Optimizing Mobile Asset Protection in Areas Where Protective Resources Are Limited

Barry Webster, William Arrasmith, and Lok Acharya

Abstract—**Protecting valuable assets that are not in fixed locations but rather are capable of being relocated from place to place is an endeavor that has a wide variety of applications. Assets could be military in nature, such as personnel or equipment, or civilian, which could encompass anything from cargo shipments to moving from one home to another. In cases where any of these assets find themselves under threat of attack, one would of course prefer to have sufficient protective resources to provide a reasonable level of security for the asset(s) at all times. However, there can be many cases where such protection is not possible. It may be too costly to provide constant protection. Or, it may be that an asset has a mandatory relocation time, and there are simply too few available resources to provide complete protection. It could even be the case that a portion of the available resources are required to protect an even more valuable asset elsewhere. This paper presents a methodology for optimizing the protection of an asset when it needs to be relocated and there are insufficient resources to provide protection at all points along its journey.**

Index Terms—**Agent-based simulation, game theory, mixed strategies, mobile asset protection.**

I. Introduction

Assets can be found all around us. It is safe to say that any group, as well as the individuals comprising that group, possess (or want to possess) items that they consider to be valuable. Any such items of value can be counted as assets. It could very well be the case that items accorded great value by one group (or individual) are considered to be of little or no value by another group/individual, and vice versa. However, since the items are valued by at least one group/individual, then those items are assets to whichever people value them.

Assets can be viewed in various ways. They could be items that increase the net worth of the holder, such as money or equipment or buildings. They could also be items that serve as tokens of someone's status or position within society, such as badges or licenses or keys. Assets can be seen as items that increase the standing of a group in a plenary fashion, such as flags or totems or relics. They can even be items that serve only to increase one's sense of well-being, such as photos or mementos or charms.

While assets provide some level of value to the holder, it can also be the case that there is another group/individual that wants to possess a particular asset for themselves, or for some reason simply does not want that asset to be possessed by the current holder. In such situations, the group/individual not possessing the asset may derive value by taking possession of the asset and becoming the new holder, or destroying it to prevent the current holder from possessing it any longer.

It is these types of situations with which this paper is concerned. That is, this paper addresses situations in which one party possesses a particular asset, and another party wishes to appropriate that asset for themselves or destroy it. The party possessing the asset will of course wish to protect it against capture or destruction. To do so, that party will need to have access to resources capable of providing such protection.

If sufficient security resources can be acquired such that the asset in question can be protected at all times, the problem of protecting the asset becomes moot. It becomes a case of simply allocating the necessary resources to the asset, and a constant, uninterrupted level of protection is provided. However, there are many situations in which resources sufficient to provide constant protection are not available. Examples of such situations include:

- Sufficient resources could be made available, but to allocate them so as to provide complete protection for the asset would not be cost-effective. This could be the case if an asset of only moderate value is going to be mobile for a long time and/or distance (perhaps moving cross-country), and the cost of providing complete protection for the entire trip exceeds the value of the asset.
- Sufficient resources are not available at the present time, but the asset must be transported immediately anyway. This could happen if there is an unanticipated need to relocate the asset while the protective resources are tied up elsewhere, such as the need to ship medical supplies in the face of a medical emergency.
- Sufficient resources are not available either at all or for a long term. This could be because sufficient protective resources simply are not available at all, or they are currently assigned to another asset which is considered to be of greater value.

If situations such as these arise, there will be assets that are going to be transported and will be in need of protection, yet there will not be sufficient resources to provide complete protection throughout the entire trip. For those events, a method will need to be devised to optimize the use of whatever resources will be available in order to provide the maximal amount of protection given the limitations of the protective resource availability. It is the development of this optimal resource allocation methodology that is the focus of this paper.

II. Background for the Scenario

The work done for this paper builds on the work done for two previous papers dealing with intrusion detection [1], [2].

Manuscript received January 3, 2016; revised February 28, 2016.

The authors are with the Department of Engineering Systems at the Florida Institute of Technology, Melbourne, FL 32901 USA (e-mail: bwebster@fit.edu, warrasmi@fit.edu, lokprasadacharya@gmail.com).

DOI: 10.7763/IJMO.2016.V6.502

In the first work, a methodology was discussed for using very small Unmanned Aerial Vehicles (UAVs), called *micro-UAVs*, to detect intruders across large areas, where it is not possible to patrol the entire area all at once [1]. In the second work, a methodology was discussed for optimally deploying infrasound detectors to interdict intruders attempting to attack an asset from potentially a number of different approach paths of varying degrees of difficulty [2].

In these two previous works, the focus was on using various technologies in combination with optimization techniques to detect intrusion attempts against an asset. It also was the case in both works that the assets in question were static, i.e. in a fixed position and non-moving. Here, several of the concepts that played a role in the previous works (e.g. optimal usage of limited resources and preventing intruders from exploiting discernable patterns in resource deployment) are still meaningful and are incorporated, but the focus shifts from intrusion detection to intrusion prevention, and from static assets to mobile assets.

In order to be able to determine the optimal use of protective resources for mobile assets, it is necessary to create a framework in which to study the problem. There are a limitless number of potential frameworks that could be used, and obviously it would be impossible to conduct studies on even the majority of them. Rather, it is necessary to have an operating scenario that is generic enough that it can be applied to a wide variety of real-world situations, yet specific enough that it adequately represents the problem domain. It is also necessary to make some simplifying assumptions when creating the operating scenario, but not to the extent that the scenario no longer reasonably reflects reality.

Fortunately, this can be accomplished through the judicious selection of a model to implement the scenario. Models are highly stylized and simplified representations of real situations, yet are still capable of providing a great deal of insight into the scenarios for which they are created. For example, regression models of system behavior are frequently well off target when used as predictors of future results of the operation of the system. So, if they are so often wrong in their predictive capacity, then what is the point of using them? The answer is that even if the model is almost always unable to correctly predict future outcomes, it is still capable of providing the researcher with highly useful information, such as which factors contribute the most to system performance, and how sensitive the system behavior is to perturbations in factor values.

Thus, for the purposes of this paper a scenario was created, and a model representing that scenario was constructed in order to conduct tests of the operations of the scenario. The scenario created is as follows: we posit a vehicle, carrying an asset of some arbitrary value. The vehicle is transporting the asset from a given starting location to a given destination, through territory that is known to harbor persons who would like to see the asset either captured or destroyed. These “hostiles” will attempt to intercept the vehicle before it can reach the designated destination. If this happens, the asset is considered lost and the trip has failed. If the vehicle manages to reach the designated destination with the asset intact, the trip has succeeded. Resources are available to provide protection for the asset, but the number of resources is insufficient to provide protection for the asset at all times.

As mentioned previously, some simplifying assumptions are necessary to make the scenario workable, provided that these assumptions do not render the scenario unrealistic. Here it is assumed that the vehicle is travelling along a straight path from its origin to its destination. Though paths taken by mobile assets in reality are likely to be anything but purely straight, the assumption is still valid because the protection of a mobile asset is not a function of the shape of its path, but rather of the characteristics of that path.

This leads to the next assumption. It is assumed that there are several points along the path (called *waypoints* for identification purposes) where the vehicle could potentially be attacked by hostiles. Outside of these waypoints, the vehicle is not at risk of being attacked. This assumption is valid because travel paths followed by mobile assets may often pass through areas of terrain (such as mountainous or watery regions) where only certain portions of the path are suitable for mounting an attack against a moving vehicle. A related assumption is that the vehicle is travelling at a constant speed, which is typical for convoys or vehicles carrying larger assets (e.g. machinery).

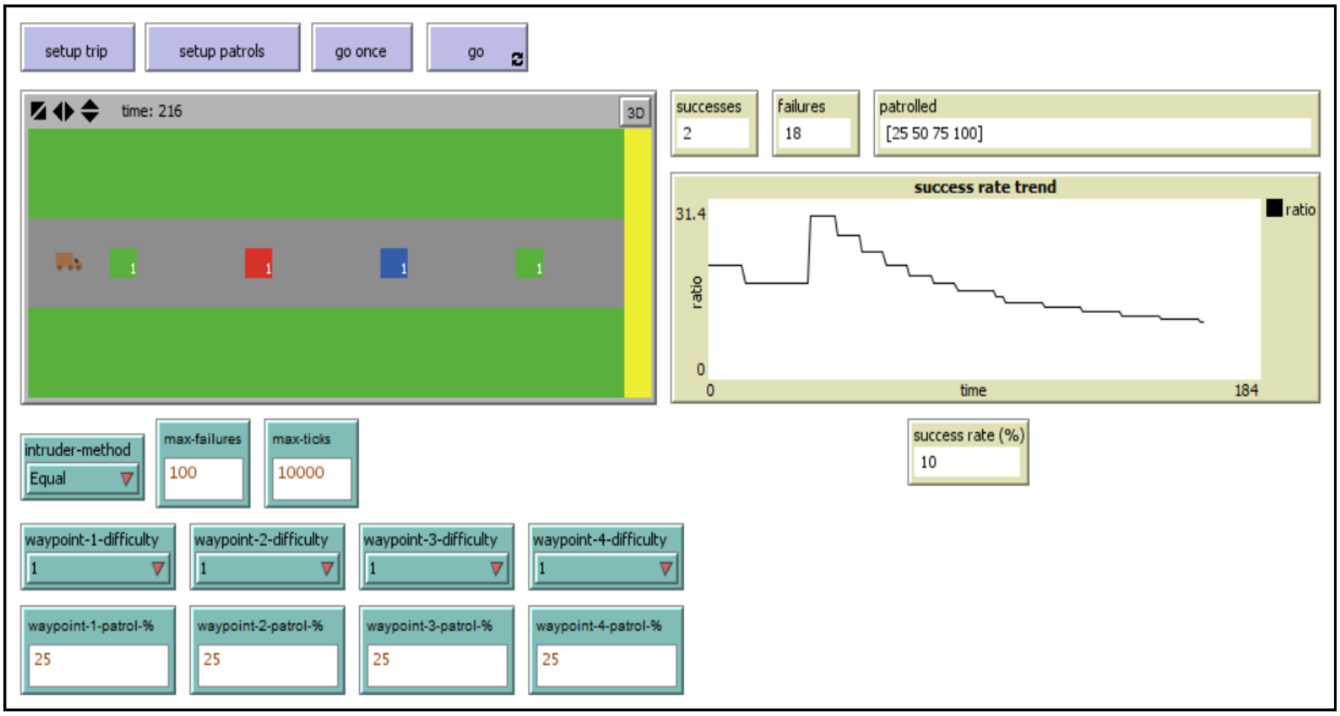
Another assumption is that if protective resources are deployed at a given waypoint, the vehicle is invulnerable to attack. Conversely, if no protective resources are deployed at a waypoint and an attack occurs, the attack will always succeed. These assumptions were made to avoid unnecessarily complicating the scenario with extensive probabilistic calculations to determine if an attack is successful. In other words, the point of the scenario is to attempt to maximize the likelihood that protective resources will be deployed at waypoints where attacks occur, not the precise probability of success of those attacks.

There is no distinction made as to the exact nature of the available protective resources, or the technologies that are used by those resources to provide protection for the asset. They are simply resources of some kind that are capable of protecting the asset from capture/destruction if they are deployed where an attack occurs. One distinction that does need to be made is that whatever the nature of the protective resources, they cannot be transported along with the asset. This reflects both the fact that one of the basic tenets of this paper is that constant protection of the asset throughout its journey is not available, and the fact that in many cases, protective assets capable of providing protection against a well-equipped intruder would need to be such that they could not be carried by the vehicle.

Given the aforementioned framework and accompanying assumptions, we have a scenario that is reasonably generic yet realistic, and which can be used to test methodologies for optimizing the deployment of available protective resources. The next step was to construct a model that accurately reflected the scenario.

III. Analyzing the Scenario

Given the nature of the scenario as defined, it was decided that an agent-based simulation model would be appropriate for analyzing the scenario and evaluating protective resource optimization methods. An agent-based simulation is one in which, rather than modeling a sequence of events that occur in a particular order, a collection of entities, or *agents*, is defined. Each agent is created with a predefined set of behaviors that it is capable of performing. The agents exist within an "open world" environment, in which they can potentially encounter other agents and interact with them over time. When interactions occur, the involved agents will participate according to their behaviors. So, for example, if one agent's behavior is such that it seeks to acquire money, then whenever that agent encounters another it will ask that other to give it some money – perhaps a particular quantity, perhaps all that the other agent has.



time: 216

successes 2

failures 18

patrolled [25 50 75 100]

success rate (%) 10

intruder-method Equal

max-failures 100

max-ticks 10000

waypoint-1-difficulty 1

waypoint-2-difficulty 1

waypoint-3-difficulty 1

waypoint-4-difficulty 1

waypoint-1-patrol-% 25

waypoint-2-patrol-% 25

waypoint-3-patrol-% 25

waypoint-4-patrol-% 25

Fig. 1. *NetLogo* interface.

In addition to interacting, agents can produce other agents, and they can also "die" and be removed from the simulation environment if certain specified conditions are met. The process of producing other agents, as with interacting, occurs according to an agent's defined behavior for doing so. It may produce duplicates of itself, or "hybrids" consisting of some of its own traits combined with some from other agents with which it interacts, or completely new agents having new traits.

An agent-based simulation is ideal for modeling the defined scenario, since that scenario consists of a series of interactions between the vehicle carrying the asset, the protective resources, and intruders seeking to gain access to the asset. Each of these actors has a clear objective that it is trying to achieve, so defining their respective behaviors is straightforward.

The particular mechanism chosen to implement the simulation is a tool called *NetLogo* [3]. NetLogo is a self-contained agent-based simulation environment, consisting of a graphical user interface (GUI) builder and a facility for programming the operations of the simulation. It has facilities for constructing the "world" of a simulation as well as a wide variety of GUI components and reporters for monitoring and tracking the state of the simulation. It also has its own programming language, and an extensive library of simulations that can be referenced.

The GUI designed for the simulation is shown in Fig. 1. Along the top left of the GUI are four buttons that are used, respectively, to initiate a pathway for the mobile asset as defined by the user, to initiate a plan for protecting the asset, to step through the simulation one iteration at a time, and to run the simulation to completion.

Below these buttons is a window that depicts the path of the vehicle. The vehicle is shown as a truck icon moving along a roadway in the middle of the window. The boxes in the roadway are the waypoints, which have a number in their lower right corner that indicates the relative difficulty of attacking the vehicle at that waypoint (a higher number indicates greater difficulty). The boxes are color-coded to indicate if there is no intruder attacking at that waypoint (green), there is an intruder attacking at an unguarded waypoint (red), or the waypoint is being protected (blue). The vertical stripe at the right of the window indicates the destination of the vehicle. To the right of this window are reporters that show statistics for the simulation, including: total number of successful trips, total number of failed trips, cumulative probabilities of each waypoint being protected, a running graph of the success rate for getting the asset to the destination, and the current overall success rate.

In the lower left of the GUI are the user-definable parameters for setting up the simulation. Included here are: the method that intruders will use for selecting a waypoint to attack, the maximum number of trip failures that can occur before the simulation will automatically terminate, the maximum number of "ticks" of the simulation clock that can occur before automatic termination, the difficulty rating for each waypoint, and the percentage of time that each waypoint will be protected by protective resources.

In this version of the simulation, there are four waypoints. To simulate the limitations on the protective resources, one waypoint will be selected by intruders to be attacked, and one waypoint will be selected to be protected, for each trip of the vehicle. To run the simulation, the user selects values for the intruder attack method (which can be random, proportional according to the relative difficulties of the waypoints, or optimal according to a mathematical formula which will be discussed in the next section), the maximum number of trip failures, the maximum number of ticks of the simulation clock, and the difficulty ratings for each waypoint (which are integers ranging from one to four).

Once these values have been set, the user clicks on the "setup trip" button. This will create the pathway for the vehicle to take in transporting the asset. The user can then decide on a plan for how often to protect each waypoint with the one available protective resource. This is where the optimal ratio of waypoint protection can be calculated, the method for which will be discussed in the next section. The percentage of time that the protective resource will be assigned to each waypoint is entered, at which point the user clicks on the "setup patrols" button to enter the protection plan into the simulation.

The user can then elect to step through the simulation one tick of the simulation clock at a time (by repeatedly clicking on the "go once" button), or allowing the simulation to run to completion by clicking on the "go" button. The simulation itself then consists of repeated attempts of the vehicle to transport the asset along the pathway as defined and reach the destination without being successfully attacked. As the vehicle moves along the pathway, it will of course have to pass through each of the waypoints before reaching the destination. If the vehicle reaches a waypoint that the intruder has not selected for attack, it simply passes through the waypoint and continues. If it reaches a waypoint that is currently being protected, again it passes through that waypoint and continues. If it reaches a waypoint that is targeted for attack by the intruder and is not currently being protected by the available protective resources, the asset is lost and the trip fails. If the vehicle succeeds in passing through all waypoints and reaching the destination, the trip succeeds.

At the conclusion of each trip, the vehicle is returned to the starting point and another trip commences. This process continues until either the defined maximum number of failed trips occurs, or the defined maximum number of ticks of the simulation clock have occurred. Each trip is conducted under the same parameter settings, and this repetition is allowed so as to be able to determine an average asset transportation success rate for the pathway as defined, which is shown in the reporters to the right of the simulation. In this way, any number of different configurations of pathways can be defined and tested, and for each configuration, any number of protection plans can be defined and tested. Having defined the operating scenario and created a simulation model to implement that scenario, the next step was to use the model to test methods for optimizing the success rate of transporting the asset.

IV. Results of the Scenario

To validate the model and gauge whether it was operating correctly, an initial series of tests was conducted in which each waypoint was assigned the same difficulty rating and the same likelihood of being protected, and the intruder was set to choose a waypoint to attack at random. In this configuration, for each trip of the vehicle one of the four waypoints would be selected at random to be protected, and one of the waypoints would also be selected at random to be attacked. Given this configuration, it would be expected that one out of four times the waypoint selected for protection and the waypoint selected for attack would be the same, resulting in a predicted asset transportation success rate of 25 percent. If the model was operating properly, then it should report an average success rate of close to 25 percent, and indeed, test runs yielded success rates within one percentage point of 25, which provided confidence that the model was functioning properly.

At this point, the model could be used to assess the effectiveness of protection plans for the asset. But, why is it that the protection plans are expressed in terms of the percentage of time in which each waypoint will be protected? The answer relates to the fact that there are insufficient protective resources to simultaneously protect all the waypoints in the asset's transportation path (for the simulation, this is reflected by having only one protective resource for four waypoints). This is the main focus of this paper, but again, why is it necessary to define percentages of time that each waypoint will be protected?

In reality, suppose that we decide that we will always deploy whatever protective resources are available to protect a particular set of waypoints (perhaps the ones that are easiest for the intruders to attack). If we do this, then in a short amount of time the intruders will realize that it is always the same set of waypoints that is being protected, and will just attack one of the waypoints that they know will be unprotected. Likewise, suppose that we rotate the available protective resources around the waypoints in a regular fashion. Again, the intruders will be able to discern that the waypoints are being protected according to a pattern, and they will follow the pattern to attack waypoints that they know will not be protected at a given time. Thus, if we are to maximize the likelihood that the asset will be successfully transported, we cannot deploy the available protective resources according to any predictable pattern.

This makes it sound as if each time an asset is transported along a given pathway, we should just randomly select waypoints to be protected according to the available protective resources, and all other things being equal that is in fact the case. However, this assumes that all waypoints are equally likely to be attacked, and as alluded to earlier there are many situations in which this is not true. It could easily be the case that some waypoints are easier to attack than others, meaning that intruders would be more likely to attack these waypoints than ones where they would have a much harder time in mounting an attack. However, as we have seen, even if some waypoints are more likely to be attacked we cannot always deploy the available protective resources to protect those waypoints, or even protect them according to a predictable pattern, as this will invite failure.

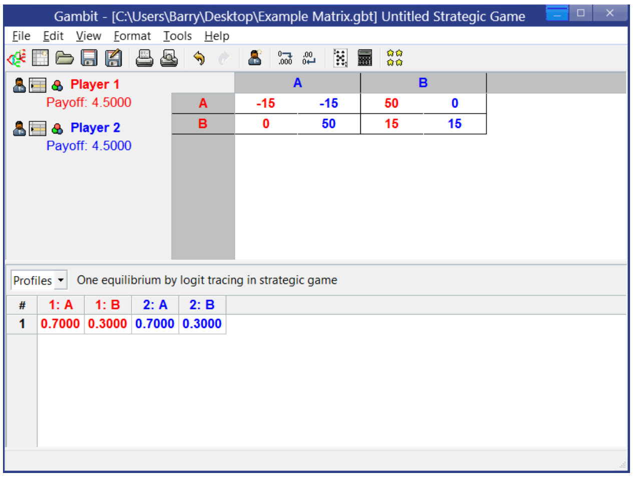
So, it is clear that whatever protective resources are available, if these resources are insufficient to simultaneously protect all waypoints at all times, then it will be necessary to randomly deploy the protective resources to the waypoints at various times. In doing so we will not allow intruders to have any *a priori* knowledge of which waypoints will be protected at a given time. But, the fact remains that some waypoints may be more likely than others to be targeted for attack, so even if intruders do not know beforehand which waypoints will be protected, they still will be more likely to want to attack the preferred waypoints. Thus, if we randomly deploy the protective resources in equal measure, the waypoints that are more likely to be attacked will be assigned protection less often than they should, and we still will not achieve the optimum asset transportation success rate possible.

Given these facts, is it possible to guarantee that the optimal deployment ratio of the available protective resources for a given pathway can be achieved? The answer is yes, and can be found in the use of *mixed strategies*. The use of mixed strategies is an element of the field of game theory, which is the systematic study of decision-making where a decision made by one party depends in large part on the decisions made by other parties participating in the same situation. That is definitely the situation here, as the decision of where to deploy the available protective resources depends in large part on which waypoints the intruders are likely to attack, and the choice of which waypoints to attack depends in large part on which waypoints will be protected.

The use of mixed strategies allows us to mathematically determine the optimal ratio at which to deploy the available protective resources by maximizing the *expected value* of the asset transportation success rate [4]. That is, the deployment ratio will be set such that the success rate achieved over time will be the same regardless of which waypoints the intruders choose to attack [4]. What this does is to make the intruders *ambivalent* to choosing which waypoints to attack, since no matter what they choose, the success rate over time will be the same [4]. Thus, we do not need to know what waypoints the intruders are planning to attack, nor do we need to care. By following the calculated mixed strategy, the success rate will be maximized.

But, how do we know that this specific deployment ratio as determined by calculating the appropriate mixed strategy is in fact optimal? To answer this, we need to see what happens if we use any deployment ratio other than the one that the mixed strategy tells us is optimal. We have already seen that the mixed strategy was calculated such that no matter what the intruders decide to do, the expected value of the asset transportation success rate is the same. If we use any other ratio, then the expected values for the success rate under the different attack plans that are possible for the intruder *must* no longer be the same. This in turn means that the expected value for the success rate under at least one attack plan must be better than it is for other attack plans.

If the expected value of the asset transportation success rate for a particular attack plan is less than for another plan, then the intruder should *always* follow one of the attack plans that carries the lowest expected success rate, in order to minimize the success of transporting the asset. But, if the intruder is always following a particular attack plan, then the available protective resources can always be deployed to counter that plan. That is, the intruder will always be attacking the same waypoints, so the protective resources can always be deployed to those waypoints. But then, if the protective resources are always being deployed to the same waypoints, then we are right back where we started. The intruders will adopt a different attack plan to counter the current deployment plan, which will then need to itself be countered, and so on, and we will always be in pursuit of countering what the intruders are doing, and thereby never achieving the best success rate. Thus, it is *only* when the optimal mixed strategy is being followed that the asset transportation success rate can be guaranteed to be optimal [4].


Gambit - [C:\Users\Barry\Desktop\Example Matrix.gbt] Untitled Strategic Game
File
Edit
View
Format
Tools
Help

Player 1
Payoff: 4.5000

Player 2
Payoff: 4.5000

	A		B	
A	-15	-15	50	0
B	0	50	15	15

Profiles ▾ One equilibrium by logit tracing in strategic game

#	1: A	1: B	2: A	2: B
1	0.7000	0.3000	0.7000	0.3000

Fig. 2. Example gambit interface.

Knowing this, the optimal mixed strategy can be calculated for any situation such as this in which a mixed strategy can be used to find the best way to randomly select decision options. These calculations can be done by hand; however, this can become a complicated process, particularly if there are more than four possible options that can be followed. Because of this, a tool called *Gambit* was used to help find the optimal mixed strategies for the simulation [5]. An example of the Gambit interface is given in Fig. 2.

To use Gambit, a matrix is created having one dimension for each participant. Within each dimension are listed all of the available options for the participant with which the dimension is associated. Entries within the matrix are then made representing the *payoffs* associated with each particular combination of options for each participant. A payoff represents the relative value of an outcome to a given participant, usually expressed as ordinal numbers where positive numbers indicate desirable outcomes, negative numbers represent undesirable outcomes, and zero values represent that the status quo has been preserved (i.e. the overall satisfaction of the participant has not changed as a result of the outcome). Once the matrix is constructed, Gambit will calculate the optimal mixed strategy based on the contents of the matrix. In the example shown in Fig. 2, there are two participants (Player 1 and Player 2), each with two possible decision options (A and B), and thus we have a 2x2 matrix. In each cell of the matrix, the first number listed is the payoff for Player 1 (the “row” player), and the second number listed is the payoff for Player 2 (the “column” player). Based on the participants, possible options, and payoffs given in the matrix, Gambit has calculated that in order to achieve the optimal expected payoff, both Player 1 and Player 2 should choose the “A” option 70 percent of the time, and the “B” option 30 percent of the time. These values are shown in the lower half of the interface.

Even given the fact that the operational scenario defined for this paper was a simplified representation of potentially real situations, and also that the use of tools such as NetLogo and Gambit rendered the testing of the scenario substantially easier, exhaustive testing of the scenario remained all but impossible. The model defines four waypoints, each of which can be assigned one of four levels of difficulty. This amounts to 4^4, or 256 possible configurations of just the waypoints themselves. In order to exhaustively test the scenario, each of these configurations would have to be tested against all possible protective resource deployment plans. Even if these plans were restricted to the use of only integer percentages for the deployment ratios, that would still result in 100^4, or 100,000,000 different possible plans, for a total of a minimum of 2.56 billion different tests that would need to be run if we are to prove that the calculated ideal mixed strategy can be shown through simulation to be in fact optimal. Each of these tests would also need to be repeated in order to obtain viable average asset transportation success rates that could be compared to make this determination.

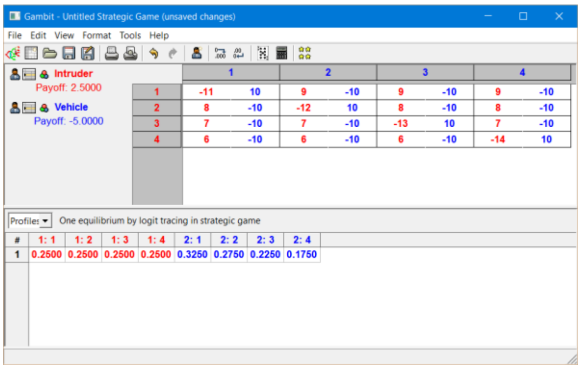
Clearly, such testing is well beyond the realm of feasibility. Thus, some representative sample configurations were tested so as to observe if the calculated mixed strategy showed indications of optimality. One of those tests was the one already mentioned, which was to assign the same difficulty rating to all waypoints, and deploy the protective resource to each waypoint with the same frequency. This gave a baseline performance indicator, which showed what sort of asset transportation success rate could be expected in a completely randomized configuration. As discussed, these tests resulted in an average success rate reading of almost exactly 25 percent, which is as expected.

The other set of configurations that were tested were chosen for a specific reason. In these configurations, each of the waypoints was assigned a different difficulty rating. To calculate the optimal mixed strategy, the following payoff structure was assigned:

- The asset was accorded a value of 10.
- If the intruder was successful in attacking the asset, they would receive a payoff of the value of the asset minus the difficulty rating of the waypoint where the attack occurred. So, for example, if a successful attack occurred at a waypoint with a difficulty rating of 2, then the payoff to the intruder would be 10 – 2 = 8.
- If the intruder was not successful in attacking the asset (i.e. the waypoint selected for attack was protected), they would receive a payoff of -10 minus the difficulty rating of the waypoint. So as before, if the waypoint attacked had a difficulty rating of 2, but was guarded by the protective resource, the attack failed and the intruder would receive a payoff of -10 – 2 = -12.
- For the vehicle, if it succeeded in reaching the destination with the asset intact, it received a payoff of the value of the asset, or 10.
- If the vehicle underwent a successful attack, the asset was lost so the payoff would then be -10.

The configuration details, along with this payoff information, were entered into Gambit, and an optimal mixed strategy was calculated. The Gambit matrix and solution are shown in Fig. 3. The calculated optimal mixed strategy for the intruder, given in red at the left of the solution in the bottom half of the interface, reveals why this particular set of configurations and payoffs were selected for testing. Note that the values given for the frequencies at which the intruders should choose to attack each of the four waypoints are all the same. That means that the intruder can choose to attack each waypoint with equal probability. In other words, we can simply choose which waypoint will be attacked by the intruder for a given trip at random. This greatly simplifies the problem, and allows us to focus on testing only the calculated mixed strategy for the protective resource.

These values are given in blue at the right of the solution in the bottom half of the interface, and show that the calculated optimal mixed strategy for protecting the asset is to protect the waypoint with the lowest difficulty rating 32.5 percent of the time, the waypoint with the second lowest difficulty rating 25.5 percent of the time, the waypoint with the third lowest difficulty rating 22.5 percent of the time, and the waypoint with the highest difficulty rating 17.5 percent of the time.



Intruder
Payoff: 2.5000

Vehicle
Payoff: -5.0000

	1		2		3		4	
1	-11	10	9	-10	9	-10	9	-10
2	8	-10	-12	10	8	-10	8	-10
3	7	-10	7	-10	-13	10	7	-10
4	6	-10	6	-10	6	-10	-14	10

One equilibrium by logit tracing in strategic game

#	1: 1	1: 2	1: 3	1: 4	2: 1	2: 2	2: 3	2: 4
1	0.2500	0.2500	0.2500	0.2500	0.3250	0.2750	0.2250	0.1750

Fig. 3. Gambit solution for test configuration.

Intuitively, these values make sense since attacking waypoints with lower difficulty ratings result in higher payoffs to the intruder if the attack is successful, so waypoints with lower difficulty ratings would tend to be preferred by the intruder and thus should be protected more often, but is there any evidence that using this mixed strategy results in better asset transportation success rates than would be obtained at random? Repeated runs of the simulation resulted in success rates as high as 31.03 percent, with an overall average of 27.354 percent across all runs. These numbers are not dramatically higher than random, but they are in fact higher. Given that the protective resource is at a substantial disadvantage to begin with (one resource to protect four waypoints), *any* increase in the asset transportation success rate would be desirable.

V. Conclusion

It is clear that to optimize the asset transportation success rate for transporting mobile assets through hostile areas with limited access to protective resources cannot be accomplished by dedicating those resources only to some waypoints exclusively, or by rotating the deployment of those resources according to any discernable pattern. Optimizing the success rate can only be accomplished through deploying the protective resources probabilistically. However, this should not be done in a completely random fashion, without concern for the environment in which the asset is being transported.

Though not conclusive, evaluating the efficacy of the optimal mixed strategy through the simulation provided evidence that using optimal mixed strategies to decide how often to deploy available protective assets to the various waypoints yields better asset transportation success rates than other random methods. This corroborates what the mathematics were indicating from the beginning.

Thus, a recommendation can be made that optimizing protection of mobile assets can be accomplished by calculating an optimal mixed strategy for the particular pathway over which the asset will be transported, and then deploying the available protective resources according to that mixed strategy. That being said, there are a number of ways in which the work done for this paper can be extended.

The first extension that could be done would be to do additional testing. Though it has been shown that exhaustive testing is not feasible, additional testing of other scenario configurations certainly would be, given that the initial testing has indicated that using the optimal mixed strategy technique is useful for the configurations tested. Other extensions that could be made include:

- Allowing for variable numbers of waypoints to be represented in the simulation
- Allowing for protective resources to be able to cover more than one waypoint at a time in the simulation
- Allowing for the representation of additional methodologies that can be used by the intruder in determining which waypoint(s) they will attack
- Allowing for multiple attacks to occur along the vehicle’s pathway in a given trip
- Develop and integrate a model for the probability of a successful attack given factors such as weapon’s class, sensor availability, attack strength, defense strength, motivation, surprise, and training level

In short, there is plenty of room for additional research to be conducted in this area. However, one thing that is certain is that regardless of whether some or all of the extensions listed are performed, all of them will still need to include the optimal mixed strategy methodology as part of their operations.

REFERENCES

[1] B. Webster and W. Arrasmith, "Optimal systems engineering driven search and scan pattern determination for detecting non-cooperative moving ground targets using micro-UAV "swarm" concept and game theory," in *Porc. International Conference on Innovative Technologies (IN-TECH)*, Rijecka, Croatia, 2013.

[2] B. Webster, W. Arrasmith, and L. Acharya, "Infrasound-based intrusion detection with game theoretic resource optimization," *International Journal of Modeling and Optimization,* vol. 4, no. 3, pp. 182-187, 2014.

[3] U. Wilensky. (1999). NetLogo. center for connected learning and computer-based modeling. Northwestern University, Evanston. [Online]. Available: http://ccl.northwestern.edu/netlogo/

[4] A. K. Dixit, S. Skeath and D. H. Reiley, "Simultaneous-move games: Mixed strategies," *Games of Strategy*, New York, NY: W. W. Norton & Company, Inc., 2004, pp. 214-270.

[5] R. D. McKelvey, A. M. McLennan, and T. L. Turocy. (2014). Gambit: Software tools for game theory, version 14.1.0. [Online]. Available: http://www.gambit-project.org

Barry Webster was born in Elmira, NY on May 19, 1963. He earned a B.S. in computer science from the Pennsylvania State University in University Park, PA in 1984. He went on to earn an M.S. in computer science in 1995, a Ph.D. in computer science in 2004, and an M.S. in systems engineering in 2005, all from the Florida Institute of Technology in Melbourne, FL.

He began his career in 1985 working as a systems engineer for Grumman Aerospace Corporation on Long Island, NY. He spent a total of 21 years with the company (which eventually became Northrop Grumman Corporation), holding positions in systems, software, and support engineering departments, ultimately becoming the senior database administrator for the engineering directorate. In this capacity, he was responsible for managing the operation of over 50 databases and associated applications and tools, used at installations around the world. After relocating to Melbourne, FL in 1987 he became associated with the Florida Institute of Technology, first as a student, earning three graduate degrees while working full time, then as a researcher on a sponsored program, and then as an adjunct professor. In 2007 he made the transition to Florida Tech as a full-time member of the faculty within the Department of Engineering Systems (though still consulting for Northrop Grumman part-time for another three years), where he remains to the present day. As part of his Ph.D. studies, he was also accepted for a doctoral internship at NASA’s Ames Research Center in Mountain View, CA, where he worked in the Autonomous Systems Department on automated telescope control systems and algorithms for solving NP-Hard telescope scheduling problems. His research interests include artificial intelligence, decision theory, and game theory.

Dr. Webster is a member of the Association for Computing Machinery (ACM), the Institute for Operations Research and the Management Sciences (INFORMS), and the Game Theory Society (GTS). He has chaired international conference sessions in database management and artificial intelligence, received several citations for his work in database management, and three “Best Paper” awards for works on game theory.

William W. Arrasmith was born in Bad Aibling, Germany on 7 January, 1961. He received his Ph.D. in engineering physics from the Air Force Institute of Technology (AFIT) in Dayton, OH in 1995. He earned an M.S. in electrical engineering from the University of New Mexico in Albuquerque, NM in 1991. He obtained a B.S. in electrical engineering from Virginia Tech in Blacksburg, VA in 1983.

In his current position, he is a professor of Engineering Systems at the Florida Institute of Technology (FIT) in Melbourne, FL. Prior to FIT, he served in the United States Air Force for over twenty years, retiring with a rank of Lt. Colonel. During his time in the Air Force, he held several positions including chief, advanced science and technology division, applied technology directorate at the Air Force Technical Applications Center; assistant professor, weapons and systems engineering department, united states naval academy; program manager, physics and electronics directorate, Air Force Office of Scientific Research; director, Flood Beam Experiment, Air Force Research Laboratory (Kirtland Air Force Base); and project engineer, Teal Ruby Systems Program Office, Space Division. Recent related publications include William W. Arrasmith, E. Skowbo, and J. Olson, “An Overview of the Detection and Characterization of Man-Made Signals-of-Interest Using an Infrasound Array,” Budapest, Hungary: IN-TECH 2013 Conference Proceedings, 2013; and Barry Webster, and William W. Arrasmith, “Optimal Systems Engineering Driven Search and Scan Pattern Determination for Detecting Non-cooperative Moving Ground Targets Using Micro-UAV “Swarm” Concept and Game Theory,” Budapest, Hungary: INTECH 2013 Conference proceedings, 2013 (Best Paper). His research interests include applied systems engineering, advanced sensing/detection techniques, and methods for imaging through atmospheric turbulence.

Dr. Arrasmith is a member of Phi Kappa Phi, Tau Beta Pi, and the American Society of Engineering Education (ASEE) and has two national and one international patent pending. He received the President’s Award for Service at Florida Tech in 2013 and the Walter Nunn Excellence in Teaching Award in the College of Engineering at Florida Tech in 2010.

Lok P. Acharya was born in Nepal on June 18, 1982. He holds a B.E. in computer engineering from Purbanchal University in Nepal, and an M.S. in electrical engineering from George Washington University in Washington, DC. He is currently a Ph.D. student in systems engineering at the Florida Institute of Technology in Melbourne, FL.

He is presently a database systems engineer at PCTEL Inc. in Melbourne, FL. He has held many positions in the past, including graduate research/teaching assistant, Information Technology Engineer, and Quality Assurance Engineer. His current research interests are in the areas of game theory and agent based modeling.

Mr. Acharya is a member of the IEEE.