This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2008 proceedings.

Coordination and Selfishness in Attacks on Visual Sensor Networks

Alexandra Czarlinska and Deepa Kundur
Department of Electrical and Computer Engineering, Texas A&M University
Tel: (979) 862-8684, Fax: (979) 862-4630, {czlinska, deepa}@ece.tamu.edu

***Abstract*— Event-driven visual sensor networks consist of collaborating camera nodes and scalar sensors which aid in the detection of events of interest in the environment. This collaboration is significant since the camera nodes generally utilize lightweight image processing in order to determine if a frame is relevant to the given application. The reliability of the supporting scalar sensor however may be compromised by an actuation attack which perturbs the sensor's measurements. In this work we examine the achievable actuation of hostile nodes that are not globally coordinated and that may be selfish or untrustworthy in their preferences. We compare our findings with existing research which assumes that all the hostile nodes are coordinated to actuate with the same parameter. We determine that given certain conditions, local optimization may actually result in a stronger stealthy attack than the global coordination case.**

***Index Terms*— Visual Sensor Networks (VSNs), Attack Coordination, Event-Detection, Sensor Network Security, Game Theory**

I. Introduction

Networks of wireless miniature cameras referred to as visual sensor networks (VSNs) are envisioned for a variety of applications such as distributed surveillance [1], [2]. These visual networks inherit many of the issues present in sensor networks, such as limited battery life, limited storage and processing abilities. Indeed the nature of the rich visual data collected by the camera nodes exacerbates many of these problems. In the case of wireless nodes deployed throughout an environment, the acquired image frames must be processed efficiently by the camera nodes and transmitted to a cluster head in a way that minimizes the energy required for transmission. Among the growing body of literature addressing these problems, there is a particular interest in solutions that exploit collaboration between the nodes and the spatial and temporal correlation among the nodes' data [3], [4], [5].

One particular type of collaborative approach is the *event-driven* VSN paradigm where camera nodes receive information from neighboring scalar sensors that detect motion or collect other parameters regarding the environment such as temperature or sound [6]. The information received from the scalar sensors can be utilized by the camera nodes for a variety of purposes, such as to determine if an event of interest occurred in the environment. This approach is appealing in that it enables frame selection to occur at the source instead of transmitting all the acquired frames to the cluster head for processing and selection. The role of the scalar sensors in this scenario is to supplement or even replace potentially costly image processing of frames at the camera nodes in order to determine their relevance to the surveillance task [6]. Figure 1 depicts one possible scenario where each camera node receives decision support from a scalar sensor before transmitting frames to the cluster head.

In comparison with other approaches, the event-driven scalar-assisted approach may be considered a "push" approach in that the visual nodes transmit selected frames to the cluster-head when such frames become available. In contrast, in a "pull" approach, the cluster-head advertises what features are of interest in the application [7]. The feature advertising thus pulls data that matches the search from the visual nodes. The appeal of the push-based approach in the limited-resource regime of VSNs is that the camera nodes are able to "rid" themselves of the collected frames in a timely manner. Thus the burden of visual data handling is passed onto the cluster-head which may have greater resources at its disposal. In contrast, in the pull-based approach the visual nodes may be required to store frames during a time interval until they receive a request or until the validity of the frames expires (in which case the frames are discarded).

In further comparison of the two approaches, we also note the significance of the *definition* of an event in the push based approach. In the pull based system, the definition of an event of interest is issued by the cluster head and tends to refer to specific features that are application dependent. In the push based system however, the nodes may need to decide whether a frame is relevant without a specific request from the cluster head. In such cases the event definition is usually based on the detection of a specified amount of motion and thus benefits from collaboration with scalar sensors.

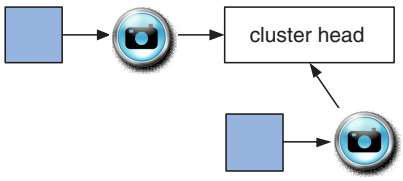

Fig. 1. Visual sensor network consisting of scalar sensors and camera nodes.

To realize the potential of event-driven VSNs, the reliability of the scalar sensors must be assured. This is particularly true in VSNs where the camera nodes utilize a lightweight image processing algorithm for event detection which may not always yield a suitable probability of detection and false alarm [6]. It is known however that scalar sensors are susceptible to a

1525-3511/08/$25.00 ©2008 IEEE

variety of attacks as well as occasional errors due to harsh environmental conditions. In particular, attacks that occur at the physical level of sensing cannot be prevented using cryptographic means [8]. Among this class of attacks we consider the actuation attack which is generally perpetrated by a foreign hostile network (i.e. a network not under the control of the legitimate scalar and camera nodes). The foreign hostile nodes are dispersed throughout the environment and may perturb the measurements collected by the scalar sensors away from their true readings. This may cause the scalar sensors to report an event when no event occurred and vice versa. Figure 2a) depicts a possible scenario where n hostile nodes are deployed in the environment of the legitimate scalar sensors and where they attack with probability q.

A. Focus & Contribution

In [8] and [6] the effects of an actuation attack are examined via game theoretic analysis for the case where all n hostile nodes are coordinated to employ the same value of attack probability q. It is shown that suitable values of q exist such that the attack remains stealthy (i.e. it is not detected by the cluster head). In this work we seek to understand how coordination and trust levels among the hostile nodes in their selection of the parameter q affect the resulting strength of the attack (the average expected number of affected scalar sensors) and the attack's stealth. Specifically we employ Nash equilibria to examine:

1. The case where each hostile node i chooses its parameter q_i independently from the other nodes based on a maximization of its utility function.
2. The case where each hostile node i chooses its parameter q_i independently from the other nodes, but where it's utility function may not be the same as that of other nodes. Specifically, we allow each node to exercise preferences based on its trust level for the other hostile nodes participating in the attack.

In both cases we wish to determine the resulting optimal selection of the parameter q_i and to compare it to the case where $q_i = q$ for all i as in [8] and [6].

II. Background & Recent Advances

A. Visual Sensor Network Approaches

We briefly overview other approaches to efficient visual data handling in VSNs, partly for completeness and partly to place in perspective the relative significance of visual-scalar collaboration. The various approaches may be broadly classified into the following categories:

1. Data correlation and node collaboration-based techniques:
   a. Signal processing techniques for the elimination of redundant data among the nodes based on spatial and temporal overlap in the cameras' field of view. This approach is particularly attractive in dense deployments and multi-hop environments where cameras likely witness correlated events [9], [3].
   b. Information and coding theoretic exploitation of spatial data correlation utilized for distributed image compression, such as via Wyner-Ziv coding [10].
   c. Event-driven approach based on collaboration between lightweight image processing nodes and scalar sensor decisions regarding the presence or absence of an event. This approach relies on a variety of toolsets such as game theory and image processing. [11].
2. Bandwidth-based techniques:
   a. Bandwidth augmentation such as through the use of free-space optical communications in lieu of radio wireless communications [12].
   b. Allocation of existing bandwidth with particular focus on fair and efficient allocation among competing nodes which gather visual data of varying surveillance significance [13].

B. Recent Game Theoretic Results on Actuation

An actuation attack is a type of attack that is perpetrated by a hostile foreign network (i.e. a network comprised of nodes that are not under the control of the legitimate scalar sensor network) and which disrupts sensor readings away from their true values [8]. For the purpose of generality and tractability, the attack is modeled by considering its *effect* on the sensors' *decisions* about the presence or absence of an event. Under no attack, each sensor i makes a binary yes/no decision X_i where the realization $x_i = 1$ denotes "event present" and where X_i has Bernoulli distribution $Bern(p)$. The *effect* of the attack is modeled as flipping a decision from 0 to 1 and vice versa with Bernoulli probability q, where each hostile node employs *the same* value of q. Specifically, the realization $y_i = 1$ represents a hostile node i actuating and $y_i = 0$ represents no actuation. The overall effect is that a scalar node i makes decision z_i where $z_i = x_i \oplus y_i$.

The hostile network wishes to affect the decisions of the scalar sensors but to remain stealthy in the attack (i.e. undetected by the cluster head). To perform attack detection, each scalar sensor sends its detection decision not only to its corresponding camera node but also to the cluster head. The cluster head thus has at its disposal the data vector $\mathbf{x} = [x_1 ... x_n]$ and computes its weight $w(\mathbf{x})$ which is a sufficient statistic for attack detection (such as using an optimal Neyman-Pearson detector). To remain stealthy, the attacking network must thus select the parameter q such that $|w(\mathbf{Z}) - w(\mathbf{X})| \leq \epsilon$ for some relaxation factor ϵ. That is, the weight of the actuated data must lie sufficiently close to the expected weight for an attack to remain undetected. We now summarize the salient results obtained from a Nash game theory analysis of this attack under the stated assumptions.

1. All hostile nodes utilize the same value of parameter q. The optimal value of this parameter depends on parameters p (probability of event) and n (network size).
2. In order to maintain stealth, the optimal value of q is typically small, that is, $0 < q \ll 0.5$.
3. The optimal value of q tends to increase with decreasing network size n and increase for p close to 0.5 (common events). In terms of the effect of p, the case where $p = 0.5$

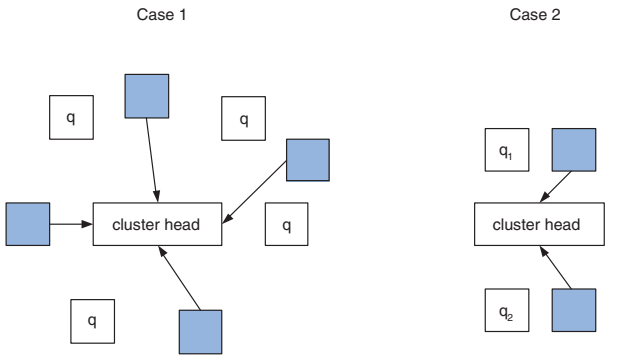

Fig. 2. (a) Case 1: n hostile nodes are deployed against n legitimate scalar sensors. Each hostile node actuates with probability q. (b) Case 2: $n = 2$ nodes. Each hostile nodes actuates with varying q.

is a best case scenario for the attacker and a worst case scenario for the legitimate scalar sensors.

III. Coordination & Optimal Attack Strategies

In this work we wish to examine the case where the hostile nodes do not choose a common q value, but rather choose this parameter independently based on their local utility functions. Thus we wish to understand the role that coordination plays in achieving a strong and stealthy attack.

We consider the scenario where $n = 2$ hostile nodes are actuating against two legitimate scalar sensors as shown in Figure 2b). As in [8], we assume that the case where a legitimate scalar sensor i witnesses an event of interest when actuation is absent is denoted by $x_i = 1$, and that this event occurs with Bernoulli probability p such that $Pr(X_i = 1) = p$. Conversely $x_i = 0$ denotes the condition where no event of interest is recorded by scalar sensor node i when actuation is absent and this event carries probability $Pr(X_i = 0) = 1 - p$.

Let the action of a hostile node i be denoted by Y_i where the realization $y_i = 1$ denotes actuation and $y_i = 0$ denotes no actuation. We assume that the Bernoulli probability that a hostile node y_i actuates is given by $Pr(Y_i = 1) = q_i$. Let $\mathbf{x} = [x_1 x_2]$, $\mathbf{y} = [y_1 y_2]$ and $\mathbf{z} = [z_1 z_2]$. We examine the case where the stealth relaxation parameter is $\epsilon = 0$ (Section II-B), and thus in order to evade detection, each node i in the hostile network wishes to maximize it's utility function π_i given by Eq. 1 which depends on the parameter q_i that it chooses, as well as on the parameter q_j that the other hostile node chooses independently.

$$\pi_i(q_1, q_2) = Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} = Pr\{w(\mathbf{X}) = w(\mathbf{X} \oplus \mathbf{Y})\} \tag{1}$$

The probability of Eq. 1 can be expressed and simplified as shown in Eqs. 2 to 4. The final simplified utility function $\pi_i(q_1, q_2)$ is given by Eq. 5 which has been written to emphasize the form of the interaction between q_1 and q_2.

$$\begin{aligned} Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} &= Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 00\} \\ &\cdot Pr\{\mathbf{X} = 00\} + Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 01\} \\ &\cdot Pr\{\mathbf{X} = 01\} + Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 10\} \\ &\cdot Pr\{\mathbf{X} = 10\} + Pr\{w(\mathbf{X}) = w(\mathbf{Z}) | \mathbf{X} = 11\} \\ &\cdot Pr\{\mathbf{X} = 11\} \end{aligned} \tag{2}$$

$$\begin{aligned} Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} &= \\ Pr\{(w(Y_1) = 0 \wedge w(Y_2) = 0)\} &\cdot (1-p)^2 + \\ Pr\{(w(Y_1) = 0 \wedge w(Y_2) = 0) &\vee \\ (w(Y_1) = 1 \wedge w(Y_2) = 1)\} &\cdot 2p(1-p) + \\ Pr\{(w(Y_1) = 0 \wedge w(Y_2) = 0)\} &\cdot p^2 \end{aligned} \tag{3}$$

$$\begin{aligned} Pr\{w(\mathbf{X}) = w(\mathbf{Z})\} &= (1-q_1)(1-q_2)(1-p)^2 + \\ ((1-q_1)(1-q_2) + q_1 q_2) &\cdot 2p(1-p) + \\ (1-q_1)(1-q_2) &\cdot p^2 \end{aligned} \tag{4}$$

$$\begin{aligned} \Pi_i(q_1, q_2) &= \alpha \cdot (q_1 + q_2) + \beta_p \cdot (q_1 \cdot q_2) + \gamma \quad i = \{1, 2\} \\ \alpha &= -1 \\ \beta_p &= -2p^2 + 2p + 1 \\ \gamma &= 1 \end{aligned} \tag{5}$$

Based on the utility of Eq. 5, it can be shown that the best response $B_i(q_j)$ of node i to a strategy q_j of node j is given by Eq. 6, where T_p is a threshold point that depends on β_p from Eq. 5 (and hence on parameter p, that is, the probability of an event under no attack). The intersection(s) of the best response functions of the players (if any) provide the set of Nash equilibria of the game. It can be shown based on Eqs. 5 and 6 that there are two pure action Nash equilibria $(q_{1,N}, q_{2,N})$ for this game as given by Eq. 7, and that the resulting utility $\pi_i(q_{1,N}, q_{2,N})$ for node i at each equilibrium is given by Eq. 8.

$$\begin{aligned} B_i(q_j) = 0 \quad if \quad q_j < T_p \\ B_i(q_j) = 1 \quad if \quad q_j > T_p \\ T_p = \frac{1}{\beta_p} \\ \beta_p \in [1, 1.5] \end{aligned} \tag{6}$$

$$(q_{1,N}, q_{2,N}) = \{(0,0), (1,1)\} \tag{7}$$

$$\pi_i(0,0) = 1 \qquad \pi_i(1,1) = \beta_p - 1 \tag{8}$$

To better illustrate the interaction of the players and the consequences of the game, Figure 3(a) depicts a utility manifold $\pi_i(q_1, q_2)$ between the two hostile nodes over the entire domain of q_1 and q_2. The two Nash equilibria occur at $(q_{1,N}, q_{2,N}) = (0,0)$ and $(q_{1,N}, q_{2,N}) = (1,1)$ as predicted via Eq. 7 and as confirmed by examining the best response intersections shown in Figure 3(b). We note two salient features of this result which we will examine further:

1. When each hostile node i is permitted to choose its *own* attack parameter q_i, the possibility of a much *stronger* stealthy attack emerges. As discussed in Section II-B, the optimal attack parameter q is typically *small* (but not zero) when q is chosen globally and there are n attacking nodes. However for $n = 2$ and independent q_i's, there are two extreme optimal values of q_i; one at $q_i = 0$ and the other at $q_i = 1$ thus permitting the nodes to attack either with probability 0 or with probability 1.
2. The threshold or dividing point T_p between the two equilibria depends solely on the parameter β_p and thus

on the underlying probability of an event p which is *not* controlled by the hostile nodes.

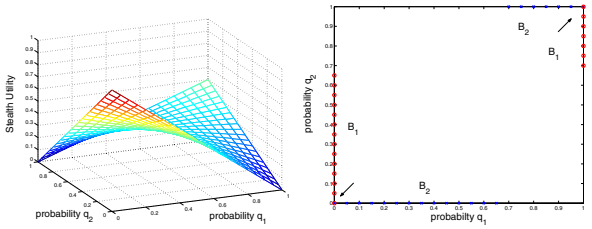

Fig. 3. (a) Utility manifold for a hostile node i versus the full set of actions q_1 and q_2 for the case where $p = 0.5$. The two Nash equilibria for this game occur at $(0, 0)$ and $(1, 1)$ and the T_p threshold is the saddle point. (b) Best response functions of nodes 1 and 2 showing the two Nash equilibria at the intersection points.

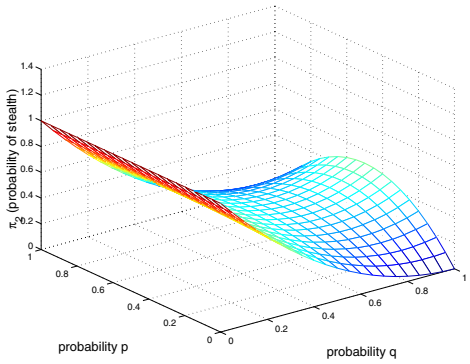

Fig. 4. Best response (optimal global value) of q is 0 for all values of p.

We now expand upon the significance of each of the above points. According to point 1, allowing each of the two nodes to pick its own local q_i value can actually lead to a *stronger* stealthy attack. However the comparison is not decisive since the global q result discussed in Section II-B and [8] applies to the case of n nodes and not specifically $n = 2$ nodes. For a more direct comparison, we note that it suffices to set $q_1 = q_2 = q$ in Eq. 4, as shown in Eq. 9.

$$\begin{aligned} Pr\{w(\mathbf{x}) = w(\mathbf{z})\} &= (1-q)^2(1-p)^2 \\ +((1-q)^2 + q^2)p(1-p) &+ 2(1-q)^2p^2 \end{aligned} \tag{9}$$

Upon simplification, the new utility function $\pi_i(p, q)$ is given by Eq. 10, where we have made explicit the dependence of the utility on the parameter p (not under the control of the hostile nodes). It can be shown that the optimal value of global attack parameter q for $n = 2$ nodes is given uniquely by $q_N = 0$ for all values of p as given in Eq. 11 and shown in the manifold of Figure 4. Although the utility achieved at this optimal global q is $\pi_i(q = 0) = 1$, it is a trivial solution where the actuation attack occurs with probability 0 (i.e. no attack is carried out, leading to stealth inherently). Thus we arrive at the interesting conclusion that local optimization (independently chosen q_i) leads to the *possibility* of a stronger stealthy attack in contrast with global optimization (a single value of q).

$$\begin{aligned} \pi_i(p, q) &= \alpha \cdot q + \beta_p \cdot q^2 + \gamma \\ \alpha &= -2 \\ \beta_p &= 1 + 2p - 2p^2 \\ \gamma &= 1 \end{aligned} \tag{10}$$

$$q_N = \{(0, 0)\}, \quad \pi_i(0, 0) = 1 \tag{11}$$

However we note that in the case of local optimization, a second equilibrium is also possible, namely the $(0, 0)$ equilibrium from Eq. 7. Furthermore according to point 2, the decision threshold T_p between these two points depends on the parameter p which is not controlled by the hostile nodes. We are thus left with the question of *how* a hostile node will select its action and which equilibrium will actually occur. If the two hostile nodes have a means of communicating, it suffices for the two nodes to agree upon a common action (i.e., either both pick $q = 0$ or both pick $q = 1$). Importantly, agreement between the two nodes may be reached by simply having one of the nodes (called the leader) announce its choice first. As shown in Figure 5(a), the second node's (the follower's) optimal action is to always *match* the action of the first node in order to maximize its utility. We note however that explicit *communication* between the nodes may be replaced in some instances by implicit *coordination*. For example, both nodes could agree a priori to choose $q = 1$ whenever they observe some event ζ in the environment, and to choose $q = 0$ otherwise.

The more interesting case however occurs when neither communication nor coordination is available to the two hostile nodes. Even if we assume that both nodes can determine the value of p (such as through extended observation) and can thus determine the threshold T_p, each node needs to know if the other node has chosen a q below or above T_p to choose its best q (Eq. 6). In the absence of such knowledge, each node if forced to *mix* between its pure optimal actions of $q = 0$ and $q = 1$ with some probability as shown in Figure 5(b). We assume that Player 1 (node 1) chooses action $q_1 = 0$ with some probability x and that it chooses $q_1 = 1$ with probability $1 - x$. Similarly, Player 2 (node 2) chooses action $q_2 = 0$ with probability y and $q_2 = 1$ with probability $1 - y$. The new utility $\pi_i(x, y)$ obtained by node i based on its mixing variable x and the mixing variable of the other node y is given by Eq. 12. It can thus be shown that a third *mixed* strategy Nash equilibrium emerges, where the optimal Nash x and y mixes are given by Eq. 13 along with the corresponding utility $\pi_i(x_N, y_N)$ at equilibrium given by Eq. 14.

$$\pi_i(x, y) = xy + (1 - x)(1 - y)(\beta_p - 1) \tag{12}$$

$$(x_N, y_N) = (\frac{\beta_p - 1}{\beta_p}, \frac{\beta_p - 1}{\beta_p}) \tag{13}$$

$$\pi_i(x_N, y_N) = \frac{\beta_p - 1}{\beta_p} \tag{14}$$

We make three key observations regarding this result. First we observe that the mixing probabilities only depend on β_p (and thus p) and do not require the nodes to know each other's actions. The second observation is that the range and maximum value of the new utility $\pi_i(x_N, y_N) \in [0, 0.5]$ is generally smaller than the range and maximum of the

previous utility $\pi_i(q_{1,N}, q_{2,N}) \in [0,1]$. Eliminating the need for coordination thus comes at the price of a decrease in the utility (i.e. stealth of the attack) and can be understood as a trade-off. Finally, the third observation regarding the new *mixed* equilibrium reveals an interpretation for the T_p threshold dividing the two pure action equilibria. We examine Eq. 5 and suppose that hostile node 1 plays with q_1 set to T_p, that is, $q_1 = 1/\beta_p$. We observe that the resulting utility π_2 for hostile node 2 is given by $\pi_2(q_1 = T_p, q_2) = 1 - 1/\beta_p$. Thus the utility of node 2 is independent of its own q_2 selection or in other words, node 2 is *indifferent* in its q_2. Furthermore, the achieved utility of $1-1/\beta_p$ is *equal to* the utility achieved at mixed equilibrium shown in Eq. 14. By the properties of mixed equilibria [14], these two observations imply that the T_p threshold (saddle point in Figure 3(a)) *is* the mixed strategy equilibrium.

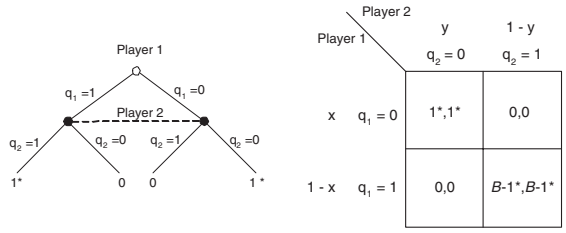

Fig. 5. (a) Player 1 is a leader with two actions and player 2 is a follower with 2 actions. The end points of the game show the obtained utility. The optimal utility is marked by a star and occurs when the follower matches the action of the leader. (b) A mixed-action game with mixing probabilities x and y. The (u_1, u_2) numbers inside each cell represent the utility of player 1 and 2 respectively.

IV. Effects of Trust & Selfishness on Coordination

As before we consider the case where $n = 2$ hostile nodes are deployed against 2 scalar sensors as shown in Figure 2(b). The utility function of each hostile node however is allowed to be non-symmetric with respect to the other due to (possibly) selfish goals and varying trust levels among the hostile nodes. The new utility functions $\tilde{\pi}_1(q_1, q_2)$ and $\tilde{\pi}_2(q_1, q_2)$ are shown in Eq. 15 where $\pi(q_1, q_2)$ is the prior stealth utility of Eq. 5. The additional $n_i q_i$ terms in the utilities represent the average expected number of scalar sensors attacked by hostile node i, and the k and m parameters indicate trust levels among the hostile nodes. Thus in the new utility, each hostile node wishes to maximize not only the stealth achieved in the attack, but also the expected number of scalar sensor nodes attacked by both hostile nodes ($n_1 q_1$ and $n_2 q_2$). The local selection of a q_i parameter by node i is however affected by its real and perceived trust levels as detailed below:

$$\begin{aligned} \tilde{\pi}_1(q_1, q_2) &= \pi(q_1, q_2) + k_{12} \cdot n_1 q_1 + k_{21} \cdot n_1 q_2 \\ \tilde{\pi}_2(q_1, q_2) &= \pi(q_1, q_2) + m_{12} \cdot n_2 q_1 + m_{21} \cdot n_2 q_2 \\ k, m \in \{-1, 0, 1\} \quad & q_1 \in [0,1] \quad q_2 \in [0,1] \end{aligned} \tag{15}$$

- k_{12} denotes the trust of hostile node 1 for hostile node 2
- k_{21} denotes the trust that hostile node 1 *believes* hostile node 2 assigns to it
- m_{21} denotes the trust of hostile node 2 for node 1
- m_{12} denotes the trust that hostile node 2 *believes* hostile node 1 assigns to it
- n_i is the number of scalar sensors that hostile node i can attack (based on actuation radius and distance). In this work we assume that $n_1 = n_2 = 1$.

As shown in Eq. 15, each parameter k or m takes on one of three possible trust levels. We utilize the convention where a level of value 1 denotes trust, a level of value 0 denotes no information (or indifference) about trust, and a level of value -1 denotes a lack of trust. Trust in the context of an actuation attack means that a hostile node i believes that the other hostile node j will select its actuation parameter q_j to achieve stealth in Eq. 5 (i.e. it will not deviate from a stealthy action to expose the hostile network).

The utility in Eq. 15 can be re-written as shown in Eq. 16 where we assume that $n_1 = n_2 = 1$. Based on Eq. 16 it can be shown that the best response $B_i(q_j)$ of node i to node j's choice of q_j is given by Eq. 17 where the threshold is now different for each hostile node as given by Eq. 18. Interestingly we observe that the new thresholds $\tilde{T}_i$ not only depend on the value of β_p, but also on the trust that a hostile node places in the other hostile node.

$$\begin{aligned} \tilde{\pi}_1(q_1, q_2) &= (k_{12} - 1) \cdot q_1 + (k_{21} - 1) \cdot q_2 + \beta_p q_1 q_2 + 1 \\ \tilde{\pi}_2(q_1, q_2) &= (m_{12} - 1) \cdot q_1 + (m_{21} - 1) \cdot q_2 + \beta_p q_1 q_2 + 1 \end{aligned} \tag{16}$$

$$\begin{aligned} B_i(q_j) &= 0 \quad if \quad q_j < \tilde{T}_i \\ B_i(q_j) &= 1 \quad if \quad q_j > \tilde{T}_i \end{aligned} \tag{17}$$

$$\begin{aligned} \tilde{T}_i &= \frac{1 - k_{12}}{\beta_p} \quad if \quad i = 1 \\ \tilde{T}_i &= \frac{1 - m_{21}}{\beta_p} \quad if \quad i = 2 \\ & \beta_p \in [1, 1.5] \end{aligned} \tag{18}$$

$$(q_{1,N}, q_{2,N}) = \{(0,0), (1,1)\} \tag{19}$$

The pure action Nash equilibria of this game are given by Eq. 19 and match the equilibria obtained earlier in Eq. 7. The best response functions leading to these equilibria however now exhibit interesting properties which we now summarize in the following points.

1. Assume that node 1 selects $q_1 = 0$ as its action. Node 2's resulting utility $\tilde{\pi}_2$ becomes $\tilde{\pi}_2(q_1 = 0, q_2) = 1 + q_2 \cdot (m_{21} - 1)$ from Eq. 16. We note that the $(m_{21} - 1)$ term can never be strictly positive since $m_{21} \in \{-1, 0, 1\}$. Therefore the best response of node 2 is to always play with $q_2 = 0$, *regardless* of the trust level m_{21} (strictly speaking, when $m_{21} = 1$, node 2 is indifferent among it's choice of q_2). This result agrees with the reasoning that if one node chooses not to actuate, the other node should also choose not to actuate in order to avoid detection.
2. Assume that node 1 selects $q_1 = 1$ as its action. Node $2's$ utility is thus $\tilde{\pi}_2(q_1 = 1, q_2) = m_{12} + q_2 \cdot (\beta_p + m_{21} - 1)$ based on Eq. 16. For $q_2 = 1$ to be a best response of node 2 (leading to the $(q_1, q_2) = (1,1)$ equilibrium), $(\beta_p + m_{21} - 1) > 0$. Specifically:

a. When $m_{21} = 1$ (trust), this condition is always true irrespective of the value of $\beta_p \in [1, 1.5]$. Therefore node 2 chooses $q_2 = 1$.

b. When $m_{21} = 0$ (no information), this condition is true when $\beta_p > 1$. Therefore node 2 must use β_p to make a decision. If $\beta_p = 1$, node 2 is indifferent among its possible q_2 selections.

c. When $m_{21} = -1$ (no trust), this condition can never be true (it would require $\beta_p > 2$). Therefore node 2 chooses the action $q_2 = 0$ and the equilibrium degenerates to the "safe" $(q_1, q_2) = (0, 0)$ equilibrium.

Finally we note that the new utilities obtained at each equilibrium are given by Eq. 20. Importantly, the utility at the $(1, 1)$ equilibrium is now affected by the mutual trust of the nodes. Furthermore, the maximum of the utility is no longer 1 as in Eq. 5 since the utility of Eq. 15 measure both stealth and the average expected number of affected scalar sensor nodes. To visualize the effect of this new utility, Figure 6 shows a sample case where each node trusts the other node but is unsure whether that trust is reciprocated ($k_{12} = 1$, $k_{21} = 0$, $m_{12} = 0$, $m_{21} = 1$). We observe that this case still results in two pure Nash equilibria as shown in Figure 6(b) although the utilities of the two nodes are no longer identical as shown Figure 6(a). In contrast, Figure 7 depicts the case where one node exhibits full trust (and believes that this trust is reciprocated), while the other node does *not* exhibit trust and does not believe that the trust is reciprocated. This situation forces a single equilibrium, namely the $(q_{1,N}, q_{2,N}) = (0, 0)$ "safe" equilibrium where no actuation actually occurs in order to maintain stealth.

Thus in this work we have shown that allowing the hostile nodes to optimize locally (independent q_is) may actually allow for a *stronger* stealthy attack under certain conditions, and that incorporating trust levels into the local optimization helps the hostile nodes to maintain stealth by choosing correct actuation levels.

$$\pi_i(0,0) = 1 \qquad \pi_i(1,1) = \beta_p - 1 + m_{12} + m_{21} \tag{20}$$

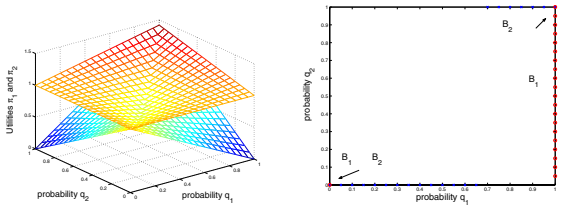

Fig. 6. Game where $k_{12} = 1$, $k_{21} = 0$, $m_{12} = 0$, $m_{21} = 1$. (a) Resulting utility manifolds for both players from Eq. 16. (b) Best response functions showing two Nash pure action equilibria.

V. Conclusions

Event-driven visual sensor networks (VSNs) are an attractive paradigm for efficient handling of rich visual data collected by nodes in applications such as surveillance. The lightweight image processing available at the camera nodes however necessitates collaboration with scalar sensors which may themselves be in error due to attack. In this paper we studied the strength and stealth properties of actuation attacks which unlike in previous studies, are carried out by hostile nodes that are not coordinated explicitly. We determine that the attack in this case may achieve a similar or *better* performance to the coordinated case, even if the hostile nodes' have varying trust levels.

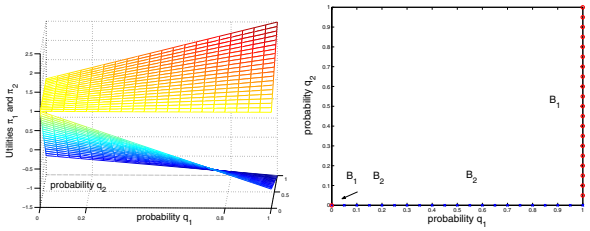

Fig. 7. Game where $k_{12} = 1$, $k_{21} = 1$, $m_{12} = -1$, $m_{21} = -1$. (a) Resulting utility manifolds for both players from Eq. 16. (b) Best response functions showing one Nash pure action equilibrium.

References

[1] I. Akyildiz, T. Melodia, and K. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks*, vol. 51, no. 4, pp. 921–60, March 2007.

[2] R. Cucchiara, "Multimedia surveillance systems," *Proceedings of the third ACM international workshop on Video Surveillance & Sensor Networks (VSSN)*, pp. 3–10, November 2005.

[3] H. Ma and Y. Liu, "Correlation based video processing in video sensor networks," in *IEEE International Conference on Wireless Networks, Communications and Mobile Computing*, Maui, Hawaii, June 2005, p. 987.

[4] K.-Y. Chow, K.-S. Lui, and E. Lam, "Efficient on-demand image transmission in visual sensor networks," *Eurasip Journal on Advances in Signal Processing*, vol. v 2007, p. 11 pages, 2007.

[5] W. Yu and K. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 459–473, May 2007.

[6] A. Czarlinska and D. Kundur, "Reliable scalar-visual event-detection in wireless visual sensor networks," in *IEEE CCNC Special Session on Image/Video Processing & Wireless Sensor Networks*, Las Vegas, 10-12 January 2008, available: www.ece.tamu.edu/˜czlinska/CCNC08/wvsn.pdf.

[7] A. Grigorova, F. D. Natale, C. Dagli, and T. S. Huang, "Content-based image retrieval by feature adaptation and relevance feedback," *IEEE Transactions on Multimedia*.

[8] A. Czarlinska, W. Luh, and D. Kundur, "Attacks on sensing in hostile wireless sensor-actuator environments," in *IEEE Globecom*, Washington, DC, 26-30 November 2007, available: www.ece.tamu.edu/˜czlinska/Glob07/AttacksSenAct.pdf.

[9] M. Wu and C. W. Chen, "Collaborative image coding and transmission over wireless sensor networks," *EURASIP Journal on Advances in Signal Processing*, vol. 2007, no. 1, p. 9, 2007.

[10] A. Liveris, Z. Xiong, and C. Georghiades, "A distributed source coding technique for correlated images using turbo-codes," *IEEE Communication Letters*, vol. 6, no. 9, pp. 379–381, 2002.

[11] V. Cevher, A. C. Sankaranarayanan, J. H. McClellan, and R. Chellappa, "Target tracking using a joint acoustic video system," *IEEE Transactions on Multimedia*, vol. 9, no. 4, pp. 715–727, 2007.

[12] D. Kundur, W. Luh, and U. N. Okorafor, "Emerging security paradigms for distributed multimedia sensor networks," *Proceedings of the IEEE Special Issue on Distributed Multimedia*, to appear 2007.

[13] F. Fu and M. V. D. Schaar, "Noncollaborative resource management for wireless multimedia applications using mechanism design," *IEEE Transactions on Multimedia*, vol. 9, no. 4, pp. 851–868, June 2007.

[14] M. Osborne and A. Rubinstein, *A Course in Game Theory*. M.I.T Press, 1994.