Adversary Aware Surveillance Systems

Vivek K. Singh and Mohan S. Kankanhalli

***Abstract*—We consider surveillance problems to be a set of system-adversary interaction problems in which an adversary can be modeled as a rational (selfish) agent trying to maximize his utility. We feel that appropriate adversary modeling can provide deep insights into the system performance and also clues for optimizing the system's performance against the adversary. Further, we propose that system designers should exploit the fact that they can impose certain restrictions on the intruders and the way they interact with the system. The system designers can analyze the scenario to determine conditions under which system outperforms the adversaries, and then suitably reengineer the environment under a "scenario engineering" approach to help the system outperform the adversary. We study the proposed enhancements using a game theoretic framework and present results of their adaptation to two significantly different surveillance scenarios. While the precise enforcements for the studied zero-sum ATM lobby monitoring scenario and the nonzero-sum traffic monitoring scenario were different, they lead to some useful generic guidelines for surveillance system designers.**

***Index Terms*—Adversary modeling, game theory, scenario engineering, surveillance.**

I. Introduction

RECENTLY, a significant amount of research has been undertaken by the visual surveillance community in areas like advanced detection, tracking, and recognition, etc. [1], [2]. However, sensor-adversary interaction which is pivotal to surveillance systems is very rarely studied. Very few works model the adversary and the typical models have been Poisson, equi-probability distributions, etc., over the entire possible action sets. This is in stark contrast with the multimedia security/cryptography studies where deep insights have been gained by modeling the performance of a "smart adversary" against the system [3].

Thus, we introduce the notion of a "smart adversary" into surveillance research. Such modeling can be used for measuring the system performance and analyzing the best and the worst-case performances. It can also be used to study the effects of changing different surveillance attributes (sensor positioning, etc.) on the system performance.

Manuscript received August 07, 2007; revised May 01, 2009. First published July 07, 2009; current version published August 14, 2009. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Gaurav Sharma.

V. K. Singh is with the Donald Bren School of Information and Computer Science, University of California, Irvine, CA 92697-3425 USA (e-mail: singhv@uci.edu).

M. S. Kankanhalli is with the School of Computing, National University of Singapore, Singapore 117417, Republic of Singapore (e-mail: mohan@comp.nus.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2009.2026459

We assert that another important concept missing from surveillance research is that of "scenario engineering." Typically, the surveillance setup is assumed to be "given" and "fixed." This may, however, not always be the case. For example, the positioning of an ATM machine within a lobby can and should be changed if it provides significant improvements in the surveillance effectiveness. Thus, we propose the use of "scenario engineering," which is defined as the process of finding the assumptions under which the system outperforms the adversary and then enforcing them on the scenario. The idea is akin to exploiting the "home ground advantage" to benefit your team wherever possible.

In our proposed work, both adversary and scenario modeling have been studied using a game theoretical framework. We assume our adversary to be a rational selfish agent who has a clear goal and utility gains/costs associated with each of his actions. We model the interaction problem as that of two selfish rational agents (system and the adversary), both trying to maximize their utilities while being acutely aware that the other agent is also trying to do the same. This fits in very well under a game theoretic framework which have extensively been used to study similar interaction problems between multiple nations, competing firms, and online bidders over the last few decades [4], [5].

We would like to point out that in the context of this work, we use the term "adversary" in a generic manner without any negative (or positive) connotations attached. The adversary is simply an agent whose motives are in partial (or complete) conflict with the surveillance system's goals. Thus, adversary could mean a robber trying to break into a house but could also mean a driver who is simply trying to speed as much as he can without paying a heavy penalty on a monitored road.

In this paper, we highlight how "adversary modeling" and "scenario engineering" can lead to significant improvements in surveillance system performance in different types of scenarios. Hence, we study two significantly different types of surveillance scenarios and discuss how the proposed features can be applied to them. The first studied scenario is an indoor zero-sum[1] surveillance game in an ATM lobby involving a malicious adversary. The second game on the other hand, is an outdoor nonzero-sum surveillance game for traffic monitoring on a highway involving a nonmalicious adversary.

The lessons from the scenario and adversary modeling in these two scenarios have lead to a generic set of guidelines which can be used by system designers when deciding on whether and which features to exploit to help the surveillance systems outperform the adversaries.

To summarize, the key contributions of this paper are as follows:

[1]In game theory, zero-sum games are those of extremely hostile nature where the loss of one player is the gain for the other, e.g., war-like situations. Nonzero-sum games on the other hand are those involving lesser hostility where one player's loss is not necessarily the other's gain, e.g., most daily-life situations.

1) modeling of rational selfish adversaries in surveillance scenarios through a game theoretic framework;
2) adoption of "scenario engineering" concept to allow modifications to the surveillance environment in order to benefit the surveillance system rather than the adversary.

To check the applicability of the proposed approaches in practical surveillance scenarios, we undertook theoretical analysis, simulation as well as practical experimentation. While the traffic monitoring scenario has been studied using analysis and simulations, the indoor ATM scenario has been studied using practical experiments in an enclosed rectangular area.

II. Related Work

There has been a large volume of work done in the computer vision, image processing, and related areas in surveillance. For example, Hu *et al.* [1] and Valera *et al.* [2] provide comprehensive discussions on the advances being made in visual surveillance research in terms of tracking, fusion, anomaly detection, etc. However, no works yet have undertaken *explicit* modeling of intruder or studied the concept of scenario engineering.

Pentland *et al.* [6] have been studying models of social interaction among humans using multimodal sensors. However, they do not undertake adversary modeling or explore surveillance-based applications. Looking from a multimedia security perspective, there has always been a notion of a smart adversary. Multiple works have benefited from an understanding of adversary behavior and the required counteractions. For example, [3] describes fingerprinting techniques which can be used to counter "multiuser collusion attacks." However, such adversary modeling-based counterapproaches have not yet been explored in the surveillance domain.

Work in the context-based awareness area also has a similar motivation as ours. For example, Kanter *et al.* [7] describe the creation of "personalisable" interactive spaces. However, they differ drastically on their focus. While we undertake an adversary analysis to ensure that the surveillance system settings help the system outperform the user (adversary), there the motivation is just the opposite.

A preliminary version of this paper appeared as [8]. That paper provided an exposition to the ideas of adversary and scenario modeling, but only considered an indoor zero-sum game scenario. In this work, we extend the ideas to a nonzero-sum outdoor surveillance game and also provide a generic set of guidelines as to how the system designers can design surveillance systems which perform better against adversaries.

Game theory, first proposed by John von Neumann and Oskar Morgenstern in 1944 has since been applied to many important areas like economic modeling of markets, bargaining scenarios, etc. [4], [9]. It must be noted that the game theoretic approach differs significantly from traditional operations research approaches as they normally consider the optimization function for only *one* rational agent. Game theory on the other hand considers the optimization problem for (at least) *two* agents even when their gains may be conflicting with each other.

Recently, the ARMOR project has employed the use of game theory for randomizing police patrols at the Los Angeles airport for better performance against adversaries [10]. This clearly highlights the growing awareness of using game theory for security applications. However, while they study a Bayesian Stackelberg game for patrol scheduling, we conduct a detailed analysis for surveillance scenarios and describe the concept of scenario engineering for enhancing system performance.

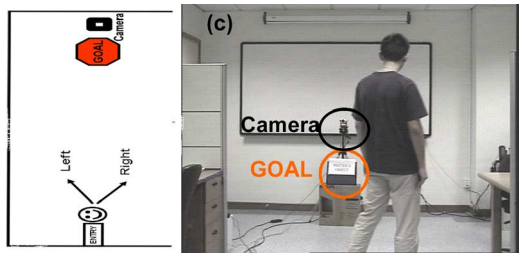

Fig. 1. Surveillance scenario: (a) schematic top view, and (b) actual layout.

To the best of our knowledge, ours is the first group to use game theory to model surveillance scenarios. Also, as far as we know, there have been no other attempts at *explicit* adversary modeling or scenario engineering in surveillance as yet.

III. Proposed Method

In this section, we describe our approach towards modifying the surveillance scenarios so as to help the system out-perform the adversary. We begin with a base-case indoor zero-sum game scenario of an ATM lobby in Section III-A. We extend the ideas to a nonzero-sum game involving traffic monitoring in Section III-B. While the scenarios and the enforcements made are specific examples, the key idea is to emphasize the need for questioning the assumptions/settings at each stage and explore ways to enhance system performance. Hence, we generalize the findings of the two scenarios into some generic insights and a set of guidelines for system designers to create more useful surveillance scenarios in Section III-C.

A. ATM Lobby Monitoring: Indoor Zero-Sum Game

Let us consider the surveillance scenario of an enclosed environment like that of an ATM lobby (or a museum subsection). We model this as a zero-sum game between a single camera surveillance system and a single intruding adversary. We assume that adversary's goal is to reach the important artifact, e.g., ATM machine (resp. expensive exhibit), while surveillance system's goal is to capture the adversary's facial images.

A typical surveillance setup in such a scenario looks similar to the one shown in Fig. 1. The adversary can move towards the goal by going towards the left or right direction. Clearly, a surveillance camera can only focus in one of the two directions, left or right. Hence, by purely random selection(s) by the adversary and surveillance system, the surveillance system has just a 50% probability of capturing the adversary's image. Our claim though, is that through adversary modeling and scenario engineering, the surveillance system can almost always outperform the adversary.

We assume both adversary and surveillance system to be rational agents trying to maximize their utilities. A game matrix representing their utilities for undertaking various actions is shown in Table I. The rows represent the direction of adversary's motion while the columns represent the direction being focused by the camera.

In the presented game matrix:

G represents the gain for adversary in getting nearer to the goal, and

c is the cost incurred by the adversary if her image gets captured.

TABLE I
SURVEILLANCE GAME BETWEEN ADVERSARY AND SYSTEM

$Adversary^{System}$	Left	Right
Left	$G-c+\epsilon$	$G+\epsilon$
Right	G	$G-c$

TABLE II
SURVEILLANCE GAME BETWEEN ADVERSARY AND SYSTEM SHOWN IN CARDINAL FORM (BEST STATE FOR ADVERSARY = 1)

$Adversary^{System}$	Left	Right
Left	3	1
Right	2	4

Also as a representation of the general case, we introduce bias such that the adversary has preference for one side than the other (no bias case is simply a special case of this). Our decision to include bias is based on multiple works like [11] and [12] which have pointed that humans have an unconscious bias in walking towards one side rather than the other. This is true even when there are clear directions provided, e.g., in museums [13]. Recent studies provide evidence for a leftward turning preference in right-handers, while non-right-handers show a bias towards the opposite turning direction [12]. For the sake of definiteness, we assume the adversary to be right-handed and the model adversary's leftward turning preference as an additional gain of ϵ.[2]

Thus, if the adversary moves towards the goal using the left direction and the camera also focuses on the left direction, then the adversary gains G by nearing the goal but incurs a cost of c because the camera can capture her image. Also, as the adversary has moved towards her preferred side, she also gets an additional gain of ϵ. On the other hand, if the adversary moves towards right and the camera focuses towards the left, then she obtains the gain G without incuring any cost.

Similarly, the values for the other two states [Left, Right] and [Right, Right] have been obtained. Note, that the matrix only shows values for the adversary as the gains for her are considered the losses for the surveillance system and vice-versa in this zero-sum game. Please note that the values G, c, and ϵ are conceptual abstractions of the kind of costs and gains one may see on such games; the actual values shall indeed vary for each specific game and situation. An equivalent of the game matrix which shows the cardinal order of utility values rather than the actual numerical utilities is shown in Table II.

The game matrix shown in Table I has no pure Nash equilibrium and one impure Nash equilibrium. Please recall that an impure equilibrium exists when both the players have no motivation in changing their adopted strategies *unilaterally* [4]. Consequently, it signifies that each player should become unbiased between his/her strategies. Thus, equating the utilities achievable by the adversary through her two strategies, we get

$$p_2\cdot(G-c+\epsilon)+(1-p_2)\cdot(G+\epsilon) = p_2\cdot(G)+(1-p_2)\cdot(G-c) \quad (1)$$

where p_2 is the probability of the surveillance system choosing strategy 1, i.e., focusing left.

This gives us a p_2 value of $(c+\epsilon)/2c$. Similarly, we obtain p_1, i.e., the probability of the adversary choosing Left as $c/2c$, i.e., 0.5 by solving for the condition when the surveillance system becomes unbiased between his strategies.

The Expected Utility for the adversary (EU_A) can be obtained by multiplying the probabilities for each possible game state (e.g., [Left, Left], [Left, Right], etc.) in the mixed equilibrium with the utility obtainable in it. It is found to be

$$\mathrm{EU}_A = G - \frac{c}{2} + \frac{\epsilon}{2}. \quad (2)$$

Clearly c is an important parameter which effects both the probabilities for [Left] and [Right] strategy selection as well as the net expected utility. From a system design viewpoint, we notice that currently the adversary utility is reasonably high. Hence, we need to explore ways to reduce it. Clearly, increasing cost c could help us achieve this target.

While there exist different ways (e.g., increased penalty, immediate counteraction, etc.) of increasing the adversary cost, one clearly feasible option to increase the adversary cost in the given setting is to employ pan-tilt-zoom (PTZ) capable cameras to obtain higher resolution adversary images which can be used for identification with a high confidence.

1) Enforcement 1: Increased Adversary Cost Through Enhanced Sensing: Hence, we enforce the use of PTZ capable cameras which undertake enhanced sensing (i.e., obtain high resolution images) of the adversary. These high resolution images can now be used to *identify* the adversary. The decision on whether to employ PTZ cameras can be based on the following intuitive reasoning.

If we employ PTZ cameras to make sure that images captured can be used for identification with a high confidence, the system incurs additional cost c_{ptz} and the adversary incurs c_{iden}, and the net impact on the adversary cost is c_{highRes}, i.e., $c_{\mathrm{highRes}} = c_{\mathrm{iden}} - c_{\mathrm{ptz}}$.

The system designers should spend additional money on PTZ cameras only if EU_A (after enforcement) $< \mathrm{EU}_A$ (before enforcement), i.e., $c_{\mathrm{highRes}} > 0$, i.e., $c_{\mathrm{iden}} > c_{\mathrm{ptz}}$.

In practice, for security of high value assets, we expect c_{iden} to often be significantly greater than c_{ptz}, and we will proceed in our discussion with that case. The net effect on the game matrix is that the effective adversary cost changed to $c' = c + c_{\mathrm{highRes}}$. While this effects the value of the EU_A, etc., it does not change any equilibria as simply the value of c can be replaced by c'. Lastly, the game matrix shown in cardinal form (Table II) remains the same.

Hence after enforcement 1, the net utility for the adversary becomes

$$\mathrm{EU}_A = G - \frac{c}{2} - \frac{c_{\mathrm{highRes}}}{2} + \frac{\epsilon}{2} \quad (3)$$

as this enforcement is applied only if $c_{\mathrm{highRes}} > 0$, we can claim that, it is worse for the adversary than before.

Clearly, our game would require multiple rounds of decisions to be made by the surveillance system and the adversary, rather than a single step. Hence, at this point, we consider the issue of *multistep optimization* in the considered game and handle the related dynamics. To understand the implications of repetition (especially when one player can assert more "power"), we employ the *theory of moves* [5], [14], which builds upon classical game theory concepts but extends it in three specific ways. First, it considers game-play to be *turn-based*, i.e., where each

[2]It is also possible to have a camera directional bias, but we assume that proper camera placement, calibration, etc., can remove that artifact. Human (intruder) bias on the other hand is intrinsic.

player takes a turn to choose their strategy rather than doing it simultaneously. This makes sense in our considered game, as the system and the adversary do not simultaneously decide their strategies but rather keep changing their strategies based on each other's response. Next, it considers the concept of *nonmyopic equilibrium* wherein each player looks ahead more than one move to consider the effects *and countereffects* of each strategy available before finally deciding on one. This is as opposed to the standard single-play Nash equilibrium which considers player's intentions to move just one step ahead. Lastly, "theory of moves" (TOM) does not give mixed strategy equilibrium solutions, which provide strategy answers as probabilities. Rather it gives a definite stable strategy as solution based on *starting state* and *which player makes the first move*.

The process of calculating the nonmyopic equilibrium works as follows:

1) Play starts at an *initial state*.
2) Player 1 can unilaterally change its strategy.
3) Player 2 can respond by unilaterally changing its strategy.
4) Such a process is repeated until the player whose turn it is, decides not to move. The resulting state is called the *outcome state*
5) A player will not move from its current state if this move:
   - leads to a less preferred final state (i.e., outcome);
   - returns eventually to the current state.

The ideas of TOM can be intuitively understood by analogies to the game of chess. Basically, TOM promulgates that the a player in her third best state should not try to go to her second best state if her opponent can undertake a counteraction to push her to her fourth best state. In other words, in a game of chess, you should not take your opponents pawn, if doing so makes your queen vulnerable. Similarly, you should avoid a move which would result in a series of actions which would bring you back to the starting state.

In effect, each player considers all his/her available options and the counteractions of the opponent to each of these actions. This results in a game-tree which has its leaf-nodes only when a previously visited state is reencountered. This is followed by a *backward pruning* phase wherein each player prunes away the less preferred outcome in its path from the leaf node to the root node. This means that at each step the players get rid of the worse of the two resultant possible options.

With this reasonable grounding in place, let us consider the game-tree for the scenario wherein the play starts at state [Right, Right] and the adversary makes the first move. The game tree is shown in Fig. 2. Note that our decisions now are based on relative preference for different states rather than the actual values. The utility values shown for each state shown in Fig. 2 are in terms of the the preference order of utilities as was shown in Table II. The game starts with the adversary's turn who has an option to continue with her strategy of focusing right, or consider the game subtree, if she changes strategy to focus towards the left. However, sticking to the right would cause repetition and hence is a possible outcome state (leaf node). Moving left, on the other hand, would allow the surveillance system to take counteraction, to which the surveillance system will react and so on leading finally to an outcome state.

As can be seen, the game tree lasts four turns before we get a state where both the options lead to previously visited states/ outcomes for the player whose turn it is. Hence, there are four

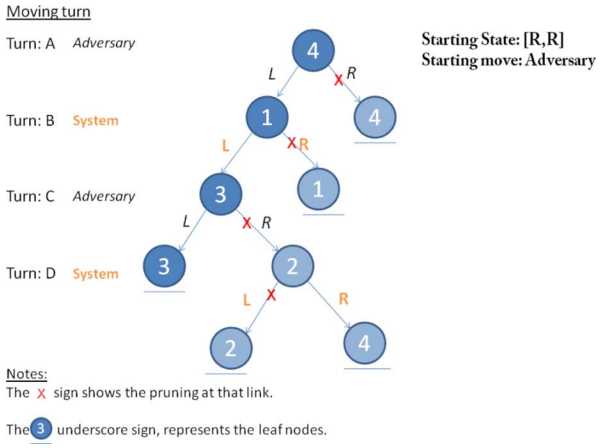

Fig. 2. Game-tree and backward pruning for starting state [R,R], adversary moves first situation.

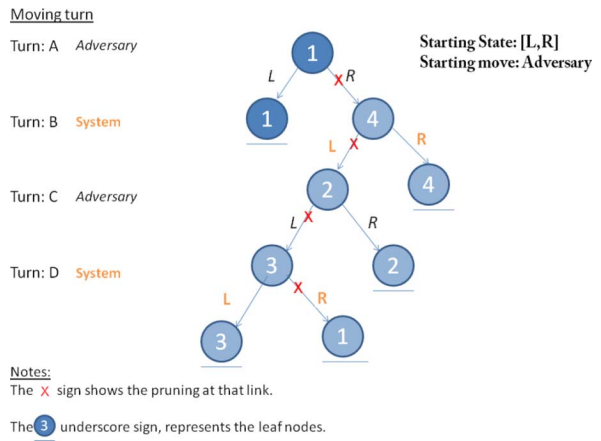

Fig. 3. Game-tree and backward pruning for starting state [L,R], adversary moves first situation.

decision points. Solving *backwards*, at turn D, the surveillance system has an option to go left to (potentially[3]) provide a utility of 2 (i.e., second best outcome) to the adversary or go right to potentially provide it a utility of 4. Given that the surveillance system wants the worst possible outcome for the adversary, he would *prune* away the path leading to the outcome of 2 thus allowing only a utility of 4 in that subtree. Following a similar mechanism, at turns C and B, right subtrees get pruned away, leading to an outcome utility of 3, as shown in the unpruned tree of Fig. 2.

Similarly (as shown in Fig. 3), we can calculate the resulting outcome if we change the initial state to [Left, Right]. The eventual outcome in this situation would have utility 1 which is different (and better for the adversary) than the (utility $= 3$) case discussed above. Thus, the starting state of the game does indeed have an impact on the expected outcome.

2) Enforcement 2: Changing the Starting State: We assert through this enforcement that the system designers can (and should) try to influence the starting point at which the conflicting interaction between the system and the adversary starts. This may be implemented in practice by allowing ATM entry only at a specific point to which the camera may already be pointing, or by using guiding rails, queues, etc., which would enforce the

[3]We use the term "potentially" as the final outcome is not decided yet.

TABLE III
EFFECT OF STARTING STATE ON THE ADVERSARY'S EXPECTED UTILITY

Starting state	adversary utility
[Left, Left]	3
[Left, Right]	1
[Right, Left]	2
[Right, Right]	3

adversary to start walking towards the ATM from a fixed point. Obviously, we cannot control his entire trajectory, but defining the entry point would already be quite useful.

Coming back to our TOM-based analysis, we have computed the resultant utility outcomes, for each starting state[4] in the considered game and the results are shown in Table III. As can be seen, if we can enforce the starting state to be one where the surveillance system is focusing on the adversary's face (i.e., [L,L] or [R,R]), then the expected utility state would be in the surveillance system's favor. Thus, the surveillance system, in a way, has got a jump-start into the game.

Intuitively, this enforcement can be seen as a version of advantage which a player would get if he could start with a favorable configuration of pieces in a game of "chess" or "go" rather than the default case.

If we notice the nuances of the game play, closely though, we would notice that, the outcome of the game-play in the two trees (Figs. 2 and 3) is largely affected by the repetitions, or rather the lack thereof, in the game-play. In real life, we cannot avoid all cyclic repetitions, rather they occur and come with a cost. Hence, we modify the game considered to allow iterations, such that they come with a cost α and β for the adversary and the surveillance system respectively.

3) Enforcement 3: Limiting the Time Availability: At this point, we enforce that the surveillance system's iteration loss (β) is negligible compared to the adversary's iteration loss α. Thus, in the considered game, the surveillance system has more "moving power" [5] than the adversary, i.e., it can keep "moving" the considered stable point and repeating the game for a very large number of cycles, while the adversary cannot do so. This makes sense as the surveillance system can afford to stay in those premises for as long as required but the adversary cannot stay for a long duration. In practice, such an enforcement can be applied by allowing people into the ATM lobby for only a limited time to finish their transaction. Again, relating back to the intuition of a chess game, this enforcement allows the surveillance system unlimited time to make his moves and thus allows cyclic repetitions, while the adversary is given much less time to complete her game-play and has to resort to "speed chess."

This modifies the considered game-tree in Fig. 3, such that when it is the adversary's turn, she cannot consider the strategies which result in cycles, but the surveillance system can do so. For example, at decision point B of the new game shown in Fig. 4, the Left option leading to utility 1 is no longer considered a leaf node, as the surveillance system is allowed to repeat states. This in effect allows the surveillance system to explore further into that subtree and is eventually useful in enforcing the utility state of 3. The adversary does not enjoy such luxury though, as evident at decision points C and E.

[4]An animated summary of all the game-trees and their pruning is available at www.ics.uci.edu/~singhv/AdvSurv/.

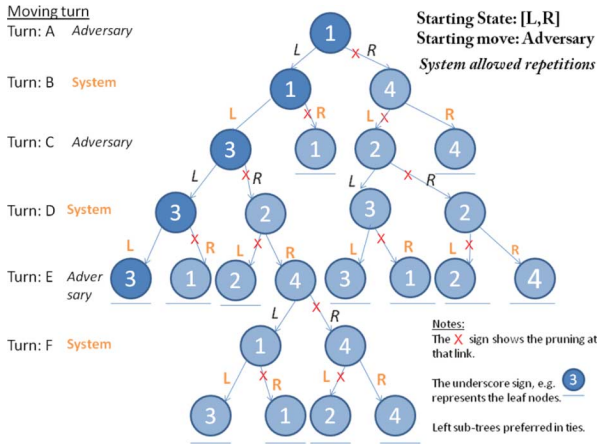

Fig. 4. Game-tree and backward pruning for starting state [L,R], the adversary moves first, and surveillance system allowed repetitions situation.

In fact it can be easily verified (via similar tree-pruning) that with this enforcement, the surveillance system can always force the adversary into the stable state of utility 3 irrespective of the starting state of the game.[5]

Thus the expected utility of this new game tree is

$$\mathrm{EU}_A = G - c' + \epsilon. \tag{4}$$

This would be similar to what we found with enforcement 2, but now this works without any boot-strapping, i.e., there are no restrictions on the initial state of the game. Intuitively, the idea is that if we allow the surveillance system large enough time to play the game, he will eventually reach the good state discussed before, and thus obtain the advantageous results discussed earlier.

Also, note that such a move–countermove forward analysis (pessimistic as it may seem for the adversary) does make sense for even her; as if she does not undertake such forward analysis to choose one stable state, she shall suffer from significant iteration losses which will make her net utility even worse than least-favorable of the stable state solutions (which shall happen in the iteration i, s.t. $i \cdot \alpha > c$).

A summary of the various enforcements, their intuitive effect, and the resulting Expected Utility are summarized in Fig. 5. We regard the transformations to be significant as through a series of reasonable enforcements we have brought down the adversary's utility from $G - (c/2) + (\epsilon/2)$ to $G - c + \epsilon - c_{\mathrm{highRes}}$ or in other words from having equal probabilities at each of the four outcome states to always ending up at her third best state.

B. Traffic Monitoring: An Outdoor Nonzero-Sum Game

The proposed ideas of adversary intention modeling and scenario engineering can also be applied to nonzero-sum games in which the system and the adversary goals are not directly opposite. Thus, one's gain is not necessarily the other's loss. In such games, there often exists an optimally stable point from which both agents have no incentive to diverge.

One such game takes place in traffic monitoring. In traffic monitoring, the system aims to ensure safety on the roads while

[5]The game-trees can now end only at the adversary's turn as the surveillance system is allowed to repeat moves. Percolating up, the surveillance system in his turn B will prune away the top 2 out of the adversary's 4 possible outcomes coming from below. In turn A, the adversary will prune away her fourth worst state, thus the only state percolating up is the third worst, i.e., 3.

S. No	Situation	Adversary Expected Utility	Analogy/ Intuition
1	Nash Equilibrium	*G- 0.5c + 0.5ε*	No unilateral desire to move away from the equilibrium.
2	Enforcement 1: Increased adversary cost through enhanced sensing	*G- 0.5c' + 0.5ε* s.t. c'=c + $c_{highRes}$ Equal probability of cardinal Expected Utility states 1,2,3,4	Increased cost for the adversary. He has more to lose.
3	Enforcement 2: Changing the starting state	*G-c' + ε* Expected Utility states is 3, given the initial state is [L,L] or [R,R]	Chess analogy: Advantage of playing with a helpful initial state e.g. opponent King on 'check'
4	Enforcement 3: Limiting the time availability	*G-c' + ε* i.e. State 3 irrespective of the starting state of the game.	Chess analogy: Advantage of playing with unlimited time to make moves while opponent has limited time.

Fig. 5. Scenario 1 summary.

a driver is interested in the opportunistic gains associated with speeding. However, both have costs associated with their efforts aimed at achieving their respective goals and hence would like to find the optimal effort levels to undertake.

To render the problem more explicit, let us consider the scenario of a traffic freeway D miles long which connects two major cities. For simplicity, let us assume that it is the only road which connects the two cities and its speed limit is $q_{2\text{allowed}}$ mph. The surveillance system can place multiple mobile surveillance units [(MSUs) which are also colloquially referred to as "speed traps"] on the road to catch any speeding incidents. Let us say that each such MSU covers $D/q1_{\max}$ miles of road and $q_{1\max}$ such units can completely monitor the entire road stretch. Hence, we measure the system effort in terms of the number of MSU's employed by it, and the driver's effort in terms of his speed. One possible strategy for the system (and the driver) is to put in their maximum possible efforts. However, this may not be the optimal strategy as even the maximum effort level does not guarantee receipt of the full reward (e.g., a fully speeding driver may still get caught by camera on the road). Thus, the key questions to be answered by the system designer (and the driver) in such a situation are:

1) For the surveillance system: What is the optimal *number of MSUs* that must be employed on the highway?
2) For the driver: What is the optimal *speed* to drive on the highway?

Our aim in studying this problem is to find out the stable strategy point which shall be optimal for both the system and the adversary and then how the scenario settings can be changed to allow the system to improve its performance.

To model such a situation, we start by defining the over-all gain function for the two agents. The system net gain (Φ_1) is modeled as

$$\Phi_1 = \Pi_1 \cdot G_1 - c_1 \cdot q_1 \tag{5}$$

where

Π_1	is a measure of how well the system is able to maintain safety on the road.
G_1	is the system gain associated with the maintenance of road-safety.
c_1	is the cost for an exhaustive safety assurance effort.
$q_1 = (q_{1\text{exerted}}/q_{1\max})$	is the safety assurance effort in terms of the number of MSUs employed as a ratio of the number of MSUs required for exhaustive coverage.

One way to look at this formulation is that the system obtains a fraction Π_1 of his gain G_1 if he incurs fraction q_1 of his cost c_1. Similarly, for the driver we can formulate his net gain as

$$\Phi_2 = \Pi_2 \cdot G_2 - c_2 \cdot q_2 \tag{6}$$

where

Π_2	is a measure of how well the driver can achieve his opportunistic goal.
G_2	is the driver's gain associated with achieving his opportunistic goal.
c_2	is the cost for the maximum possible over-speeding effort.
$q_2 = (q_{2\text{exerted}} - q_{2\text{allowed}}/q_{2\max} - q_{2\text{allowed}})$	is the (over-)speeding effort as a ratio of the maximum over-speeding possible.

The terms Π_1 and Π_2 in turn are formulated as follows:

$$\begin{aligned}&\Pi_1 \propto \text{SystemStrictness}\\ &\Pi_1 \propto \text{DriverSlowness}\\ &\Pi_1 = \lambda_1 \cdot \text{SystemStrictness} \times \lambda_2 \cdot \text{DriverSlowness}\end{aligned} \tag{7}$$

and

$$\begin{aligned}&\Pi_2 \propto \text{SystemLeniency}\\ &\Pi_2 \propto \text{DriverQuickness}\\ &\Pi_2 = \lambda_3 \cdot \text{SystemLeniency} \times \lambda_4 \cdot \text{DriverQuickness}\end{aligned} \tag{8}$$

where

$$\begin{aligned}\text{SystemStrictness} &= \lambda_5 \cdot q_1^{1/k}\\ \text{DriverQuickness} &= \lambda_6 \cdot q_2^{1/k}\end{aligned}$$

with such a gamma-function like nature chosen for these functions to represent that their values increase more rapidly at their lower levels than at higher ones. Similarly, we define the "system leniency" and "driver slowness" as

$$\begin{aligned}\text{SystemLeniency} &= 1 - \lambda_5 \cdot q_1^{1/k}\\ \text{DriverSlowness} &= 1 - \lambda_6 \cdot q_2^{1/k}.\end{aligned}$$

Hence, after the definition of all the parameters, the over-all equation for the system gain, as shown in (5), can be rewritten as

$$\Phi_1 = \left(\lambda_1 \cdot \left(\lambda_5 \cdot q_1^{1/k}\right)\right) \times \left(\lambda_2 \cdot \left(1 - \lambda_6 \cdot q_2^{1/k}\right)\right) - c_1 \cdot q_1 \tag{9}$$

and for the driver, (6) can be rewritten as

$$\Phi_2 = \left(\lambda_2 \cdot \left(\lambda_6 \cdot q_2^{1/k}\right)\right) \times \left(\lambda_1 \cdot \left(1 - \lambda_5 \cdot q_1^{1/k}\right)\right) - c_2 \cdot q_2. \tag{10}$$

However, for the ease of representation, let us take $k = 2$ and λ_i for all i to be 1. This simplifies (9) and (10) to

$$\Phi_1 = \sqrt{q_1} \cdot (1 - \sqrt{q_2}) \cdot G_1 - c_1 \cdot q_1 \tag{11}$$
$$\Phi_2 = \sqrt{q_2} \cdot (1 - \sqrt{q_1}) \cdot G_2 - c_2 \cdot q_2. \tag{12}$$

We continue the rest of our discussion with these formulated values of system and adversary gain. Please note that we do realize that above-mentioned notions of safety and opportunistic speeding gains are abstract and difficult to quantify; but we feel that studying a surveillance scenario with them does make sense, as they do represent some specific attributes which traffic security administrators might consider when making policy decisions.

1) Finding the Optimal Effort: As can be observed from the obtained equations [(12) and (13)], the overall gains for each agent (system and the driver) are dependent on the effort values chosen by the other. Thus, this problem of optimization which has to be solved by both agents becomes interesting as it is a two-agent optimization problem with each trying to maximize their own utility, potentially at the cost of the other agent's utility. This makes this problem very different from traditional single-agent optimization problems as studied in operations research.

In such a context, game theory defines an optimal response for each agent in terms of a Nash equilibrium point, i.e., a *stable* strategy point at which each agent has no incentive for unilateral deviation [4].

The approach to finding such an equilibrium point is as follows. We first find the optimal effort for the system taking driver effort to be a constant. This gives us the optimal system response for any given driver effort. Then we repeat the same process for the driver taking the system effort to be constant. Then we solve the two obtained equations *simultaneously* to find the Nash equilibrium. Thus, the Nash equilibrium gives us a point at which each of the two agents has simultaneously maximized their functions for the other agent's exerted effort. Consequently, there is no incentive for either agent to unilaterally deviate from this point.

In the modeled scenario, the optimal effort for the system can be computed by finding the partial derivative of function Φ_1 as follows:

$$\frac{\partial \Phi_1}{\partial q_1} = \frac{1}{2} \cdot (1 - \sqrt{q_2}) \cdot G_1 \cdot \frac{1}{\sqrt{q_1}} - c_1 \tag{13}$$

and then setting it to zero to obtain the optimal effort value as follows:

$$\sqrt{q_1} = \frac{1}{2} \cdot (1 - \sqrt{q_2}) \cdot \frac{G_1}{c_1}. \tag{14}$$

A similar process can be undertaken for the driver's utility function to obtain his optimal response function

$$\frac{\partial \Phi_2}{\partial q_2} = \frac{1}{2} \cdot (1 - \sqrt{q_1}) \cdot G_2 \cdot \frac{1}{\sqrt{q_2}} - c_2 \tag{15}$$
$$\sqrt{q_2} = \frac{1}{2} \cdot (1 - \sqrt{q_1}) \cdot \frac{G_2}{c_2}. \tag{16}$$

To find the Nash equilibrium, we must solve (14) and (16) simultaneously resulting in their optimal values which are now independent of each other's effort [4]

$$\sqrt{q_1} = \frac{2 \cdot c_2 \cdot G_1 - G_1 \cdot G_2}{4 \cdot c_1 \cdot c_2 - G_1 \cdot G_2} \tag{17}$$
$$\sqrt{q_2} = \frac{2 \cdot c_1 \cdot G_2 - G_1 \cdot G_2}{4 \cdot c_1 \cdot c_2 - G_1 \cdot G_2}. \tag{18}$$

The obtained net gain obtained by both the agents under such a scenario becomes

$$\Phi_1 = \left[\frac{2 \cdot c_2 \cdot G_1 - G_1 \cdot G_2}{4 \cdot c_1 \cdot c_2 - G_1 \cdot G_2}\right]^2 \cdot c_1 \tag{19}$$
$$\Phi_2 = \left[\frac{2 \cdot c_1 \cdot G_2 - G_1 \cdot G_2}{4 \cdot c_1 \cdot c_2 - G_1 \cdot G_2}\right]^2 \cdot c_2. \tag{20}$$

2) Enforcement 1: External Influence: As can be noticed from (19) and (20), the gains for the two agents are fairly symmetric in the modeled scenario. However, we as system designers have more power to influence the scenario than the adversary. Hence, we use Enforcement 1: External influence, which states that the surveillance system designers can use their relationship with other law enforcement agencies to alter the over-speeding cost (c_2) for the drivers.

This makes sense and can be enforced at multiple levels by the surveillance system assuming that it is controlled/supported by an enforcement agency. For example, the enforcement agency can *increase* or *decrease* the cost by

1) using more (or less) frequent speed breakers, traffic lights, and changing their number, position, etc.;
2) increasing or decreasing the fines.

To mathematically verify the effect of these changes, we find the slope of system gain function (19) w.r.t. c_2, which evaluates to

$$\frac{\partial \Phi_1}{\partial c_2} = \frac{4c_1(G_1)^2 G_2(2c_1 - G_1)(2c_2 - G_2)}{(4c_1c_2 - G_1G_2)^2(4c_1c_2 - G_1G_2)}. \tag{21}$$

Looking at (20) carefully, we realize that the gradient value is determined by the interplay of three specific components viz.

A defined as $2c_1 - G_1$;
B defined as $2c_2 - G_2$; and
C defined as $4c_1c_2 - G_1G_2$.

These components partition the possible scenario into different "zones," which each have separate strategies for enhancing system performance. A summary of the different possible scenarios (based on positive$(+)$ or negative$(-)$ evaluation of components), the function gradients and the optimal strategy to alter the adversary cost is summarized in Table IV.

We consider this to be a very interesting result. It first points out that there is no specific one-fits-all strategy about altering the adversary costs to improve the system performance; rather it depends on the parameters of the specific scenario being studied. Second, it is not always beneficial to increase your adversary's costs. Sometimes it may be better to *reduce* his/her costs in order to improve your net gains.

To further improve the system performance, we draw inspiration from Stackelberg competition in Duopolisitic markets [9]. In such markets, often one company acts as a "leader" and is able to choose its effort (say production) level before a "follower" company enters the market. When, the second company enters the market, it must optimize its effort based on the market

TABLE IV
OPTIMAL STRATEGY FOR ALTERING THE ADVERSARY COST FOR DIFFERENT SCENARIOS POSSIBLE

A	B	C	$\frac{\partial \Phi_1}{\partial c_2}$	driver cost should be:
+	+	+	+	Increased
+	+	-	Situation infeasible	.
+	-	+	-	Decreased
+	-	-	+	Increased
+	+	+	-	Decreased
+	+	-	+	Increased
+	-	+	Situation infeasible	.
+	-	-	+	Increased
.	.	0	Undefined	.

parameters as well as the effort level *already* chosen by the first company. This is in contrast to a level playing field situation where both companies enter the field at the same time and simultaneously try to maximize their gains. The advantage for a far-sighted "leader" in such a setting is that he can *a priori* consider the game and tune his effort to a level which optimizes his over-all gain when the "follower" enters. This is a clear example of a "leader" exploiting his "prime mover advantage" to improve on his obtainable gain in a duopolistic setting.

3) Enforcement 2: Prime Mover Advantage: We employ a similar enforcement on our two player game such that the surveillance system can act as a "leader" and outperform the "follower" (adversary). We enforce that the surveillance precommits to a chosen effort level and makes such a commitment transparent to the adversary. This in effect reduces the option space available to the adversary, and he has to optimize within it.

We believe that such an enforcement is feasible because the surveillance system typically makes decisions like how many MSUs to employ, etc., much before the driver enters the scene. As long as the system signals such effort level information to the driver, the system has in effect forced the Stackelberg competition constraints. There are many interactive warning signs, etc., in place already at most metropolitan cities. While, most current such boards do not specify the effort level, i.e., the number of MSUs being employed by the system, we assert that it should be the way to go in future. Thus, warning messages like "You are being monitored by 40 surveillance cameras" (Fig. 6: Picture taken at a Singapore train station) should be displayed via message boards on freeways as they can actually force the driver to reassess the game and recompute his/her optimal speed.

Let us discuss the process for the system to compute the optimal effort under these new settings and what would be the response from the driver.

We noticed earlier in (14) and (16) that the optimal efforts for both the system and the driver depend on each other. Also, while the system does not know the driver's precise effort level chosen before-hand, it does know the function which a rational adversary shall use to evaluate it's optimal response. This is simply the value q_2 shall be as depicted in (16). Thus, the system can use this value to model its net gain (11) which now becomes

$$\Phi_1 = \sqrt{q_1} \cdot \left(1 - \frac{G_2}{2 \cdot c_2} \cdot (1 - \sqrt{q_1})\right) \cdot G_1 - c_1 \cdot q_1. \quad (22)$$

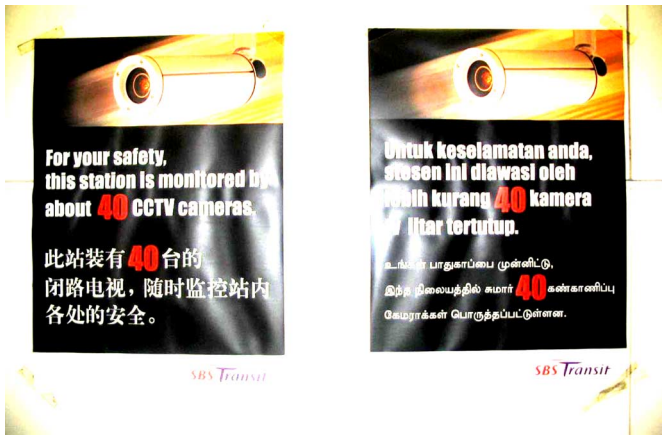

Fig. 6. Security message as displayed at a Singapore train station.

Note that this equation is now independent of q_2, and hence can be optimized with respect to only q_1 to find the optimal value. We follow the usual process of taking partial differential and equating it to zero to obtain the optimal q_1 value as:

$$\sqrt{q_1} = \frac{2 \cdot c_2 \cdot G_1 - G_1 \cdot G_2}{2 \cdot (2 \cdot c_1 \cdot c_2 - G_1 \cdot G_2)}. \quad (23)$$

The driver will follow the usual optimization process with (15). However, the specific value of $q1$ in its equations now will be as chosen by the system in (23). Thus

$$\sqrt{q_2} = \frac{G_2}{2 \cdot c_2} \cdot \frac{4 \cdot c_1 \cdot c_2 - G_1 \cdot G_2 - 2 \cdot c_2 \cdot G_1}{2 \cdot (2 \cdot c_1 \cdot c_2 - G_1 \cdot G_2)} \quad (24)$$

and drivers net profit is

$$\Phi_2 = \frac{(G_2)^2}{4 \cdot c_2} \cdot \left[\frac{4 \cdot c_1 \cdot c_2 - G_1 \cdot G_2 - 2 \cdot c_2 \cdot G_1}{2(2 \cdot c_1 \cdot c_2 - G_1 \cdot G_2)}\right]^2. \quad (25)$$

Consequently, the profit for system is

$$\Phi_1 = \frac{[2 \cdot c_2 \cdot G_1 - G_1 \cdot G_2]^2}{8 \cdot c_2 \cdot (2 \cdot c_1 \cdot c_2 - G_1 \cdot G_2)}. \quad (26)$$

4) Enforcement 3: Perception Play: A volume of work has been done under hyper-game theory [15], [16] which highlights that the players involved in games often do not play games as they are, but rather how they *perceive* them to be. Thus, a player makes an optimal decision only on the basis of what he thinks the current game is. This idea is often employed in psychological warfare, etc., to "play with the mind" of the adversaries via bluffing, etc. We, however, suggest a much mellower enforcement in our surveillance scenario. We enforce that the surveillance system can increase *awareness* of the driver, regarding the "ills of speeding," "importance of road courtesy," etc., which can bring down the *perceived* gain by speeding for the driver. This results in lower perceived value of G_2 as shown in (23)–(26). To observe the precise effect of decreasing G_2 on the system net profit, we evaluate the slope of system gain function (20) w.r.t. G_2

$$\frac{\partial \Phi_1}{\partial G_2} = \frac{G_1^2(2c_2 - G_2)(-4c_1c_2 + G_1(2c_2 + G_2))}{8c_2(-2c_1c_2 + G_1G_2)^2}. \quad (27)$$

Further analysis of this function yields the following:

1) If $G_2 < c_2 \cdot ((4 \cdot c_1/G_1) - 2)$, then slope is negative and the G_2 values must be decreased.
2) If $G_2 > 2 \cdot c_2$, then also the slope is negative and the G_2 values must be decreased.
3) However, if $((4 \cdot c_1/G_1) - 2) < G_2 < 2 \cdot c_2$, then the function is unstable due to a discontinuity at $G_2 = (2 \cdot c_1 \cdot c_2)G_1$

However, we focus on the stable region of the function and notice that it makes sense to decrease the adversary's perceived gain to improve the system performance.

C. Generic Treatment

As discussed in Sections III-A and III-B, we noticed that in both zero-sum and nonzero-sum games there exist many opportunities where the surveillance systems can benefit by a scenario engineering approach. In this section, we summarize the process of analyzing the surveillance scenarios and provide some generic guidelines to aid other system designers intending to apply scenario engineering approaches in their chosen surveillance scenarios. While, we strongly believe that scenario engineering is as much an art as it is a science, we feel that certain prescriptive guidelines shall definitely be useful for a system designer to get started with the process. Our proposed analysis methodology is as follows:

A methodology for handling interactions in surveillance

Step 1) Find the adversary's intentions.
Step 2) Model the interaction game: Find the costs and gains associated for the system and the adversary.
Step 3) Find out what is the type of interaction?
  If *zero-sum game*: Strategy is to increase system gain
  and/or decrease the adversary gain.
  else
  If *non-zero-sum game*: Strategy is to increase system gain only.
Step 4) Find out what factors affect the outcome of this game.
Step 5) Find which of these factors can be changed and what is the impact of the change.
Step 6) Try changing the outcome of the game in your favor. Factors to be explored are:
  a) Spatial factors
  b) Temporal factors
  c) External factors
  d) Perceptual factors
  e) Stealth factors
Step 7) Choose the most appropriate factor to modify.
Step 8) Are the game results acceptable?
  If *No*: Repeat from Step 4
  else
  If *Yes*: Done

Needless to say, in the presented methodology, the exact factor to adjust and the value of adjustment shall depend on the precise game being studied. However, the generic factors highlighted apply to many surveillance tasks and can and should be used where appropriate. Let us look at each one of them in slightly more detail.

1) Spatial Factors: The physical dimensions (e.g., shape, geometry, guide-rails) under which the game is being played often determines the choice(s) available to the players and changing them influences the outcome of the game. For example in the surveillance of an enclosed ATM lobby (Section III-A), we found that using a fixed entry point or guide rail, etc., helps the surveillance system. In other scenarios like wild-life monitoring, etc., changing the position of the cameras or sometimes even the animal's point of interest (say a water stream) can influence the obtainable gains from a surveillance system.

2) Temporal Factors: In surveillance interaction games, the costs, efforts, and gains chosen by one player invariably affect the other player. In many circumstances foreknowledge of the other player's strategy can (positively or negatively) influence the effort and strategy for a player. For example, if the surveillance system could predict the next move of the intruder, it could obviously improve its performance. However, there may also be instances where foreknowledge is harmful to a player. For example, as studied in Section III-B, it turns out that the warning signs like "This area is being monitored by 40 surveillance cameras" help the system more than the adversary. Similarly, some shops which put notices like "this premise is surveillance protected by XYZ security company" may actually be benefiting by providing this additional information to their adversaries. Thus, the merit of providing or withholding such information before the adversary makes his choice can be studied by the system designers for the specific game at hand and used to influence the outcome.

3) External Factors: Surveillance interaction games are also often based on certain tacit assumptions about the settings under which the game is taking place. There may be factors which are not directly involved in the game but changing which can affect the outcome of the game. As the surveillance systems are normally employed by law enforcement agencies which can influence more factors than the adversaries, it may be possible to exploit some of such external factors by the surveillance systems to improve their performance. For example, in a traffic monitoring game (Section III-B), we realized that various enforcements can be made to alter the cost of speeding for the cars. Similarly, in a museum's surveillance, the people entering could be asked to keep their (say RFID) tags on at all times to make the monitoring easier. The feasibility of such factors should also be considered by the system designers while holistically analyzing the surveillance games.

4) Perception Changes: As discussed in a hyper-game theory context [15], [16], games are played as they are perceived to be. Given the wider variety of resources normally available to the law enforcing agencies controlling the surveillance systems, it may be possible for them to influence the perceived utilities and costs in the game. For example, as shown via enforcement 3 in the traffic-monitoring game, awareness signs like "Speeding Kills," etc., can be used to influence the perceived gain and cost values associated with the game. Similarly, messages like "shoplifting is a serious crime" or "this store carries has less than $30 at night" could be used to influence the adversary's perceived values of gain and costs.

5) Stealth Factors: As discussed above, the players decide their strategy based on their assessment of the gains and the

costs. Further, the players decided the game based only on their interpretation of the factors and the options available. Hence, stealth and surprise can also be used as tools to outperform the adversary in certain instances. However, such factors must be weighed against Kerckhoffs' principle (that the system must be secure even if it is transparent to the adversary) [17] and ethical issues before being adopted. Hence, in our examples, we have not employed "stealth" as a technique. For the perception change factor used in traffic surveillance game, we have also decided to use only the "awareness" aspect. However, this does not rule out system designers, say in military settings, making use of covert surveillance to fulfill their specific goals.

IV. Results

A. ATM Lobby Monitoring

To check the veracity of our proposed approaches, we conducted multiple rounds of experiments simulating a scenario where the adversary's aim is to pick up a "precious object" kept inside a room. The adversary aims to get as near as possible to the precious object without getting her facial images captured while the system tries to get as many high-resolution facial images of her as possible.

We conducted four sets of experiments, each consisting of 40 rounds. The experiments were conducted in an enclosed environment of 20 ft by 15 ft dimension using an Axis 214 Pan Tilt Zoom camera. The volunteer adversaries were graduate students who were received a clear explanation of the purpose of the experiments and the "gains" and "losses" that can be incurred by them. They were explicitly asked to beat the system by changing their trajectory as and when required but were asked to maintain a steady walking pace and not to hide their faces.

In the base case setup, we kept the precious object at the center of the room as shown in Fig. 1(a). The camera was employed at 640 by 480 pixel resolution with active pan and tilt (but no zoom) to capture the adversary's face. The face detection was run at 320 by 240 px for efficiency though.

After this, we iteratively enforced the three scenario engineering enforcements and checked their impact on the number of "successful steals" and the number of high-resolution facial images found. We define "successful steals" as those cases in which the system cannot obtain at least three high-resolution facial images. We define high–resolution images as those which capture facial information at minimum 100 by 100 px resolution (see Fig. 7), which can also be used for automatic face recognition at an accuracy of around 90% [18]. The underlying assumption here is that the adversary shall lose enough utility to counter her gain upon reaching the precious object, if her three high-resolution images are captured.

As shown in Table V and Fig. 8, we found that in the base case setup, the adversaries were on average able to successfully steal the precious object 62.5% of the time. Also, the average number of high-resolution faces captured per stealing attempt was 2.2. We noticed that there were a significant number of frames with insufficient resolution facial images. Thus, we used enforcement 1, "increase the adversary cost through enhanced sensing," and added a feature to zoom towards the adversary faces upon detection. This reduced the number of successful steals to 25% and the average number of high-quality facial images captured

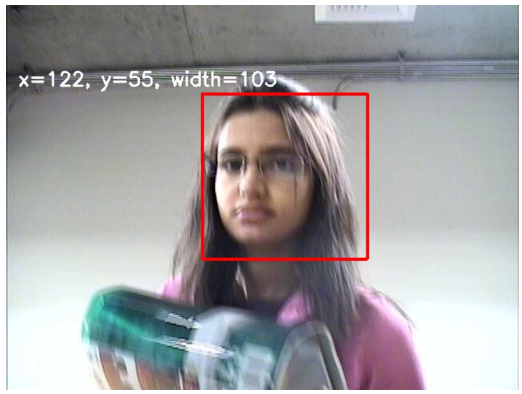

Fig. 7. Sample high-resolution image of an adversary trying to steal the precious object.

TABLE V
Number of Rounds With Successful Steals

Base case	Enfo. 1	Enfo. 2	Enfo. 3
25 (62.5%)	10 (25%)	4 (10%)	3 (7.5%)

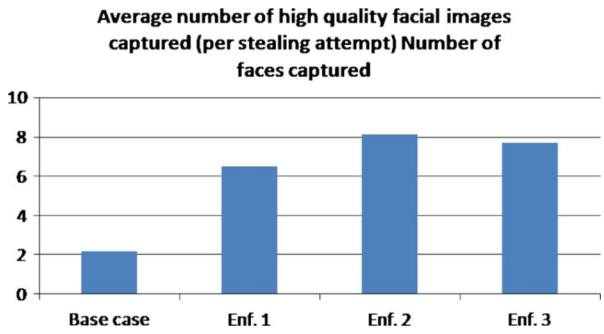

Fig. 8. Number of faces detected.

increased to 6.5. We noticed that some adversaries were able to counter the system by going away from the camera and approaching it in an obtuse trajectory.

Hence, we employed Enforcement 2, "changing the starting state," and boot-strapped the cameras by explicitly pointing the camera with the intruder facial position in the first frame. Thus, in effect, the game started with the adversary being in a disadvantageous position. This was done in experiments using the point-and-click pan-tilt interface provided by the Axis cameras. From there on, the system and the adversary were on their own trying to out-perform each other. We noticed though, that with this enforcement, the number of successful steals was reduced to 10%, and the number of images captured increased to 8.1. Lastly, to study the effect of enforcement 3, we changed the alloted time for intruders to "steal" to only 12 s. This duration was assumed to be enough for picking the object as this was the average time taken by adversaries to steal the object in round 2 (using just Enforcement 1). We noticed that this enforcement was also useful and only 7.5% of adversaries were able to get away without having three facial images captured. The average number of facial images captured was 7.7. This was marginally less than what was obtained after enforcement 2, but we still consider the results positive, as the enforcement 3 results were obtained without any boot-strapping.

Based on these four rounds of experiments, we observed that the three "scenario-engineering-based" enforcements did indeed help in increasing the surveillance system performance.

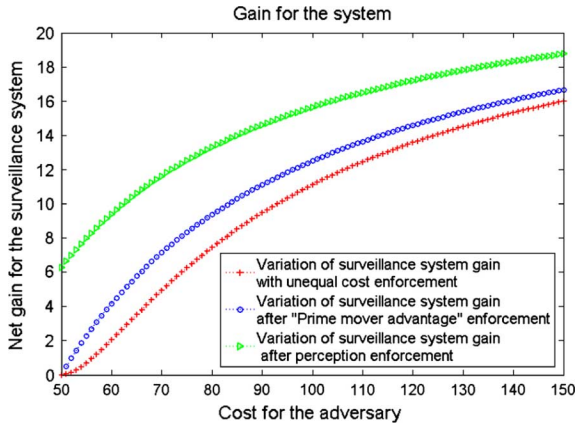

Fig. 9. System net profit: Effect of the three enforcements.

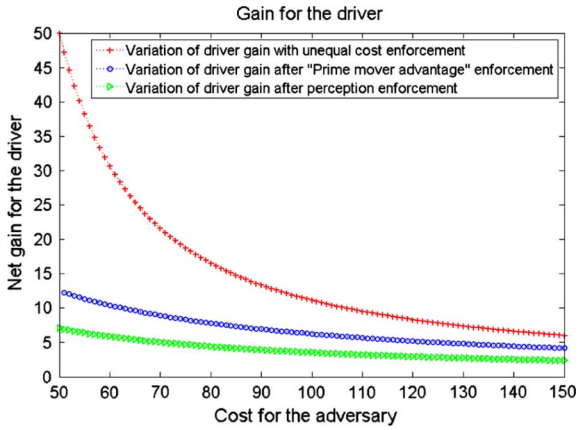

Fig. 10. Driver net profit: Effect of the three enforcements.

B. *Traffic Monitoring*

To study the effect of various scenario-engineering-based enforcements on the traffic monitoring game, we studied the impact of various enforcements on adversary and system performance. Due to the infeasibility of conducting experiments on real freeways with MSUs, etc., we have decided to study these effects via computational experiments undertaken using Matlab. They shall be indicative of the process which we can expect to see in the real-life traffic situation.

The parameters assumed for the experiments were as follows. We assumed the traffic speed limit to be 50 mph and the maximum possible speed to be 150 mph. We also assumed that the number of MSUs can be varied from 1 to 100, which is the maximum required to exhaustively cover the entire road length. We initially set the costs (c_1 and c_2) and gains (G_1 and G_2) to all be a symmetric value of 100 each. We will keep adjusting these values upon enforcements as required.

The base case calculations resulted in an equilibrium point at the system deployment of 11 MSUs and a speed of 61.1 mph for the driver. In this case, both the system and the adversary obtained a net profit of 11.1 units.

To study the effect of "external influence" enforcement, we varied the cost for the adversary from 50 to 150 units. Other parameters were kept at the same values as earlier, i.e., $G_1 = G_2 = 100$, $c_1 = 100$. As can be seen in Figs. 9–12 ("+" sign plot) which show the system profit, driver profit, system effort, and driver effort, respectively, the lower values of cost resulted in higher equilibrium speeds (and profits) for the driver. On the other hand, higher costs had the impact of reducing the driver speed and the obtained profit while the system profits increased. Note that this makes sense, as the considered parameters represent a scenario of the first "zone" (positive values for $2c_1 - G_1$, $2c_2 - G_2$, and $4c_1c_2 - G_1G_2$) as shown in Table IV, where increasing the driver cost should have a positive influence on the system profit.

Next, we enforced the "prime mover advantage" enforcement to allow the system to choose its effort value first. As can be seen in Fig. 11, the calculated optimal system effort was 25 MSUs ("o" sign plot). This resulted in lower speed and profits for the driver as shown in Figs. 10 and 12.

Lastly, we imposed the "perception play" enforcement, and assumed that the driver's perceived gain (G_2) has been changed from 100 to 80. This resulted in even lower equilibrium speed and profit values for the driver as shown in Figs. 10 and 12 ("▷" sign plot). Also, as seen in Fig. 9 the system profit further improved with this enforcement. Thus, using a series of reasonable enforcements, we have been able to increase the system profit from 11.1 units in the base case to significantly higher values, e.g., 16.6 units for $C_2 = 120$.

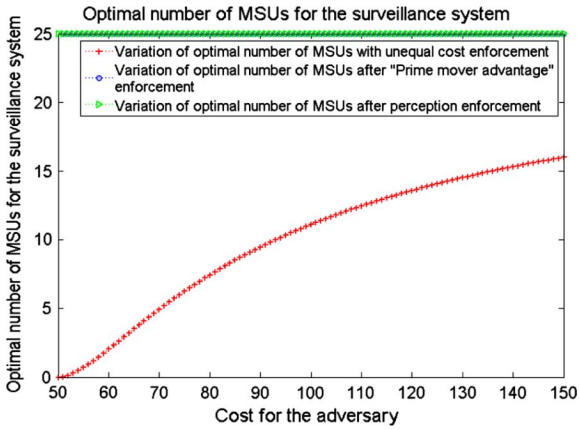

Fig. 11. System effort levels (number of MSUs): Effect of the three enforcements.

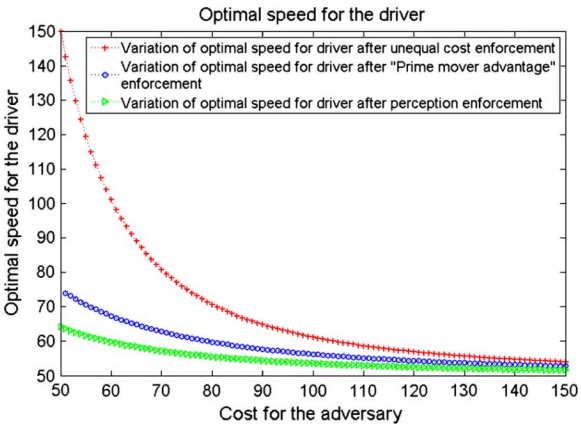

Fig. 12. Driver effort levels (speed): Effect of the three enforcements.

Please note that these improvements also provide a prescriptive estimate of the amount of "extra effort" which is justifiable for the law-enforcement agencies to put in to help the surveillance systems perform better against the adversary. For example, at an adversary cost of 70 units (refer Fig. 9), the system profit increases from 4.93 to 7.14 units with the employment of prime mover advantage enforcement. Hence,

the enforcement agency should spend no more than 2.21 units (roughly the cost of two MSUs) to enforce that the adversary is aware of the number of cameras being employed.

Through our experiments, we have verified the impact of the various proposed enforcements on the outcome of the surveillance interaction games being considered. In both the studied games, we found that imposing a series of feasible enforcements can significantly improve the surveillance system's performance. However, there remain many open problems in this area:

1) considering adversarial, friendly, rational, and irrational adversaries in a common framework;
2) using the dynamics of adversary behavior for better sensor placement;
3) understanding multiplayer dynamics involving group with intragroup and intergroup constraints.

V. Conclusion

In this work, we have employed a game theoretic framework to model selfish adversaries in surveillance applications. We found that such a modeling of adversaries can provide us with performance bounds for surveillance systems and also provide prescriptive guidelines to improve the system performance. We further employed the "scenario engineering" approach to modify the scenario itself so that the surveillance system can perform better against the adversary. By studying two separate scenarios, one an indoor zero-sum game of monitoring an ATM lobby and another of an outdoor nonzero-sum game of traffic monitoring, we have studied the feasibility of the proposed ideas. The learnings resulting from the two scenarios have been summarized into a set of generic guidelines for system designers to consider while trying to improve the surveillance effectiveness.

To demonstrate the key ideas, we have currently modeled simple but practical scenarios. In the future, we hope to extend this work to more complex real-life surveillance scenarios involving multiple agents.

References

[1] W. Hu, T. Tan, L. Wang, and S. Maybank, "A survey on visual surveillance of object motion and behaviors," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 34, no. 3, pp. 334–352, Aug. 2004.

[2] M. Valera and S. A. Velastin, "Intelligent distributed surveillance systems: A review," in *IEE Proc. Vision, Image and Signal Processing*, 2005, pp. 192–204.

[3] M. Wu, W. Trappe, Z. J. Wang, and K. Liu, "Collusion-resistant fingerprinting for multimedia," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 15–27, Mar. 2004.

[4] E. Rasmusen, *Games and Information: An Introduction to Game Theory*. Malden, MA: Wiley-Blackwell, 2006.

[5] S. J. Brams, *Theory of Moves*. Cambridge, U.K.: Cambridge Univ. Press, 1993.

[6] A. Pentland, T. Choudhury, N. Eagle, and P. Singh, "Human dynamics: Computation for organizations," *Pattern Recognit. Lett.*, vol. 26, pp. 503–511, 2005.

[7] T. Kanter, "Event-driven, personalisable, mobile interactive spaces," in *Symp. Handheld and Ubiquituous Computing*, Bristol, U.K., 2000.

[8] V. K. Singh and M. S. Kankanhalli, "Towards adversary aware surveillance systems," in *IEEE Int. Conf. Multimedia and Expo*, 2007, pp. 2038–2041.

[9] M. J. Osborne and A. Rubenstein, *A Course in Game Theory*. Cambridge, MA: MIT Press, 1994.

[10] P. Paruchuri, J. P. Pearce, M. Tambe, F. Ordonez, and S. Kraus, "An efficient heuristic approach for security against multiple adversaries," in *Conf. Autonomous Agents and Multiagent Systems*, 2007, pp. 1–8.

[11] W. G. Simpson, "Unconscious bias in walking," *Nature*, vol. 29, pp. 356–356, 1884.

[12] C. Mohr, T. Landis, H. S. Bracha, and P. Brugger, "Opposite turning behavior in right-handers and non-right-handers suggests a link between handedness and cerebral dopamine asymmetries," *Behav. Neurosci.*, vol. 117, pp. 1448–1452, 2003.

[13] E. S. Robinson, "The psychology of public education," *Amer. J. Public Health*, vol. 23, pp. 123–128, 1993.

[14] A. Ghosh and S. Sen, "Theory of moves learners: Towards non-myopic equilibria," in *Conf. Autonomous Agents and Multiagent Systems*, 2005, pp. 74–80.

[15] A. K. Said and D. A. Hartley, "A hypergame approach to crisis decision-making: The 1973 middle east war," *J. Oper. Res. Soc.*, vol. 33, no. 10, pp. 937–948, 1982.

[16] R. Vane, "Advances in hypergame theory," in *Workshop on Game Theoretic and Decision Theoretic Agents—Conf. Autonomous Agents and Multi-Agent Systems*, Hakodate, Japan, 2006.

[17] A. Kerckhoffs, "La cryptographie militaire," *J. Sciences Militaires*, vol. 9, pp. 5–83, 1883.

[18] J. Wang, C. Zhang, and H. Shum, "Face image resolution versus face recognition performance based on two global methods," in *Asian Conf. Computer Vision*, Jeju Island, Korea, Jan. 2004.

Vivek K. Singh received the B.Eng. (Comp. Eng.) and M.Computing (part-time) degrees from the National University of Singapore in 2002 and 2005, respectively. He is working toward the Ph.D. degree in the Experiential Systems Laboratory, University of California, Irvine.

He earlier worked as a Research Assistant at the National University of Singapore. From 2002 to 2006, he was a Lecturer at the Institute of Technical Education, Singapore.

Mohan S. Kankanhalli received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Kharagpur, and the M.S. and Ph.D. degrees in computer and systems engineering from the Rensselaer Polytechnic Institute, Troy, NY.

He is a Professor at the School of Computing at the National University of Singapore. He is on the editorial boards of several journals, including the *ACM Transactions on Multimedia Computing, Communications, and Applications*, *ACM/Springer Multimedia Systems Journal*, and the IEEE Transactions on Multimedia.