

Risk and Decision Analysis 00 (2008) 1–9
 DOI 10.3233/RDA-2008-0010
 IOS Press

1

Adversarial design games and the role of anticipation in sensor networks

Jeffrey V. Nickerson*

Center for Decision Technologies, Howe School of Technology Management, Stevens Institute of Technology, Hoboken, NJ 07030-5991, USA

Abstract. Sensor networks are not anticipatory, but ideally they should be. In order to detect intruders, the environment of the possible attack scene can be monitored, and the position of sensors modified in order to increase the probability of detection. When faced with a resourceful intruder, the problem of sensing context becomes more difficult, and must expand to include monitoring for information about the intruders' objectives and resources. We call the continuous contest between intruders and sensor network designers an *adversarial design game*, and discuss ways the sensor network designers may proceed, using human design processes and automated design techniques.

Keywords: Sensor networks, intrusion detection, design science, anticipation, evolutionary algorithms, terrorism, war games

1. Introduction

Sensor networks are usually designed to react to signals. But in a network covering a large area, there are too many possible sources of signals. Consequently, we need to direct the network's attention to the salient aspects of the environment. What we really want from a sensor network is a terse, accurate description of the current situation, and a prediction about what might happen next [21].

If sensor networks could do this, they would be *anticipatory*. So far they are not, and maybe they never will be. Rosen claimed that anticipation is a characteristic of living things, and therefore cannot be automated. He provided a mathematical proof [45,46]. While some say his proof is wrong [8,27]; others say it is correct [29,30]. If Rosen's claim is false, then modeling anticipation may provide a way to improve artificial intelligence. If his claim is true, then attempts to fully automate anticipation will fail. Instead we will need hybrid systems, in which the memory and search capabilities of computers are combined with human beings who possess higher anticipatory skill [38]. Thus, an attempt to understand anticipation in relation to automation is useful either way.

* Address for correspondence: Jeffrey V. Nickerson, Center for Decision Technologies, Howe School of Technology Management, Stevens Institute of Technology, Castle Point on Hudson, Hoboken, NJ 07030-5991, USA. Tel.: +1 201 216 8124; Fax: +1 201 216 5385; E-mail: jnickerson@stevens.edu.

We shall discuss anticipation in the context of sensor networks. Specifically, we shall consider networks built to detect intrusions into a space. We present a series of design problems, and increasingly complicated solutions to these problems. One of our contributions comes from pointing out the potential synergies between research in the disparate fields of anticipation, sensor networks and creative design. Our work has pragmatic implications for designers of intrusion detection systems, and theoretical implications for the modeling of sets of situations we call *adversarial design games*. First we discuss related work. Then we develop an illustrative example of an adversarial design game. Later, we will discuss how to assist the designers of sensor networks.

2. Related work

We shall survey, in turn, literature from several fields: anticipation, context modeling, sensor networks, and design.

2.1. Anticipation

The modern literature on anticipation is rooted in the systems biology of Rosen [45,46]. Rosen felt that anticipation is a fundamental aspect of living things. For example, our metabolisms are anticipatory, in the sense that a metabolism will start adjusting itself even

1 ahead of conscious decisions to change a direction of
 2 movement. For Rosen, anticipation can be partially
 3 explained as a simulation that occurs on a different
 4 timescale. In other words, in considering a decision,
 5 we might quickly simulate the expected results of that
 6 decision, projecting ourselves forward in time. That is,
 7 once we have imagined the results, we use them to
 8 guide our decision. This anticipatory simulation has to
 9 happen quickly; we need to run through what might
 10 happen before it actually happens.

11 2.2. Context modeling

12 Nadin stated that anticipation is the *human sense of*
 13 *context* [39, p. 27]. In other words, if we really under-
 14 stand the situation we are in, we are in a position to
 15 predict what could happen next – better yet, to “come
 16 up with a number of conflicting models for future action”
 17 [39, p. 27]. Thus the problem of anticipation is
 18 in essence the problem of recognizing the situation we
 19 might find ourselves in, not just the position we were
 20 or are in.

21 This insight provides a bridge to the artificial intel-
 22 ligence literature on the automated representation of
 23 context. McCarthy [33] defined context in predicate
 24 calculus. But it is not feasible to represent all aspects
 25 of an environment. Barwise and Perry [5] constructed
 26 a situation theory in which only the relevant aspects of
 27 a situation are portrayed and then augmented as a situ-
 28 ation changes. Their theories have been applied mainly
 29 in linguistic applications (e.g., Akman and Surav [3].
 30 Context is proving important in vision applications
 31 [22]. Context modeling has also been applied to sur-
 32 veillance applications [7] and to sensor systems [21].
 33 Tracking someone moving through a crowd is easier if
 34 an algorithm can be used to anticipate the next position
 35 of the subject.

36 More generally, context is important because typi-
 37 cality – whether something is normal or usual, as
 38 opposed to abnormal or extraordinary – changes ac-
 39 cording to context [4]. There is another stream of lit-
 40 erature that addresses this issue under the term *sit-*
 41 *uation awareness*. Low situation awareness has been
 42 correlated with accidents. We can think of accidents
 43 as failures to anticipate. Indeed, Endsley’s model for
 44 situation awareness has three components: perception,
 45 comprehension, and projection. Projection, the high-
 46 est level of awareness, includes anticipation as well as
 47 mental simulation [13,14].

48 2.3. Sensor networks

49 Most sensor literature is focused on the engineer-
 50 ing challenge of covering as large an area as possible
 51 with sensors. There is usually a multi-objective opti-
 52 mization problem involved: for example, cover an area,
 53 but minimize the number of sensors and the energy in-
 54 volved in their communication (e.g., Jourdan and de
 55 Weck [25]). While multi-objective optimization has a
 56 long history [50], the advent of efficient genetic algo-
 57 rithms [12] has facilitated multi-objective analyses of
 58 a wide range of problems [11]. In many cases, these
 59 papers suggest that the ideal configuration of sensors is
 60 in an evenly spaced line or a lattice. This makes sense:
 61 the regular spacing of sensors would seem to achieve
 62 the goal of full coverage while minimizing communi-
 63 cation costs.

64 Recently, there has been interest in applying game
 65 theoretic techniques to sensor-related issues. In some
 66 cases, the game is a cooperative one; but in situations
 67 such as intrusion detection, non-cooperative models
 68 can mimic intrusion and defense [1,2,26,28,57].

69 2.4. Design

70 Design, it can be argued, is anticipatory. We design
 71 an object with the hope that, once built, it will satisfy
 72 our given objectives [37]. Some kinds of design can be
 73 reduced to well-defined optimization problems: for ex-
 74 ample, the discovery of new forms in mechanical engi-
 75 neering (e.g., Tu et al. [53]). In such problems, the re-
 76 quirements are predetermined, and there is a test to be
 77 applied to see if the design fulfills those requirements.
 78 But ill-defined problems are more common. New el-
 79 ements, new evaluations, new criteria may be intro-
 80 duced. Formulating the problem and producing a so-
 81 lution are intertwined [20,36]. In such problems there
 82 are multiple – and changing – objectives. For exam-
 83 ple, in designing a new product, we not only need to
 84 anticipate how the product will look, once created, but
 85 also, once implemented, if it will still fulfill the fickle
 86 requirements of the consumers.

87 In the literature on design, the most intriguing the-
 88 ories state that designing something new always in-
 89 volves going outside and beyond the original problem
 90 definition [15]. Solutions can appear to spring from
 91 nowhere, but much design is done methodically. In-
 92 deed, many designers have been inspired by the same
 93 biological systems theory that Rosen helped develop
 94 [24]. Rittel [44] thought that the crucial aspect of large
 95 design problems was that they were over-constrained.

1 He proposed a method he called *systematic doubt* to
 2 formally negate each of the constraints assumed in a
 3 problem statement and thus generate a previously ig-
 4 nored solution (see Nickerson [42]).

6 2.5. Summary of related work

8 Our look at the literature of these disparate fields
 9 suggests the following: sensor network research can
 10 model the relation between intrusion and defense as
 11 a kind of game. Understanding context is recognized
 12 as being important in sensing. From the work of
 13 Nadin [39], we can associate context with anticipa-
 14 tion and conclude that anticipation is important to sens-
 15 ing. There is an opportunity to explore the relatively
 16 unstudied relationship between the design of sensor
 17 systems and anticipation. We turn to this relationship
 18 next.

21 3. An adversarial design game

23 3.1. Defending against accidental intrusions

25 We will now take a look at a scenario in sensor net-
 26 work intrusion detection and trace it through a num-
 27 ber of different stages. We are going to describe the
 28 placement of sensors as a kind of contest that we shall
 29 call an *adversarial design game*. Just as creative de-

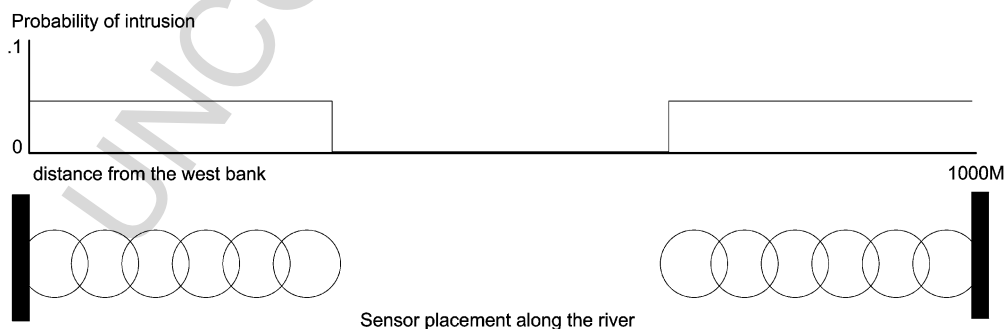
52 sign has been characterized as the solving of ill-defined
 53 problems, adversarial design games involve designing
 54 in the face of multiple and changing objectives.

55 Consider the detection of an intruder into a river. Let
 56 us first presume that the intruder does not intend to do
 57 harm, but is lost. Consider, for example, the incursions
 58 of whales up estuaries and rivers. Whales cannot swim
 59 against strong currents. In rivers and estuaries, currents
 60 go to zero at the edges and are strongest in the center.
 61 Therefore, we shall presume the probability of in-
 62 trusion is low in the center and high on the edges. In
 63 Fig. 1, we show a simplified example of this: probabi-
 64 lity of intrusion is zero in the center of the river. In
 65 Fig. 2, we show the deployment of sensors that will
 66 maximize the probability of detection. The configura-
 67 tion shown above may appear strange, but if it is really
 68 impossible for the whale to swim up the center, then
 69 such a scheme increases the probability of detection
 70 [51,52,54].

71 The whale’s possible intrusion is being anticipated
 72 through the attention paid to the environmental con-
 73 straints under which the whale operates. Whales rarely
 74 swim up a particular river, so we have little data on
 75 which to base our sensor placement. However, whales
 76 are constrained by the currents, which we can monitor
 77 with sensors. Since the currents of rivers and estuaries
 78 change frequently, we can build sensors that monitor
 79 the environment and move themselves into an optimal
 80 configuration through reinforcement learning – with



37 Fig. 1. The probability of an intrusion on the vertical dimension, and the location across the river on the horizontal dimension, from bank to bank.



50 Fig. 2. On the top, the probability of an intrusion on the vertical dimension, and the location across the river on the horizontal dimension, from
 51 bank to bank. On the bottom, the distribution of sensors according to the river location.

reinforcement coming from the environment [6,48]. More generally, adaptive sensor systems can use proxies always present in the environment to “train” for important but infrequent events.

3.2. Planning intentional intrusions

Suppose we need to detect divers who intend to intrude. Whales swim up rivers because they are lost; they are not intending to deceive the sensor system. But divers who want to intrude will use deceptive tactics, and will search for vulnerabilities in the sensor defense. Thus, designing against thinking, resourceful opponents is more complex than designing against the laws of nature. The laws of nature still play a role. Divers will also be limited in respect to the speed with which they can proceed against a current, and so our scheme may still work [54].

Let us treat the problem as a form of a game in which intruders can win by penetrating the sensor net. Let us imagine intruders have discovered that sensors are placed only at the edges of the river. How do the intruders win the game? This is a different type of game: it is an instance of an *adversarial design game*. We define this very general game as *a continuing contest between two opposed parties, in which each party has a changing set of objectives, as well as extendable resources; and there is partial uncertainty as to the objectives and resources of the other party*. This can be thought of as a soft-constraint design problem [20]. Let us imagine the divers’ team has large monetary resources that can buy equipment or even invent equipment. Then the divers may purchase devices – e.g., underwater motors – that will propel them at a speed great enough to move through the center of the river.

We may look at the divers’ design problem as including two objectives: to intrude on the space, and to minimize the cost of doing so. If there are no defensive sensors, then the cost of the operation is low. But if there are sensors placed on the edges of the river, then the cost of operation will be high, and may involve raising money to buy the motors.

3.3. Defending against intentional intrusions

Given the likelihood of intentional intrusion, let us consider the design problem of the defenders. The defenders have to think like the intruders and design possible attack scenarios. Let us assume this process is successful: the use of a motor is a strong possibility. The goals of the defenders are to prevent attacks while

simultaneously minimizing the cost of the defense. If the defenders believe that the intruders do not have access to a motor, then the optimization is as in Fig. 2: put sensors only on the sides of the river. But if the defenders believe that the intruders might have access to a motor, then the situation is different.

Take note that the defenders have to anticipate the attackers’ design. That is, the defenders need to be at least as good a design team as the intruders. The defenders will have been given the task of designing a sensor network, but without being told about motors. The defenders have to discover this potential (possible) attack scenario – even though it is outside the statement of the original problem. That is, the defenders have to elaborate several possible attack scenarios in order to prepare for the potential actual attack.

Let us assume that the defenders have imagined the attacker might use a motor. Now the defenders have to figure out whether the attackers have sufficient resources – money or contacts – to field a motor. Figuring this out is a different kind of sensor problem, one that falls into the area of signal or human intelligence. The defenders now need to expand their concept of sensing from a set of local environmental and target sensors to include remote information sensing which seek to detect the resources that the attackers might use.

Let us assume that the defenders conclude that the attackers indeed have access to motors. How should the defenders proceed? One possible way is to evenly space the sensors across the river. This probably will not work. If the divers have motors, they will proceed more quickly, and the sensors may therefore have to be placed farther from the area to be protected in order to provide enough time to intercept the intruders [43,55].

There is another solution: design a new type of sensor that detects underwater motors. It is easier to detect motors than to detect divers, thus these sensors will have greater range. Consequently, the defenders invent, at great expense, a new kind of sensor that will detect motor-assisted divers. Figure 3 shows the configuration. We assume that the motors are large, ungainly, and noisy, and thus cannot be used on the sides of the river, because the diver could be seen or heard in shallower water. Then, these wider range sensors will only monitor the center of the river, and they will be placed farther away from the area to be protected so as to provide sufficient time to intercept the intruders.

3.4. The intruders’ counter-strategy

Now let us assume that the intruders learn of the new set of motor sensors. How can the intruders proceed? If the intruders are truly bent on penetrating the space,

52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102

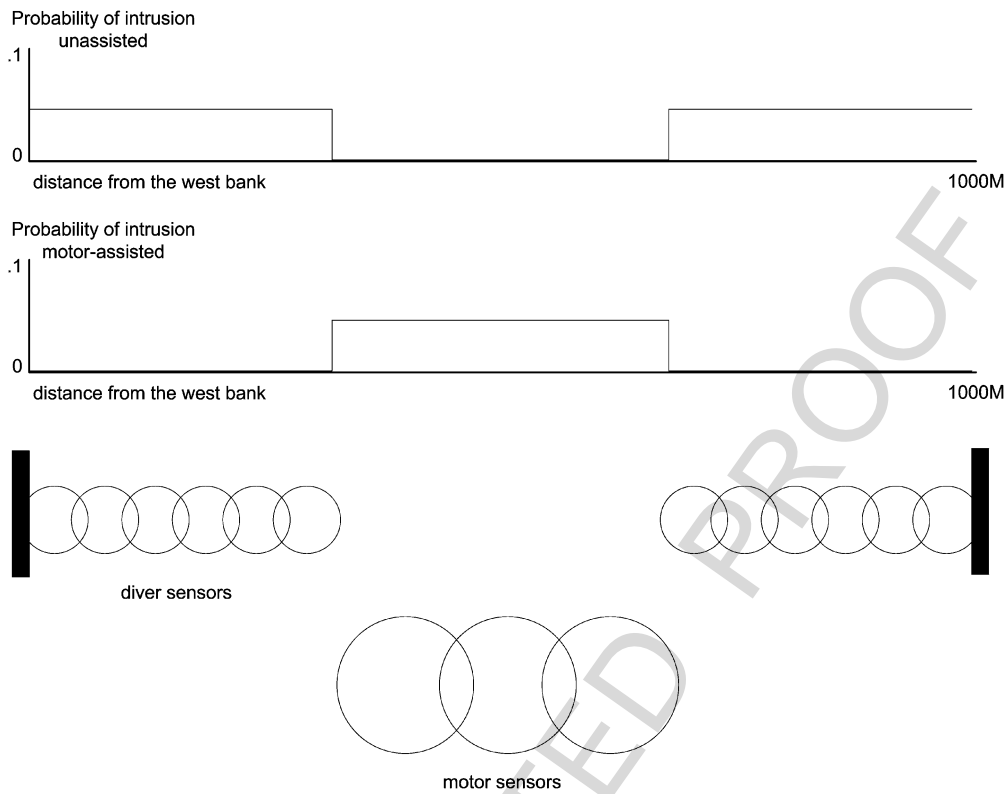


Fig. 3. A configuration of two different types of sensors to counter the possible use of motors in an attack.

then they may consider buying (or inventing) silent underwater motors. Alternatively, the intruders can readjust their objectives. They might decide that more work on motors will be too expensive. But if they can convince the defenders they are doing such work, the defenders will have to spend a great deal of money to build a defense system against a silent motor. The intruders decide to change their objective. Now the goal becomes bankrupting the defenders. Their next step may have nothing to do with intrusion, but instead focus on the information component of the contest. They stage cell phone conversations that they believe will be monitored, and in which they discuss a newly acquired (but really non-existent) motor.

3.5. The defenders' counter-counter-strategy

The defenders hear the cell phone conversations. Are they to believe them? There is always the possibility that the intruders are just trying to bankrupt them. The defenders again have to focus on acquiring more information. They need to figure out if the objective of the divers is still to intrude, or whether the divers have shifted to another goal. Again, the sensing should

include signal and human intelligence. The context of the problem now includes the resources and goals of the opponent.

3.6. And so on

It is obvious that the game can go on and on. The central point of the illustration is that the defense against intrusion is a problem of understanding context. At one level, the physical environment provides constraints that can be useful in shaping a sensor configuration. At another level, the environment to be sensed should ideally include the objectives and resources of the intruders. Acquiring such information involves a more complex sensor placement problem, which makes use of signal and human intelligence.

3.7. Examples of adversarial design games

There is evidence that terrorists and those who oppose them play a design game having lethal consequences. For example, we can safely say that an attack is designed if components of the attack – say, bombings – happen in different places, but at exactly

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51

52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102

1 the same time. Simultaneous explosions might accom- 52
 2 plish several objectives. First, the knowledge of one at- 53
 3 tack cannot be used to guard against the second attack. 54
 4 Also, terror effects are multiplied. Finally, the attacks 55
 5 may be intended to show that they are designed, that a 56
 6 resourceful force is behind them.

7 Whatever the motivation, the most deadly attacks 57
 8 are simultaneous. The Beirut bombings (1983) were 58
 9 within minutes of each other. The Bombay bombings 59
 10 (in 1993) involved 13 explosions over three hours. The 60
 11 embassy bombings in Nairobi and Dar es Salaam (in 61
 12 1998) were physically far apart, but practically simul- 62
 13 taneous. The attacks of September 11, 2001 involved 63
 14 four concurrent attacks on different targets. The attacks 64
 15 in Bali (in 2002) involved three simultaneous bomb- 65
 16 bings. Ten bombs exploded within minutes during the 66
 17 Madrid bombings in 2004. And in the London bomb- 67
 18 bings (in 2005), three bombs detonated simultaneously, 68
 19 and a fourth bomb detonated a short while later [35]. 69

20 Simultaneity is not the only characteristic of design 70
 21 involved in terrorist attacks. Many attacks have precu- 71
 22 sors: training, tests, and previous failed attempts. For 72
 23 example the *S.S. Cole* attack in 2000 consisted of initial 73
 24 scoping out of the target, practice runs in Aden har- 74
 25 bor, a failed attempt because the attack boat sank, a re- 75
 26 planning phase, a redesign of the boat-explosive com- 76
 27 bination, and then a successful attack [34]. 77

28 Thus there is evidence that terrorist attackers act as 78
 29 designers – raising funds, improvising resources, con- 79
 30 sidering alternatives, and refining technologies in order 80
 31 to accomplish a set of objectives. The 9/11 attacks were 81
 32 an example of the imagination of the attackers being 82
 33 greater than the imagination of the defenders, some- 83
 34 thing noted in the 9/11 Commission report [41]. It was 84
 35 not that nobody had anticipated the attacks; a widely 85
 36 read author of fiction had (cf. Clancy [9,10]). But the 86
 37 crucial defenders – those who designed and managed 87
 38 the immigration systems and passenger screening sys- 88
 39 tems at airports – had not anticipated such an attack. 89
 40
 41

42 **4. Defending against attack: Adversarial design** 43 **game aids**

44
 45 If terrorist intruders are acting as designers, then 90
 46 defenders against such attacks have a difficult prob- 91
 47 lem. The defenders need to design a strategy, or sev- 92
 48 eral strategies, anticipating that the intruders will de- 93
 49 sign around any defense they come up with [23]. That 94
 50 is, the defenders need to be better designers than the at- 95
 51 tackers, anticipating what the attackers will design and

devising something unexpected enough that the intrud- 52
 ers will not anticipate the full extent of the defense. 53
 The problem is made more difficult by built-in asym- 54
 metries: it is much more expensive to defend a city than 55
 it is to set off a bomb in a city. 56

How, then, can the problem of defense or protec- 57
 tion against such asymmetric attacks be handled? Pos- 58
 sible targets can be hardened. We can, as we have sug- 59
 gested, defend those places that seem more likely to be 60
 attacked due to the nature of the environmental con- 61
 straints under which the attackers operate. 62

When the possible attacker is determined and re- 63
 sourceful, then the problem has no easy solution. We 64
 suggested that the problem has to be thought of as 65
 multi-objective, and that the objectives can change. 66
 One strategy, which most security researchers follow, 67
 is to reduce the game to something that can be solved 68
 easily by making simplifying assumptions. For exam- 69
 ple, soft, changing goals are simplified into hard, static 70
 goals. Resources are fixed. Multi-objective problems 71
 are weighted so they can be reduced to single objective 72
 problems. Then security problems can be solved in the 73
 abstract. Such strategies are pragmatic: not everything 74
 can be analyzed, so problems are simplified until they 75
 yield to known techniques. There are some very in- 76
 sightful examples of such analyses [19,49]. The major 77
 shortcoming of this reductive methodology is that the 78
 biggest threat in terrorism is a new type of attack that is 79
 conceived creatively. (By creative, we mean something 80
 that has not been conceived or carried out before; or 81
 the act has been forgotten and therefore seems novel.) 82
 The attacks of 9/11 are proof of the inadequacy of such 83
 a reductionist paradigm (cf. [39], pp. 115–116). How 84
 can such attacks be anticipated? 85

First, we shall consider human-intensive solutions 86
 to the problem, and then address how automation can 87
 help. Let us consider sensing itself. From our example, 88
 knowing the currents of the river is most useful if we 89
 know whether or not the intruder has a motor. We can 90
 use sensors to detect (“sense for”) a motor. We can also 91
 sense for the purchase of the motor. In other words, 92
 we can expand our concept of sensing to encompass 93
 the transactions that marshal resource in support of an 94
 attack. The intelligence, then, changes our prior prob- 95
 ability options in respect to the technology to be de- 96
 fended against. 97

Earlier, we discussed literature related to design. 98
 This literature suggests that a designer wants to meet 99
 the externally imposed design criteria, but is not afraid 100
 to stretch or ignore the criteria and the stipulated con- 101
 straints. The designer goes for something that is unex- 102

pected. Thus the designer of a sensor system needs to be creative in imagining possible attacks, and then even more creative in imagining a new form of defense. Such creative, anticipatory design is possible, but it may not emerge from work performed under standard procurement contracts, whose objectives include minimizing contract risk. It is more likely that it will emerge in fundamental research contracts or, additionally, in small start-up companies.

Creative design can come about as part of war gaming exercises. From a theoretical perspective, red-team/blue-team exercises, in which people play the role of attacker and defender, should be effective in generating good defensive ideas. Our illustrative example, mentioned above is a small-scale example of red-team/blue-team thinking. From a practical perspective, caution is necessary. War games fulfill many objectives. They might help generate designs of possible enemy attacks. But, since they involve more people, they also become training aids, morale boosters and public relations exercises. When these goals conflict, sometimes the design lessons may be ignored (see, for example, an account of war gaming related to the war in Iraq [17]).

From the standpoint of automation, the design literature is also useful. Two techniques have been productive in automatically producing creative designs. The first technique involves merging and fusing prototypes of design [16,31,47]. In such a technique, existing prototypical solutions are modified and merged in order to yield new designs. The second technique, evolutionary algorithms, makes use of the first technique, prototyping, but focuses on ways to combine and alter such prototypes automatically [56]. An evolutionary algorithm generates a set of possibilities, evaluates them against multiple objectives, and then matches some ideas and mutates others, repeating the cycle until no more progress can be made. The fairly recent discovery of efficient multi-objective algorithms [12] means that large design spaces can be explored with relative ease. Many have made the argument that this mutating and merging mimics the creative process [15,40]. Some even maintain that such mutating and merging may underlie our fundamental thinking processes through which we categorize the phenomena we confront [32]. Thus it seems a productive path for research to consider exploring security problems with such algorithms.

There is, however, a step that has not been explored much: studying what happens when design objectives change. For example, systems in place in airports were

designed to counter hijackers who planned to take hostages, not hijackers who planned to crash an airplane. The objective of the game changed unilaterally, and the defending side didn't see it coming.

The range of possible objectives is large. It is just barely in the realm of possibility to contemplate exhaustively searching a space in which the number of factors is defined [18]. It is more feasible to use genetic algorithms to do such searching without being forced to consider all possibilities: some solutions will surely dominate others. This presupposes that we can enumerate a set of possible objectives; and it does not appear there is any automated way to perform this initial step.

Practically speaking, the application of such automated design aids is probably most useful when run by experienced people who know a particular domain. The automated systems may perform a function similar to human brainstorming. By proposing new solutions, they might dispel the assumptions that usually arise in complex design efforts.

5. Conclusions

Current approaches to sensing tend to be reactive. But sensing technology is most useful if it helps us characterize the current context in order to anticipate what can happen next. In the case of intrusion detection, we can achieve better designs by sensing not just the intruder, but also the environment in which the intruder must operate. The environment constrains the actions of the intruder; thus we can position sensors in a way more likely to capture the intruder. This works well if the intruder is not intending to deceive. If the intruder is indeed also a designer, the game is more difficult. We call it an *adversarial design game*. In such case, the intruder can marshal more resources in order to circumvent the defensive design. The constraints on both the intruder and the defender are soft: new resources can be recruited and new technologies invented.

Therefore, defending against designed attacks calls for anticipation at a higher level. The attack strategy itself needs to be anticipated. This might be done through red team/blue team exercises, and through gathering intelligence about an adversary's goals and resources. In the realm of automation, the exploration of the large space of possible attacks and defenses using evolutionary algorithms may be one way for defenders against attack to remove the assumptions that block our ability to anticipate.

References

- [1] A. Agah and S.K. Das, Preventing DoS attacks in sensor networks: A repeated game theory approach, *International Journal of Network Security* **5**(2) (2007), 145–153.
- [2] A. Agah, S.K. Das, K. Basu and M. Asadi, Intrusion Detection in Sensor Networks: A Non-Cooperative Game Approach, IEEE Computer Society, Washington, DC, USA, 2004.
- [3] V. Akman and M. Surav, The use of situation theory in context modeling, *Computational Intelligence* **13**(3) (1997), 427–438.
- [4] L.W. Barsalou, Ideals, central tendency, and frequency of instantiation as determinants of graded structure in categories, *Journal of Experimental Psychology: Learning, Memory, and Cognition* **11** (1985), 629–654.
- [5] J. Barwise and J. Perry, *Situations and Attitudes*, MIT Press, Cambridge, MA, 1983.
- [6] T. Ben-Zvi and J.V. Nickerson, Responding to changing situations: Learning automata for sensor placement, in: *Military Communications Conference – MILCOM 2007*, Orlando FL, October 29–31, 2007.
- [7] F. Brémond and M. Thonnat, Issues of representing context illustrated by video surveillance Applications, *International Journal of Human–Computer Studies* **48**(3) (1998), 375–391.
- [8] D. Chu and W.K. Ho, A category theoretical argument against the possibility of artificial life: Robert Rosen’s central proof revisited, *Artificial Life* **12**(1) (2006), 117–134.
- [9] T. Clancy, *Debt of Honor*, G.P. Putnam, New York, 1994.
- [10] T. Clancy, *Executive Orders*, Harper Collins, New York, 1998.
- [11] C.A. Coello, *Evolutionary Algorithms for Solving Multi-Objective Problems*, Springer, New York, 2007.
- [12] K. Deb, *Multi-Objective Optimization Using Evolutionary Algorithms*, Wiley, New York, 2001.
- [13] M.R. Endsley, Toward a theory of situation awareness in dynamic systems, *Human Factors* **37**(1) (1995).
- [14] M.R. Endsley and D.J. Garland, *Situation Awareness: Analysis and Measurement*, Lawrence Erlbaum Associates, Mahwah, NJ, 2000.
- [15] J.S. Gero and M.-L. Maher, in: *Modeling Creativity and Knowledge-Based Creative Design*, J.S. Gero and M.-L. Maher, eds, Lawrence Erlbaum Associates, Hillsdale, NJ, 1993.
- [16] J.S. Gero and G.J. Smith, Context and design agents, in: *CONTEXT 07*, 2007 (see also: <http://context-07.ruc.dk>).
- [17] M. Gladwell, *Blink: The Power of Thinking Without Thinking*, Little, Brown, New York, 2005.
- [18] S.J. Hanson, T. Matsuka, C. Hanson, D. Rebbecki, Y. Halchenko, A. Zaimi and B. Pearlmuter, Structural equation modeling of neuroimaging data: Exhaustive search and Markov chain Monte Carlo, in: *10th Annual Meeting of the Organization for Human Brain Mapping*, Budapest, 2004.
- [19] K. Hausken, Protecting infrastructures from strategic attackers, in: *18th European Safety and Reliability Conference (ESREL)*, Stavager, Norway, 2007 (in: *Game Theory and Reliability*, V. Bier and N. Azaiez, eds, Springer Series on Reliability Engineering, forthcoming).
- [20] T. Heath, Social aspects of creativity and their impact on creativity modeling, in: *Modeling Creativity and Knowledge-Based Creative Design*, J.S. Gero and M.-L. Maher, eds, Lawrence Erlbaum Associates, Hillsdale, NJ, 1993, pp. 9–23.
- [21] S. Iacob, J. De Heer and A. Salden, A pragmatic model of attention and anticipation for active sensor systems, in: *Advances in Biologically Inspired Information Systems*, I. Carreras, ed., Springer, Berlin/Heidelberg, 2007, pp. 229–243.
- [22] S. Intille and A. Bobick, Closed-world tracking, in: *Proceedings of the Fifth International Conference on Computer Vision*, IEEE Press, 1995, pp. 672–678.
- [23] J.-Y. Jian, T. Matsuka and J.V. Nickerson, Recognizing deception in trajectories, in: *28th Annual Conference of the Cognitive Science Society*, 2006 (see also: http://howe.stevens.edu/fileadmin/Files/publications/Recognizing_Deception_in_Trajectories.pdf).
- [24] J.C. Jones, A method of systematic design, in: *Conference on Design Methods*, J.C. Jones and D.G. Thornley, eds, Pergamon Press, Oxford/New York, 1963, pp. 53–73.
- [25] D.B. Jourdan and O.L. de Weck, Layout optimization for a wireless sensor network using a multi-objective genetic algorithm, in: *Vehicular Technology Conference*, Vol. 5, IEEE Proceedings, 2004, pp. 2466–2470.
- [26] S. Kumar and V. Marbukh, A game theoretic approach to analysis and design of survivable and secure systems and protocols, *Computer Network Security* **2776** (2003), 440–443.
- [27] C. Landauer and K. Bellman, Theoretical biology: Organisms and mechanisms, in: *Computing Anticipatory Systems Conference (CASYS)*, 2001 (see also: *AIP Conference Proceedings* **627** (2002), 59–70).
- [28] Y. Liu, C. Comaniciu and H. Man, Modeling misbehavior in ad hoc networks: A game theoretic approach for intrusion detection, *International Journal of Security and Networks* **1** (3/4) (2006), 243–254.
- [29] A.H. Louie, The memory evolutive systems as a model of Rosen’s organisms (metabolic, replication) systems, *Axiomathes* **16**(1) (2004), 137–154.
- [30] A.H. Louie, A living system must have noncomputable models, *Artificial Life* **13**(3) (2007), 293–297.
- [31] M.-L. Maher and F. Zhao, Dynamic associations for creative engineering design, in: *Modeling Creativity and Knowledge-Based Creative Design*, J.S. Gero and M.-L. Maher, eds, Lawrence Erlbaum Associates, Hillsdale, NJ, 1993, pp. 329–351.
- [32] T. Matsuka and J.V. Nickerson, Modeling human hypothesis testing behaviors with simulated evolutionary processes, in: *Proceedings of the IEEE World Congress on Computational Intelligence International Conference on Evolutionary Computation*, 2006, pp. 399–405.
- [33] J. McCarthy and S. Buvac, Formalizing context, in: *13th International Joint Conference on Artificial Intelligence (IJCAI)*, 1993 (see: <http://www-formal.stanford.edu/jmc/context3/context3.html>).
- [34] J. Miller, M. Stone and C. Mitchell, *The Cell: Inside the 9/11 Plot and Why the FBI and CIA Failed to Stop It*, Hyperion, New York, 2002.
- [35] MIPT Terrorism Knowledge Base, 2007 (see: <http://www.tkb.org>).
- [36] W.J. Mitchell, A computational view of design creativity, in: *Modeling Creativity and Knowledge-Based Creative Design*, J.S. Gero and M.-L. Maher, eds, Lawrence Erlbaum Associates, Hillsdale, NJ, 1993, pp. 25–42.

- [37] M. Nadin, Computational design. Design in the age of a knowledge society, *formdiskurs, Journal of Design and Design Theory* 2(1) (1996), 40–60.
- [38] M. Nadin, *Hybrid Anticipatory Control Mechanisms*, An application for a research grant, 2001; http://anteinstitute.org/pdf/ante_hacm.pdf.
- [39] M. Nadin, *Anticipation – The End Is Where We Start From*, Lars Mueller Verlag, Basel, 2003.
- [40] M. Nadin and M. Novak, MIND – A design machine, in: *Intelligent CAD Systems*, Vol. 1, P.J.W. Ten Hagen and T. Tomiyama, eds, Springer-Verlag, Berlin, New York, Paris, Tokyo, 1987, pp. 146–171.
- [41] National Commission on Terrorist Attacks, *The 9/11 Commission Report*, W.W. Norton, New York, 2004.
- [42] J.V. Nickerson, Teaching the Integration of Information Systems Technologies, *IEEE Transactions on Education* 49(2) (2006), 271–277.
- [43] J.V. Nickerson and S. Olariu, Protecting with sensor networks: Attention and response, in: *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS)*, IEEE Computer Society, 2007 (see also: <http://ieeexplore.ieee.org/iel5/4076361/4076362/04076979.pdf>).
- [44] H.W.J. Rittel and M.M. Webber, Dilemmas in a general theory of planning, *Policy Sciences* 4 (1973), 155–169.
- [45] R. Rosen, *Anticipatory Systems. Philosophical, Mathematical, and Methodological Foundations*, Pergamon Press, Oxford/New York, 1985.
- [46] R. Rosen, *Life Itself. A Comprehensive Inquiry into the Nature, Origin, and Fabrication of Life*, Columbia University Press, New York, 1991.
- [47] M.A. Rosenman and J.S. Gero, Creativity in design using a design prototype approach, in: *Modeling Creativity and Knowledge-Based Creative Design*, J.S. Gero and M.-L. Maher, eds, Lawrence Erlbaum Associates, Hillsdale, NJ, 1993, pp. 111–138.
- [48] Y. Sakamoto and J.V. Nickerson, Social behavior in a team of autonomous sensors, in: *Proceedings of the Intelligence and Security Informatics Conference*, G. Muresan, T. Altiok, B. Melamed and D. Zeng, eds, IEEE, New Brunswick, NJ, 2007 (see: <http://www.stevens.edu/jnickerson/ISI2007SensorTeam.pdf>).
- [49] T. Sandler, Counterterrorism: A game-theoretic analysis, *Journal of Conflict Resolution* 49(2) (2005), 183–200.
- [50] L.S. Shapley, Equilibrium points in games with vector payoffs, *NRLQ* (1959), 57–61.
- [51] H. Shi, D. Kruger and J.V. Nickerson, Incorporating environmental information into underwater acoustic sensor coverage estimation in estuaries, in: *Military Communications Conference – MILCOM 2007*, Orlando, FL, October 29–31, 2007.
- [52] R. Stolkin, L. Vickers and J.V. Nickerson, Using environmental models to optimize sensor placement, *IEEE Sensors Journal* 7(3) (2007), 319–320.
- [53] J. Tu, K.K. Choi and Y.H. Park, A new study on reliability-based design optimization, *ASME Journal of Mechanical Design* 121 (1999), 557–564.
- [54] L. Vickers, R. Stolkin and J.V. Nickerson, Computational environmental models aid sensor placement optimization, in: *Military Communications Conference – MILCOM 2006*, Washington, DC, October 23–25, 2006 (published in: *IEEE Proceedings of MILCOM 2006*); <http://ieeexplore.ieee.org/iel5/4086332/4043248/04086761.pdf?tp=&arnumber=4086761&isnumber=4043248>.
- [55] R. Wang and J.V. Nickerson, Search strategy optimization for intruder detection, *IEEE Sensors Journal* 7(2) (2007), 315–316.
- [56] R.F. Woodbury, A genetic approach to creative design, in: *Modeling Creativity and Knowledge-Based Creative Design*, J.S. Gero and M.-L. Maher, eds, Lawrence Erlbaum Associates, Hillsdale, NJ, 1993, pp. 211–232.
- [57] Y. Xing, R. Chandramouli, S. Mangold and S. Sankar, Price dynamics in competitive agile spectrum markets, *IEEE Journal on Selected Areas in Communications* 25(3), 613–621.