Infrasound-Based Intrusion Detection with Game Theoretic Resource Optimization

Barry Webster, William Arrasmith, and Lok Acharya

***Abstract*—Intrusion detection is a concern for any asset worth protecting. Having the capability to perform such detection can help to prevent the theft of, damage to, tampering with, or destruction of a wide range of valuable assets. These assets could be objects stored within a location such as a vault or room, or they could be an entire building containing valuable objects, a campus consisting of several buildings, or even something as large as a national border. This paper presents a concept for an intrusion detection system based on the use of infrasound, a technology well suited for this purpose due to its ability to distinguish between different types of sound sources occurring within a given area. The paper also includes a discussion of a methodology, based on principles of game theory, for optimizing the resources used in the intrusion detection process.**

***Index Terms*—Applied game theory, infrasound, intrusion detection, resource optimization.**

I. Introduction

Anyone who is in possession of an asset considered to be of value to the owner would be interested in protecting the value of that asset. In some cases, this protection would amount to simply retaining possession of the asset, i.e. preventing the asset from being stolen. In other cases, the intent would be to protect the integrity of the asset. In such cases, one would want to prevent the asset from being tampered with, damaged, or destroyed. In still other cases, the goal would be to prevent access to the asset entirely, or at least to prevent access to the asset except under specific conditions.

In all of the cases just described, the asset(*s*) would benefit from some form of intrusion detection. Methods of intrusion detection are as varied as the types of asset protection required, and then some. An intrusion detection system could be as simple as having a solitary individual physically guard the asset, or as complex as having several different tools and/or techniques operating in concert to protect a very large asset (such as a national border).

In this paper, we will introduce an intrusion detection system based on the use of *infrasound*. In this system, the intrusion detection itself is done automatically via passive infrasound receivers. The actual protection of the asset(s) is accomplished by human agents assigned to perform the manner of protection required.

An additional element that will be presented in this paper is a methodology for optimizing the use of the available intrusion detection/asset protection resources. This methodology involves using techniques from the field of *game theory* to mathematically determine the optimal deployment of those resources in order to maximize their effectiveness with regard to the type of asset protection intended. These techniques can be used whenever the amount of available resources is of necessity insufficient to provide complete coverage of the entire area for which asset protection is desired, as would be the case in situations such as protecting a national border.

II. Scope of the Paper

A complete description of an intrusion detection system and associated asset protection mechanism would need to include a definition of the type of asset that needs to be protected and the level of protection required, along with specifications of the possible modes of intrusion that would have to be defended against and the manner in which the intrusion detection system would be deployed and operated. Many of the elements of such a system description would be unique to the situation in which the system would be applied, and the possibilities for the number and type of these situations are limitless. As it is the intention of this paper to introduce the concept of an infrasound-based intrusion detection system rather than explicitly design such a system for a particular situation, some simplifying assumptions are needed.

For the purposes of this paper, it will be assumed that there exists an asset that is considered to be of value and needs to be protected from intruders. The type of protection needed is that of limiting unauthorized and/or unnecessary access to the asset, but is not an "all-or-nothing" proposition. That is, our concern is not that the asset would be stolen or destroyed, in which case the value of the asset would be completely lost. Rather, the concern is that unauthorized/unnecessary access to the asset will in some sense diminish its value. This process is incremental, meaning that each unauthorized/unnecessary access does decrease the overall value of the asset, but this decrease is not total. If enough successful accesses occur, it may be the case that the overall value of the asset drops to zero, but this total loss of value will not occur as a result of a single (or small number) of accesses. This particular scenario is comparable to situations in areas such as facility access, land area access (e.g. a park or recreation area), and border protection.

Another assumption that will be made for this paper is that the asset and intrusion detection system are land-based. That is, the asset itself is maintained on land, and all approaches to the asset that could be taken by potential intruders are also over land. Though it is theoretically possible for

Manuscript received February 1, 2014; revised May 3, 2014.

The authors are with the Department of Engineering Systems, Florida Institute of Technology, Melbourne, FL 32901 USA (e-mail: bwebster@fit.edu, warrasmi@fit.edu, lacharya2006@my.fit.edu).

DOI: 10.7763/IJMO.2014.V4.370

infrasound-based systems to be successfully constructed and operated in undersea and airborne environments, the primary principles by which such systems would operate are the same as for a land-based application. Including undersea or airborne elements would thus add little to the ideas being presented herein, and would only serve to unnecessarily complicate the discussion.

III. Infrasound

Infrasound is sound that is produced at very low frequency levels (typically less than twenty Hertz [1]).These sounds are produced in conjunction with other, higher-frequency sounds as a result of the movement or other sound-producing activities performed by both animate and inanimate objects. Each type of activity performed by each type of object will produce an infrasound “signature” unique to that type of object and what it is doing. This property allows detectors tuned to the infrasound spectrum to make distinctions identifying the type of object and type of activity being performed. For example, a rock rolling down a hill, a human riding a bicycle down that same hill, and a dog running behind the bicycle will each generate distinct infrasound signatures allowing detectors the possibility of identifying them and what they are doing.

Infrasound detectors are capable of performing quite detailed identification operations. It is possible, for instance, to detect that a particular door within a building has been opened and closed (even if the person doing the opening/closing is attempting to do so very quietly). This is possible due to the extremely long wavelengths associated with infrasound emissions. The concept is similar to waves in the electromagnetic spectrum; long wavelengths such as those found in regular radio waves are easily capable of passing through the walls of buildings and being picked up, whereas shorter wavelengths such as those found in small wireless routers have a much more difficult time passing through the same walls. Due to the shortness of the frequencies of infrasound waves, the associated wavelengths are so long that even minute sounds (like the door opening/closing just mentioned) from well within the confines of walled structures can be detected from outside of those structures.

The detection capabilities of infrasound are limited primarily by the strength of the sonic signal and the infrasound system array geometry [1].Specifically, the range at which an infrasound detector is capable of detecting a signal is directly proportional to the total output emitted by the sound being produced. This total output is a function of the amplitude (volume) of the sound and its duration. A high output sound could be very loud but short (such as an explosion), or not as loud but long-lasting (such as a motorcycle or automobile engine running). A sound could also be periodic, consisting of a series of short duration components produced at interval (such as a person walking). In effect, a strong impulsive signal that is above the infrasound sensor’s noise floor can be detected, as can a weaker, repetitive signal that can be “averaged” out of the noise. To give some idea of these ranges, without de-noising methodsa person walking could be detectable at approximately five meters. With advanced signal processing methods, a motorcycle or automobile engine revving could be detectable at distances ranging to kilometers. Truly massive sound sources like an earthquake, erupting volcano, or nuclear detonation could be detectable from virtually any place on the planet.

Infrasound detectors are passive, meaning that they simply collect the sounds that reach them. As such, they can be quite small (some currently under development are capable of being reduced to approximately the size of an ice hockey puck). The actual categorization of the sound being received is accomplished by a secondary device that uses various algorithms to interpret the received signals.

Individual infrasound detectors are unidirectional; any sound occurring within range, coming from any direction, will be detected. It is also possible to combine individual detectors to form arrays. These arrays can be arranged so as to provide an element of directionality to the detection. In direction-finding applications, sounds detected by an array will be indicated to have originated within a cone expanding outwards from the array center. Depending on the detestability of the source, the number and location of arrays, the number of detectors in an array, and their configuration, the direction that a sound is coming from can be isolated to within a cone spanning as little as one degree [1]. The location of the origination of a sound can also be determined (to within some error) based on geometric array conditions, number of arrays, source frequencies, and signal strength [1]. In this application, we look only at the direction-finding aspect.

IV. Base System Concept

Given the assumptions and descriptions mentioned in the previous two sections, a concept for an infrasound-based intrusion detection system would be as follows: an asset (A) to be protected resides at a particular location (L). There exists a set of available approach paths (P_1 through P_n) by which it would be possible for an intruder to gain access to A. Infrasound detectors are deployed at intervals around the perimeter of L. The detectors are configured so as to provide a continuous web of detection capability across the area in which the detectors are deployed. This can be accomplished either by placing individual detectors close enough together such that there are no gaps in their detection fields, or by placing arrays of detectors such that their detection cones will overlap.

When an entity (E) approaches the perimeter of L, one or more of the detectors/arrays will register the approach and transmit the related data to a control center (C). Once there, the data will be analyzed to determine if E is in fact an intruder constituting a threat to A, or if it is harmless. For example, if an animal happens to approach L, C would be able to determine that the approaching entity is a non-human biologic, and thus of no concern. On the other hand, if a person or group of persons approaches L, or if a vehicle approaches L, C would be able to determine this as well and raise an alert of potentially suspicious activity.If an alert is raised, security personnel are dispatched to intercept E. If they are successful in apprehending E prior to E being able to reach A, then A has been successfully protected. Conversely, if E succeeds in reaching A, it must then be assumed that A has been compromised, and thus has not been successfully protected.

This concept of operations is very straightforward, and very robust. Given that the infrasound detectors are passive, and collect incoming sound events continuously, and also that they are positioned such that their detection capabilities overlap, any entity approaching the covered perimeter will be detected. Then, given the ability of the processing algorithms to identify entities based on their infrasound signature, there is a very high likelihood that a detected entity will be properly categorized as a threat or as harmless.

The primary challenge facing this type of system is not one of technology, but rather one of economics. That is, the relative success of the system depends largely on the amount of funding available. If the organization responsible for protecting A is able to expend the funds necessary to procure a sufficient number of infrasound detectors, then the chances of that organization being able to successfully protect A are very good. However, the definition of what constitutes a "sufficient number" of detectors is critical. If the covered perimeter around L is designed to be relatively small, then relatively few detectors will be required to provide complete coverage. But, recalling that the range of detection is directly proportional to the strength of the sonic signal, then a small perimeter also means that regardless of whether an intruder is on foot or in a vehicle, the amount of time between first detection and the intruder reaching A will be short. This could in turn mean that if the security personnel are engaged at another position, they may not have enough time to react to the intrusion and intercept the intruder before A is compromised. A larger perimeter means more time to intercept an intruder, but it also means more detectors will be required to provide complete coverage.

As of this writing, infrasound detection systems are still rather expensive. For this work, we presume that commercial grade low-end proximity infrasound array systems can be obtained at a cost of around $15,000, and that high-end geo-locating infrasound array systems can run upwards of $250,000. Purchasing these higher-end systems in bulk could be expected to bring the price per unit down substantially, but the total price would still be high since purchasing in bulk would obviously mean that many infrasound detection systems (a.k.a. detectors)would be purchased. In any case, the cost of these detectors would not be something that a small company would want to spend, or perhaps even be able to afford.

Another option for those organizations that want to use this type of system but that are unwilling or unable to spend the money to afford complete coverage would be to obtain enough detectors to cover only a portion of the approaches to A. This would of course significantly reduce the cost of the system, but it would also carry the obvious disadvantage that some of the approaches to A would be left uncovered. As undesirable as this may sound, there are instances where this option may actually be the only one that is feasible. If the intent is to protect something on the order of a national park or a border region, the sheer size of the asset to be protected would be such that the costs to purchase, operate, and maintain the detectors could be prohibitive, even for an organization the size of a national government.

In any situation in which this option is used, the approaches to A that are left uncovered would be in effect "blind spots" through which undetected intrusive activity could occur. This problem could be mitigated by deploying the available detectors along the approaches that are deemed to be at the highest risk of being chosen by potential intruders. However, even this has its limitations; potential intruders are sure to discover which approaches are covered and which are not, even if this is as a result of trial and error with a number of would-be intruders having been caught. Once this discovery is made, the system is rendered useless since intruders will always follow the approaches that are uncovered, even if those approaches are difficult to navigate.

It is obvious that any system configuration in which complete coverage is infeasible, and where the available detectors are deployed statically, will not work. Fortunately, the small size of the detectors allows for easy relocation. To avoid the problem of potential intruders knowing that certain approaches are always covered and certain others are always uncovered, the available detectors could be periodically moved to different sets of approaches. Though beneficial, this tactic does not necessarily remedy the problem. If the detectors are relocated to certain sets of approaches at predictable intervals, the problem remains. Since the relocations are predictable, potential intruders will still know which approaches will be covered at what times, and can once again simply avoid the approaches that are currently covered.

Thus, it is clear that periodic relocation of the available detectors is necessary, but this must not be done in any predictable fashion. The question then becomes how to manage the relocation process. Is there a "best" way to conduct the relocations? The answer is yes, and this is where game theory enters the picture.

V. Game Theory Application

Game theory can be defined as interactive decision-making amongst rational individuals. That is to say, game theory involves decision-making between individuals, or amongst groups of individuals, but in a particular sense. First, the decisions being made are *interactive*, which means that the decision made in a given situation by one individual/group depends in large part on the decision being made by the other individuals/groups involved in the same situation. Second, the individuals/groups participating in the situation are *rational*. This term is not used in the typical sense, i.e. being sane. Rather, it refers to the fact that all participants in a situation are seeking to maximize their benefit as a result of that participation, and whatever decisions they make will reflect that aim [2].

To illustrate this, we can consider the example just outlined in the previous section. To reiterate, we have an asset A at location L, with possible approaches $P_1 \ldots P_n$. We also have an intruder entity E who is attempting to access A via one of the available approaches. As mentioned, if the available infrasound detectors are deployed to a particular approach or approaches and never relocated, or are relocated according to a predictable pattern, potential intruders will discover this, after which any E will be successful in accessing A. To prevent this from happening, it will be necessary to relocate the detectors periodically in an unpredictable fashion.

If the detectors are being deployed in a predictable manner, then the decision by E of which approach to take to A depends solely on E's assessment of the worth of taking a particular approach. It can be safely assumed that the worth to E of taking an approach that is being covered by the detectors would be low, whereas the worth of taking an uncovered approach would be higher. If E is rational according to the definition just given, then approaches that are covered by the detectors will never be taken. The main point, though, is that this decision does not depend on what anyone else is doing. This means the decision is not interactive, and thus does not qualify as a game theoretic situation.

On the other hand, if the detectors are being deployed unpredictably, then the situation has changed. Now the decision of which approach to take *does* depend on what others are doing. If the security personnel decide to deploy detectors along approach P_x, then the worth to E of following P_x will be low. But, if the security personnel decide not to deploy detectors along P_x, then the worth to E of following that path will be higher.Thus, E must gauge which approach (es) the security personnel will decide to cover, and then attempt to take an approach that is uncovered. At the same time, the security personnel must gauge which approach E will attempt to take, and then ensure that this approach is covered.

This type of situation is referred to in game theory as a *zero-sumpursuit/evasion* game. A zero-sum game is one in which what is desirable for one player is undesirable for the other, and vice versa[2]. In this case, what is desirable for E is to gain access to A, which is undesirable for the security personnel. Likewise, what is desirable for the security personnel is to apprehend E, which of course is undesirable for E. As for the second aspect, a pursuit/evasion game is one in which one player (the pursuer) wants to be where the other player (the pursued) is, whereas the pursued player wants to be where the pursuing player is not[2]. In this case, the security personnel (the pursuers) want to place detectors along the approach that E (the pursued) will take, but E wants to take an approach that the security personnel have not covered.

In pursuit/evasion games, an ever-present problem is that when considering what to do, one must attempt to discern what the other player is thinking about doing, and of course the other player is attempting to accomplish the same thing[2]. This can lead to a vicious cycle of thought, with the players often resorting to intuition or guesswork when making their decisions. Fortunately, game theory provides a mechanism for breaking out of this vicious cycle that is more rigorous and sound than relying on guessing.This mechanism is known as a *mixed strategy*.

In game theory, a strategy is a complete plan of action for any decisions that will need to be made during the course of the game[2]. Due to the particular way the game plays out it may be the case that the game will end without needing to make certain decisions (e.g. as a result of one decision having been made, others might be rendered moot). Nevertheless, even though some decision points might never be reached, a complete strategy calls for the player to have a plan for what to do in the event that any possible decision points are reached. A *mixed* strategy is one in which the choice of action for a decision point is selected randomly from a list of possible actions[2].

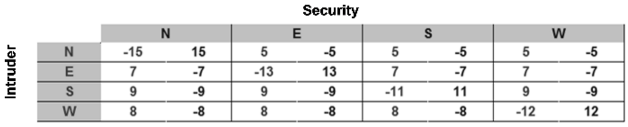
For this case, using a mixed strategy will take care of the problem of having a predictable method for relocating the available infrasound detectors. Security personnel would select which approach(es) to cover randomly, thus eliminating any pattern to which approaches will be covered and which will not. Security personnel could also randomize the time intervals at which the relocations are performed, thus making it impossible to predict when disruptions in coverage due to the relocations will occur. Using mixed strategies solves the problem of predictability, but the idea is to optimize the use of the available resources to maximize the ability to protect A.

This can be done by defining the mix ratio so as to make the *expected payoff* the same for all options available to the opposing player for a given decision. Here the expected payoff would be the relative worth of each decision option to the opposing player if that decision were to be repeated over time. By setting the expected payoff of all decision options the same, a mix ratio can be calculated that makes the opposing player ambivalent regarding which decision option to choose[2]. Since the expected payoff is the same no matter what action is taken, the opponent is forced into the position of having to develop a mixed strategy as well. If this is not done, then the opponent is not mixing and therefore must be playing according to a predictable pattern, which as we have seen leads to losing the game every time.

In [3] a simple example was given to show how an optimal mixed strategy could be calculated for a situation involving the deployment of small Unmanned Aerial Vehicles (UAVs), called micro-UAVs. That example can be adapted for use here as well. For the sake of this example, let us assume that there are four possible approaches to A; one for each of the cardinal directions of the compass. Let us further assume the following regarding the available approaches:

- The northern approach is quite treacherous, making it very difficult to traverse in order to reach A; this approach will have a difficulty rating of 5
- The eastern approach is moderately difficult to traverse; this approach will have a difficulty rating of 3
- The southern approach contains no obstacles or difficult terrain, and is thus very easy to traverse; this approach will have a difficulty rating of 1
- The western approach is slightly less difficult to traverse than the eastern approach; this approach will have a difficulty rating of 2

We can assign a value of 10 to A, representing the overall worth attributed to A by E. The net value of a successful intrusion attempt by E will then be the overall worth of A minus the difficulty of the approach taken to get to A (i.e. the value of accessing A diminishes with the amount of effort required to reach it).If E fails to access A and is apprehended, the net value of the attempt will be -10 (the negative value indicating a worth less than maintaining the status quo of not making the attempt, status quo being by convention typically valued at 0), minus the difficulty rating of the approach taken. Note that in all cases the numbers used here are *ordinal*, meaning that only the magnitude of the number matters; i.e.we can say that a value of 10 is better than a value of 5, but we cannot say that it is twice as good.To complete the example, one additional condition must be stated: we will stipulate that the security personnel have only enough equipment to cover one of the approaches at any given time. This satisfies the game requirement that there are insufficient resources to cover all four approaches simultaneously. The fact that only one approach at a time can be covered is again something that was done to keep the model simple. Any combination of one, two, or three paths being simultaneously covered could be modeled, but this would again unnecessarily complicate the example.



Security

Intruder	N		E		S		W	
N	-15	15	5	-5	5	-5	5	-5
E	7	-7	-13	13	7	-7	7	-7
S	9	-9	9	-9	-11	11	9	-9
W	8	-8	8	-8	8	-8	-12	12

Fig. 1. Example game matrix.

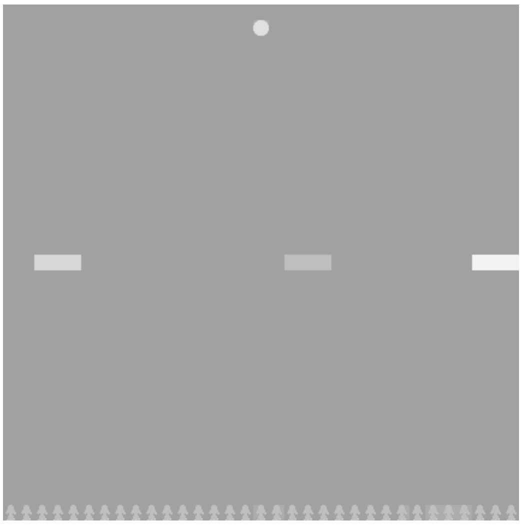


Fig. 2. Netlogooutput window.

Fig. 1shows the resulting game matrix. The intruder E is the “row” player, with payoffs listed first in each cell of the matrix. The security personnel are the “column” player, with payoffs listed second in each cell. The payoffs in each cell were determined according to the payoff calculation method just described in the previous paragraph. Note that in every cell, the payoff for one player is the negation of the payoff for the other player; which is a property of zero-sum games. The payoffs listed in each cell are for a single instance of the game. In order to find the optimal mixed strategy, it is necessary to find the expected payoff for each decision option, and then set the expected payoffs of all options for a given player equal to each other and find the mix ratio by solving the resulting set of simultaneous equations.

For the example, this was done by using a game modeling and analysis tool called Gambit[4]. The optimal mixed strategy obtained by solving the system of simultaneous equations gives the frequency at which the security personnel should place infrasound detectors to cover a particular approach path, and is as follows:

- The northern approach should be covered 13.75% of the time
- The eastern approach should be covered 23.75% of the time
- The southern approach should be covered 33.75% of the time
- The western approach should be covered 28.75% of the time

If the security personnel relocate the available detectors randomly in time and location such that the aforementioned ratios are maintained, they will maximize their potential for apprehending intruders, even as the intruders are simultaneously attempting to maximize their success rate (and even if the intruders know exactly what strategy the security personnel are following). It should come as no surprise that by doing so the security personnel are still at a disadvantage. Their overall expected payoff is -2.25, which stands to reason since there are four possible approaches to A, and only one at a time is being protected. Nevertheless, given the limitations in the example this expected payoff is the best they can hope to achieve.

VI. Experimental Model

A set of experiments was conducted to test the effectiveness of the game theoretic methodology outlined in the previous section, based on the work done in [3]. A test model was constructed using an agent-based simulator called NetLogo [5]. A picture of the model output window is given in Fig. 2. In this model, the asset to be protected is shown as a circle at the top of the output window. Possible approach paths to the asset (with accompanying user-assigned degrees of difficulty) are shown as rectangular boxes in the middle of the output window. Random intruders (shown as human figurines) were generated along the bottom row of the output window, and these intruders moved towards one of the available approach paths. If an intruder passed through an approach that was not currently being monitored, the intrusion was successful. Conversely, if the approach path was being monitored at the time the intruder passed through, the intrusion failed and the intruder was apprehended.

A number of different configurations of the model were included in the set of experiments. These configurations involved altering the number of intruders, the probabilities that a given intruder would select a particular approach path, and the frequencies at which the approach paths were monitored. A total of 10,000 experiments were run under the various configurations [6]. The data from the experiments included counts of total number of intruders generated, paths taken by the intruders, number of intruders apprehended, and number of successful intrusions. These data were then analyzed to check for statistically significant results.

VII. Conclusion

The results of the experimental model showed that the ratios of intruders apprehended to successful intruders were statistically consistent with the ratios predicted by the game theoretic analysis [6]. That is, the outcomes of the simulated intrusions using the NetLogo model were statistically the same as what the mathematical model said they should be. This provides evidence that the mathematical model used to calculate the optimal mixed strategy is reliable for use in real-world intrusion detection systems such as those described in [3] and herein. Since the mathematical model calculates which mixed strategy is optimal, and since there is evidence to support the notion that the mathematical model is applicable to actual intrusion detection scenarios, it is reasonable to infer that the game theoretic methodology would work if applied to an infrasound-based intrusion detection system as described in this paper.

There are many other avenues in this area that could be explored in future work. Investigations into differing configurations of infrasound detector arrays and their associated directional detection capabilities could prove interesting. Studies of the relationship between detector range and time of arrival of detected targets could be useful in helping to determine appropriate sizes for detector perimeters with respect to type of asset being protected. Different methods of using mobile assets (e.g. trucks) could also be investigated. In this paper, the mobile assets were used simply to transport the detectors during the relocation process. However, these mobile assets could also be used to enhance the identification and tracking of potential intruders. For example, arrays of detectors could be mounted on trucks. The trucks could then be moved to a location of interest and arranged so as to provide additional triangulation of target locations, which would allow for tracking the motion of targets and maintaining a history of their movements. Since the trucks are mobile, they could be quickly moved to areas of interest, allowing for tracking of targets along a much wider area than would be possible with fixed detectors.

Another possible direction that might be taken with this work could be to study the use of multiple platforms in the intrusion detection process. In [3] we discussed using micro-UAVs for this purpose. It could be possible to combine the use of the infrasound detectors, mobile arrays of detectors as just described, micro-UAVs, larger UAVs, and perhaps even others. One possible scenario would be as follows: a large-scale UAV, such as a Predator, would detect “hot spots” of potential threat activity at long ranges from the asset to be protected [7]. Mobile infrasound detector arrays would be moved to a position as close to a hot spot as possible to gather additional information. If an intruder does make a move towards the asset, the perimeter infrasound detectors would detect the incursion, and a “swarm” of micro-UAVs could be called in to provide visual indications of the nature of the intruder.

In sum, there is no shortage of additional work that could be done in this area. The concepts and principles described in this paper provide a foundation for developing and operating an infrasound-based intrusion detection system, upon which the additional work could build.

REFERENCES

[1] J. V. Olson and C. A. L. Szuberla, *Processing Infrasonic Array Data*, Springer Verlag, 2009.

[2] A. Dixit, S. Skeath, and D. H. Reiley, *Games of Strategy*, 3rd ed., New York: W. W. Norton & Company, 2009.

[3] 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 *Proc. the 2013 International Conference on Innovative Technologies (IN-TECH 2013)*, pp. 29-32, Budapest, 2013.

[4] R. D. McKelvey, A. M. McLennan, and T. L. Turocy.Gambit: software tools for game theory, version 13.1.1. [Online]. Available: http://www.gambit-project.org.

[5] U. Wilensky.Center for Connected learning and computer-based modeling, Northwestern University, Evanston, IL. [Online]. Available: http://ccl.northwestern.edu/netlogo/.

[6] L. P. Acharya and B. Webster, "Modeling game theory based non-cooperative search on moving targets using agent based simulation," *Internal Florida Tech paper - unpublished, Melboure*, FL, pp. 1-27, 2013.

[7] United States Government Accountability Office, Defense Acquisitions, Assessments of Selected Weapon Programs, Washington, DC: United States Government Accountability Office, 2013.

Barry Webster was born in Elmira, NY on 19 May 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. 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 conference sessions in database management and artificial intelligence, received several citations for his work in database management, and a Best Paper/Best Presentation award for a work 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, Florida, USA. Prior to FIT, he served in the united states air force for over twenty years culminating 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, 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 FIT 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.