Perfect Bayesian Equilibrium Proof

To be able to reach PBE our model must satisfy the following conditions:

1) Each player at each of its information sets must have beliefs about the node that it is located at.
2) The action of the player at each stage of the game must be the best response according to Nash Equilibrium.
3) The beliefs at any reachable node (on-the-path) must be determined according to Bayes' rule.
4) The beliefs at any unreachable node (off-the-path) must be determined according to Bayes' rule whenever it's possible.

Our proposed model guarantees that the game satisfies the PBE condition:

- Condition *1* is trivial since we assign a single probability on each node.
- Condition *2* is satisfied since we update the beliefs according to Bayes' rule and we provide the best response during each stage according to Nash equilibrium.
- Condition *3* and *4* are satisfied since the information sets are reached with positive probability based on the update belief equation that is using Byes rule.

V. NUMERICAL RESULTS

In our experiments, we assume that high reliability $\overline{R}$=0.7, low reliability $\underline{R}$=0.1, the link communication set up cost was taken as *C=2* tokens, destination gain of receiving the traffic is *W=15* tokens, and source gain of forwarding the traffic *G=5* tokens. The values of the initial belief ρ, cheating penalty *H*, and monitoring cost C_m are varied depending on the type of experiment.

Figure 2 illustrates the number of stages that are required for the posterior beliefs to converge to *1*. In this experiment, the type of the player is cooperative, $\rho = 0.3$, *H=5*, and $C_m = 1$. As shown in the figure it took the destination 7 stages to detect the type of the player.

Figure 3 illustrates the effect of resetting the posterior belief on the probability of forwarding using low reliability $\underline{R}$. We define the resetting variable as ε. In this experiment, the type of the player is selfish player, *H=5, Cm=1*. The top curve represents the probability of traffic forwarding using $\underline{R}$ when ε is a high value =0.1. While the other curve represents the probability of traffic forwarding using $\underline{R}$ when ε is a very low =0.001. We can observe from this experiment that after destination node detected $\underline{R}$, the selfish player was able to converge again and started forwarding using $\underline{R}$ when ε is high. On the other hand, using very small ε forced the selfish player to cooperate after observing its selfishness behavior. However, using very low ε is not necessarily a practical solution to reduce the selfish forwarding probability because observing low reliability can occur due to an error in the instantaneous measurements on the destination side. Therefore, defining ε

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

should be a design issue that extremely depends on the environment and the service level agreement between source and destination. The other observation we found from this experiment is that the probability of selfish player forwarding using low reliability increases at each stage. We expect this behavior since the destination node starts with a belief probability=*0.7* about the source player being selfish. As long as a destination is observing high reliability, its confidence that this player being selfish decreases, therefore playing low reliability increases to meet the Nash equilibrium point.

Figure 4 illustrates the impact of increasing the selfishness penalty *(H)* on the probability of traffic forwarding using $\underline{R}$ by the source and the probability of monitoring by the destination. Figure 8 shows that increasing H reduces the probability of traffic forwarding using $\underline{R}$ tremendously by the selfish source. On the other hand, it reduces the channel monitoring probability on the destination node. We can conclude that destination node can reduce the monitoring cost of the channel by having a very large selfishness penalty value. In practice, this can't be achieved because the source node will not accept an agreement of paying high cost as a penalty. However, destination node should try to push this value to the most extend in order to reduce the monitoring cost.

In the last experiment, Figure 5 illustrates the impact of increasing the link monitoring cost parameter on the posterior belief convergence. Having high monitoring cost converges the posterior belief in very few stages because the game will be switched into a pure game when $C_m > (\overline{R} - \underline{R})H$.

VI. Conclusion and Future Work

We developed a novel Bayesian game theoretical model that guarantees cooperative behavior in Hybrid RF/FSO networks. A Perfect Bayesian Equilibrium is applied in the multi-stage setting, extending the single-stage Nash Equilibrium model. Our numerical results explicate the impact of game parameters on the Nash equilibrium point and the convergence of posterior beliefs regarding the source player. We determine that cheating penalty is one of the most significant parameters that destination node can use to reduce the monitoring probability.

In our future work in the area of Hybrid RF/FSO networks, we are looking to provide a large-scale solution for the topology control problem by extending our model provided in [13].

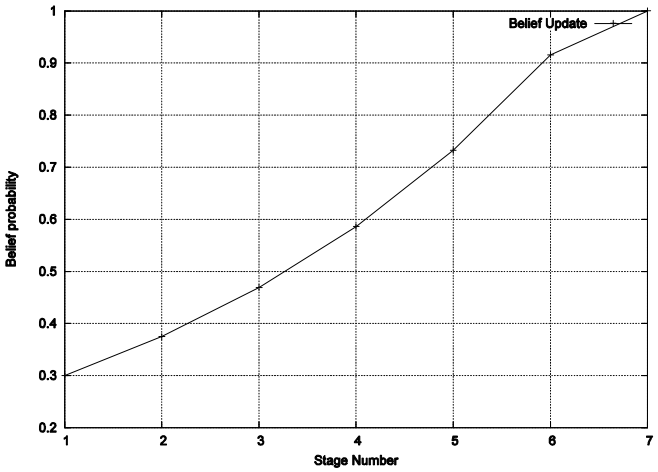

Figure 2: Posterior beliefs convergence vs. number of stages

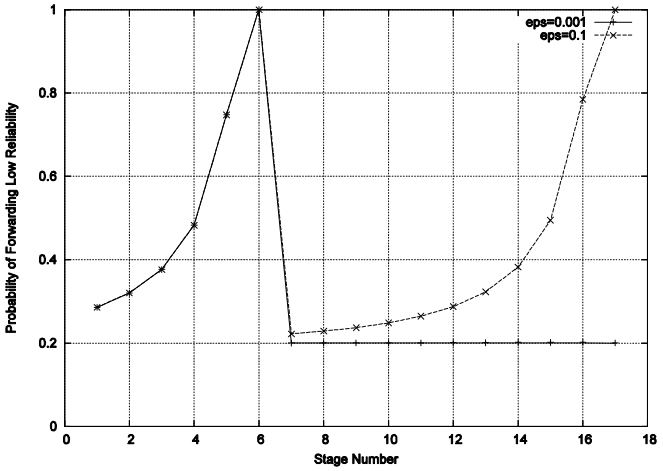

Figure 3: Probability of forwarding using low reliability ($\underline{R}$) vs. stage number using ε=0.001 and $\varepsilon = 0.1$

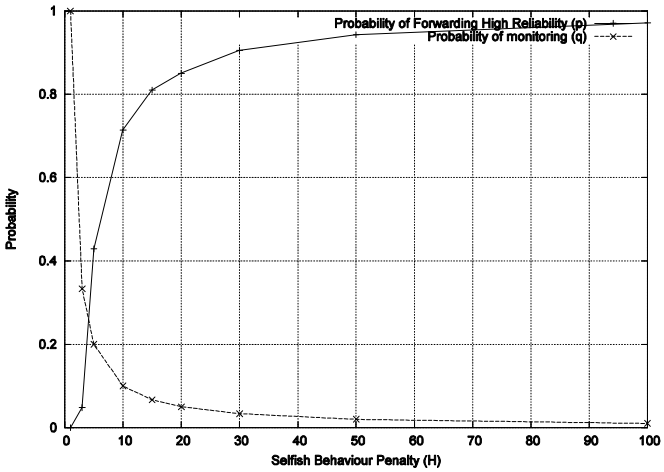

Figure 4: Probability of monitoring by destination node and probability of forwarding using high reliability ($\overline{R}$) vs. stage number

978-1-4244-4148-8/09/$25.00 ©2009

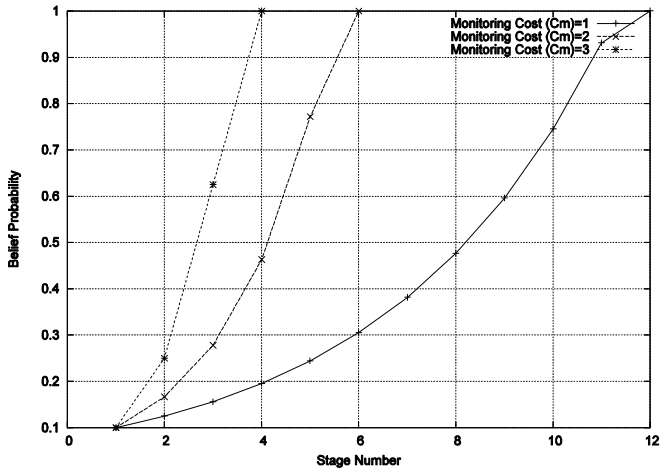

Figure 5: The effect of increasing the link monitoring cost C_m on the posterior belief convergence.

REFERENCES

[1] E. Rasmusen "Games and Information an introduction to game theory". Blackwell Pubs, 2007. 4th Edition

[2] A. Kashyap, K. Lee, M. Kalantari, S. Khuller and M. Shayman, Integrated topology control and routing in wireless optical mesh networks. *Computer Networks Journal,* Vol. 51, October 2007, 4237-4251.

[3] J. Juarez, A. Dwivedi, A. Hammons,S. Jones, V. "Weerackody, R. Nichols. Free Space Optical Communications for Next-Generation Military Networks," IEEE Commun Mag, November 2006.

[4] J. Akella, Chang. Liu, D. Partyka, M. Yuksel, S. Kalyanaraman, P. Dutta. "Building blocks for mobile free-space-optical networks," Second IFIP International Conference on Wireless and Optical Communications Networks (WOCN), 2005.

[5] J. Derenick, C. Thorne, J. Spletzer. "On the deployment of a hybrid freespace optic/radio frequency (FSO/RF) mobile ad hoc network," IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2005.

[6] A. Kashyap, A. Rawat, M. Shayman, "Integrated Backup Topology Control and Routing of Obscured Traffic in Hybrid RF/FSO Networks," IEEE Globecom 2006.

[7] D. Fudenberg and J. Tirole. "Game Theory". The MIT Press, Cambridge, Massachusetts, 1991.

[8] D. Kreps and R. Wilson. "Reputation and Imperfect Information," Journal of Economic Theory," vol. 27 no. 2, pp. 253-279, 1982.

[9] D. Kreps and R. Wilson. "Sequential Equilibria, " Econometrica, vol. 50 no. 4 pp. 863-894, 1982.

[10] H. Liu and B. Krishnamachar. "A Price-based Reliable Routing Game in Wireless Networks," workshop on Game theory for communications and networks (Game Nets), 2006.

[11] Y. Liu , C. Comaniciu , and Hong Man. "A Bayesian game approach for intrusion detection in wireless ad hoc networks," workshop on Game theory for communications and networks, 2006.

[12] P. Nurmi. "Modeling energy constrained routing in selfish ad hoc networks," workshop on Game theory for communications and networks, 2006.

[13] O. Awwad, A. Alfuqaha, D. Kountanis, D. Benhaddou, and A. Rayes. "Topology Control using Adaptive Power Control and Beam-Width in Hybrid RF/FSO MANETs," Chinacom, 2008

978-1-4244-4148-8/09/$25.00 ©2009