Training through Simulation of Border Patrol Incidents

Nickolas Vlahopoulos
University of Michigan
Ann Arbor, MI
nickvl@umich.edu

Nathan Murray, Robert Montemayor
Booz Allen Hamilton
McLean, VA
murray_nathan@bah.com, montemayor_roberto@bah.com

Geng Zhang
Michigan Engineering Services
Ann Arbor, MI
gengz@miengsrv.com

Syed Mohammad
DHS Science and Technology Directorate
Washington, DC
syed.mohammad@hq.dhs.gov

ABSTRACT

The Department of Homeland Security has a strong interest in utilizing simulation tools for training personnel on how to best plan the distribution and utilization of resources along the border in order to contain and prevent incidents. In this paper a desktop simulation capability for supporting border patrol personnel training is presented. It operates on a typical laptop computer and it therefore enables training opportunities for a large number of agents in the field. A visualization driver allows the user to select the part of the border where the incidents will take place. Data driven information is used for setting up the available resources (e.g., air, water and ground assets in the field, border patrol stations with varying capacity, deployable assets and coverage) and the adversarial threats (e.g., strength, speed, capabilities) which generate the incidents. The amount, readiness and the capabilities of the allocated resources, provide resource information for each simulated scenario. The simulation is visualized and the user can observe the evolution of the incidents, the engagements between adversaries and border patrol agents while assessing the effectiveness of the defensive layout and use of assets. This is achieved by conducting probabilistic computations in parallel with the visual display. The latter consider all possible ways that threats can accomplish their objectives and compute the probability of success of the threats, which is the opposite of the border patrol effectiveness. The match-up between the capabilities and strengths of the adversaries vs the defense is considered in the computations at every action taken by an adversary towards an objective. Detection of threats is also accounted in the analysis. By providing information about the effectiveness of the defense against adversarial actions, trainees discover the most efficient approaches for hardening the border as they visually observe the incidents.

ABOUT THE AUTHORS

Nickolas Vlahopoulos has been a Professor at the University of Michigan for 28 years and has also worked in the Industry for 7 years prior to his academic career; he has published over 100 papers and has graduated 25 PhD students.

Syed Mohammad Leads the Modeling and Simulation Technology Center at the Department of Homeland Security Science and Technology, Technology Center. He has over 20 years of Federal experience supporting DHS and DOD in research, development, engineering, and acquisition roles.

Geng Zhang is a R&D engineer at Michigan Engineering Services; he has 19 years of experience and has published 29 technical papers.

Nathan Murray is an immersive software designer with over 12 years of experience designing and developing visualizations and simulations

Robert Montemayor is a retired Border Patrol Agent with over 27 years of federal Law Enforcement and homeland security experience. He is certified as a Project Management Professional and has extensive experience in managing DHS national level programs.

Training through Simulation of Border Patrol Incidents

Nickolas Vlahopoulos
University of Michigan
Ann Arbor, MI
nickvl@umich.edu

Nathan Murray, Robert Montemayor
Booz Allen Hamilton
McLean, VA
murray_nathan@bah.com, montemayor_roberto@bah.com

Geng Zhang
Michigan Engineering Services
Ann Arbor, MI
gengz@miengsrv.com

Syed Mohammad
DHS Science and Technology Directorate
Washington, DC
syed.mohammad@hq.dhs.gov

INTRODUCTION

Simulation based training that uses virtual reality systems is immersive and provides experiences for realistic and intense scenarios (Law Enforcement Simulators, 2024). The aerospace domain has been using flight simulators for training of pilots and air controllers, but also for instrumentation and for maintenance personnel (Collins Aerospace Simulation and Training, 2024). Training for US Customs and Border Protection (CBP) agents is valuable enough that the US Government has built entire mock infrastructures and city-scale installations for training, while testing at the same time the effectiveness of operations and associated procedures (Kripa, Mueller, 2018). At the same time CBP operates twenty seven virtual reality simulators for training agents on specific scenarios such as: narcotics interdiction, armed bandit encounter, stolen vehicle stop, etc. (US Customs and Border Protection, 2024).

CBP also benefits from desktop tools that plan effective border patrolling schemes and assists in making risk-based decisions for resource allocation (Gutierrez, 2014). The work presented in this paper outlines the two main elements used for creating such a training tool. It contains a Visualization Driver (VD) and a probabilistic calculation engine. The VD is comprised of three components. The first component consists of incidents which are associated with the threats; the threats are specified by the user and they are assigned attributes of strength, speed and severity. The second component is the surveillance assets which are allocated in the vicinity of the border; their type and quantity are defined by the user. The patrol stations comprise the third component and represent the defense nodes; the user can define their coverage, the type of assets they contain and their strength. During a simulation the user can visualize the evolution of the incidents.

The graphical formalism of an Attack Defense Tree (ADTree) is used for elucidating how individual attack steps can be combined for creating a multi-stage attack scenario leading to a security breach, while at the same time considering the countermeasures of the defense (Fraile, Ford, Gadyatskaya, Kumar, Stoelinga, and Trujillo-Rasua, 2016; Kordy, Mauw, Radomirovic, and Schweitzer, 2014; Mauw, Oostdijk, 2006). In this work the graphical representation of the ADTree is structuring the computations conducted by the probabilistic calculation engine that provide for each possible route between a threat and a target, the probability of successfully reaching each target. Multiple threats and multiple targets can be specified. Each threat has its own set of offensive attributes as defined in the VD. A user defined sequence of path sections and defense nodes (ADTree elements) generate the alternative routes between each threat and each target in the ADTree. Countermeasure capabilities (e.g., walls, surveillance assets) are assigned to each path section. Finally, the properties of the stations are assigned to the defense nodes of the ADTree. Each countermeasure capability is matched against the attribute of the threat that is employed at the particular path section or defense node. Based on the relative strengths of the offensive and defensive attributes at each path section or defense node, a probabilistic calculation is completed. Concepts of detecting the threat at a particular ADTree element, or the threat already being detected at a prior element are accounted in the probabilistic calculations. Sensors can be assigned to path sections for hardening their defense. Resources can be shared between defense nodes. Threats can also collaborate by ordering their advancement towards the targets and having defensive resources diverted towards the routes of the leading threats, leaving lesser protection against the trailing threats that take different routes. The probabilities of a threat being successful at each element of the ADTree are computed and provide probabilistic assessments to the scenarios visualized using the VD.

The technical elements for the operation of the VD and of the probabilistic calculation engine are presented. Two generic examples are presented for demonstrating the various functionalities of this development and how it can be used for planning and for resource allocation.

VISUALIZATION DRIVER

The VD comprises a desktop tool that leverages CBP data to simulate the utilization of resources, human power and physical assets to various incidents initiated by threats. The sector of the border which is considered contains stations and paths. A user selects the sector of the border which will be considered and its patrol stations (defense nodes). A number of agents along with assets (e.g., ground vehicles, patrol helicopters) are assigned to the stations. Depending on the allocations, a strength score between 1 and 5 is assigned to each one of the stations. This information is used by the ADTree in the probabilistic calculations as explained in the next Section. When an incident occurs and additional resources are needed, patrol stations with available resources respond and provide a certain amount of additional resources. Paths are the routes that threats take during an incident for reaching a target (e.g., a pick-up location inland from the border). Defense nodes can use their resources to engage threats along the paths. Additionally, reinforcements can be exchanged between stations along the paths.

Shared surveillance assets can be assigned by the user to selected path sections (single or multiple paths) of the sector used in the simulations. Examples of such surveillance assets are a tethered aerostat radar system, a drone and a surveillance tower. An aerostat is a fixed ground-based asset that detects traffic when raised. A drone is an air-based asset that can constantly scan a user-defined patrol area. A surveillance tower is a ground-based asset that has a fixed scan area based on its position. A surveillance tower can be either fixed or mobile. The fixed variant has a more extended surveillance area. A relative user defined strength between 1 and 10 is assigned to the surveillance assets. The strength is considered in the probabilistic calculations conducted by the ADTree.

Incidents are generated by threats trying to reach their targets. As threats advance the surveillance assets along the chosen path become visible in the VD. Utilization of assets by defense nodes become visible as they engage the threats. Figure 1 presents a screen shot of a VD simulation.

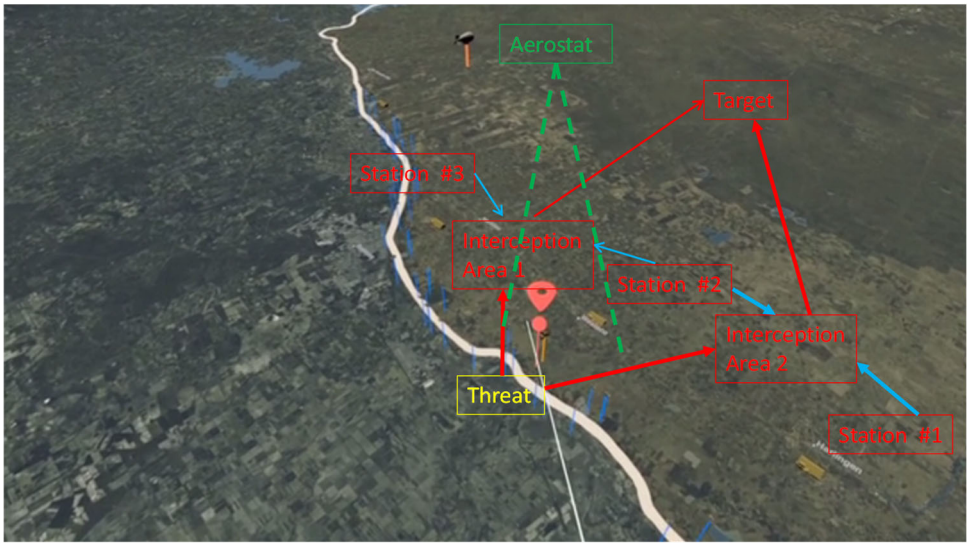

Figure 1. Representative information displayed at the VD

In Figure 1 the threat, the alternative paths, the possible interception locations, the stations and the target are labeled. The VD offers the user visual information on how the incident evolves over time. Information displayed in the VD is used for the probabilistic computations as described next.

PROBABILITISTIC CALCULATIONS IN ADTree

This Section presents the theoretical background of the probabilistic calculations in the ADTree implementation of this paper. The material is divided into three parts, discussing the baseline computations (they take place for both static and dynamic simulations), the dynamic computations that reflect collaboration between threats, and the dynamic calculations for sharing resources between defense nodes.

Baseline Probabilistic Calculations

Each path section or each defense node comprise an element of the ADTree. There is complete freedom defining the structure of the ADTree to reflect the scenario visualized in the VD. Threats follow alternative sequences of path sections and defense nodes to reach a target along each available route. The definition of the stations in the VD identifies the defense nodes and their strength. Offensive (threats) or defensive (path sections and defense nodes) attributes get assigned a strength corresponding to a level between 1 and 5. In this manner, at each path section or at each defense node a match-up between offensive and defensive attributes takes place. The presence of surveillance assets (rated between 1 and 10) increases the defensive strength of the associated paths. Probabilistic calculations are conducted for determining the probability of the threat completing the particular path section or defense node successfully and also the probability of completion without been detected. Figure 2 graphically presents these probabilistic calculations.

The bell shaped curve is the probability distribution function (pdf) for a threat competing against the defense of a path section or a defense node. A Normal distribution is considered and defined by its center value X_C and its standard deviation σ. The center of the distribution X_C is associated with the strength of the threat and is evaluated as:

$$X_C = X_{C_o} - S_T * m \qquad (1)$$

Where X_{C_o} is a constant associated with the relative placement of the pdf in the horizontal axis, S_T is the strength of the threat's attribute exercised in the particular path section or defense node, and the multiplier m determines how influential the strength S_T is in placing the center of the distribution. The higher the strength of the threat is, the more the center of the pdf (and therefore the pdf) moves to the left.

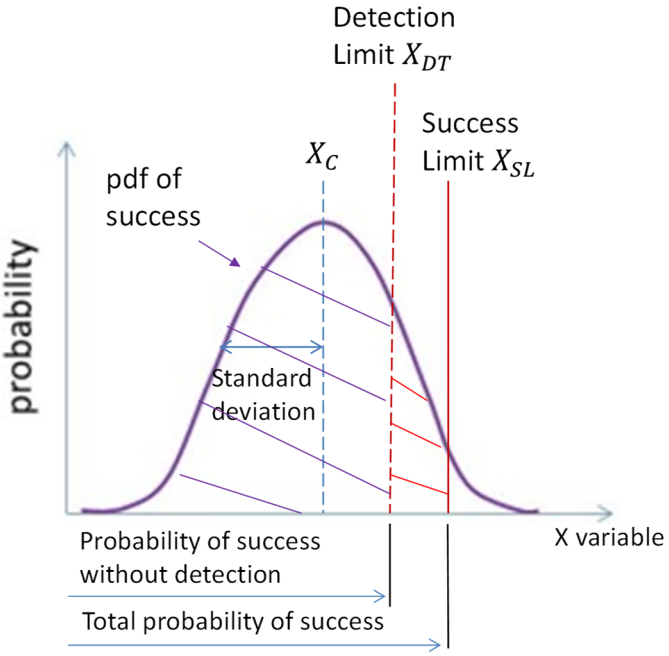

Figure 2. Probabilistic Calculations at Each Path Section or Defense Node of the ADTree

The strength of the defensive capability of the path section or the defense node are reflected in the placement of the variables X_{DT} and X_{SL} with respect to the pdf curve. The area under the pdf up to the point X_{DT} is equal to the

probability of the threat being successful while also remaining undetected. The area under the pdf curve between X_{DT} and X_{SL} provides the probability of the threat being successful but being detected. Therefore, the stronger the defense the more these values shift to the left and when the defense becomes weaker these two values shift to the right. The defensive capability is used in computing variables X_S and X_D. These two variables are used in computing X_{DT} and X_{SL}. X_S is linked with the point up to which the threat will be successful and it is defined as:

$$X_S = X_{S_o} - S_D * m \qquad (2)$$

Where X_{S_o} is a parameter associated with the relative placement of the defensive capabilities in the horizontal axis. S_D is the strength of the defensive characteristic associated with the particular path section or defense node. The multiplier m is common between equations (1) and (2) in order to consistently account for the strengths of the offensive and defensive attributes in the relative placement of X_{DT} and X_{SL} with respect to the pdf. The higher the S_D the more to the left X_{DT} and X_{SL} (that depend on the X_S value) are placed.

The detection limit X_{DT} indicates up to which point in the pdf curve the threat will be successful in completing the path section or the defense node without being detected. It is evaluated as:

$$X_{DT} = X_S - DTF * |X_S| \qquad (3)$$

Where DTF is the detection fraction (acquiring values less than 1), and $DTF * |X_S|$ represents how much to the left of X_S the X_{DT} location should be placed. The better the detection capabilities are, the higher the value of DTF is. For a path section sensor(s) are allocated based on the selections from the VD (e.g., drone, aerostat, surveillance towers) that have preset DTF values. Finally, the location X_{SL} up to which the threat will complete the path section or the defense node regardless of being detected is defined as:

$$X_{SL} = \min(X_S, X_{DT} + X_R) \qquad (4)$$

Where X_R represents the response capability of the defense once the threat is detected. The better the response capability, the smaller the X_R value is and the closer the X_{SL} can be placed to the X_{DT}.

The area under the pdf curve up to the location X_{DT} is equal to the probability P_1 of the threat being successful while remaining undetected. It is evaluated as:

$$P_1 = CDF\left(\frac{X_{DT} - X_C}{\sigma}\right) \qquad (5)$$

Where CDF is the cumulative distribution function operation. The area under the pdf curve between X_{DT} and X_{SL} represents the probability P_2 of the threat being successful after it has been detected:

$$P_2 = CDF\left(\frac{X_{LS} - X_C}{\sigma}\right) - P_1 \qquad (6)$$

Finally, if a threat was already detected at a previous path section or defense node, then only the probability P_3 of the threat being successful while already detected at a prior ADTree element is computed as:

$$P_3 = CDF\left(\frac{UDF * X_{SL} - X_C}{\sigma}\right) \qquad (7)$$

Where UDF is the upstream detection factor (acquiring values less than 1), representing how much to the left the X_{SL} location moves when the threat has already been detected at an upstream element of the ADTree. In this case probabilities P_1 and P_2 are not computed.

The probabilistic calculations at each path and defense node are combined along each possible route between a threat and a target forming a probability tree for determining the final probability of a threat reaching a target. All possible routes are considered for multiple threats and multiple targets. Figure 3 presents a very simplistic ADTree in order to explain how the end result is computed. The left side in Figure 3 depicts the ADTree and the right side the set of

probabilistic computations that take place at each path section and defense node. The meaning of the probabilities inside each box is: p_{i1} is the probability of the threat being successful at the i[th] element (path section or defense node) without been detected; p_{i2} is the probability of the threat being successful at the i[th] element but while it is detected; p_{i3} is the probability of the threat being successful at the i[th] element while it was detected at a previous element.

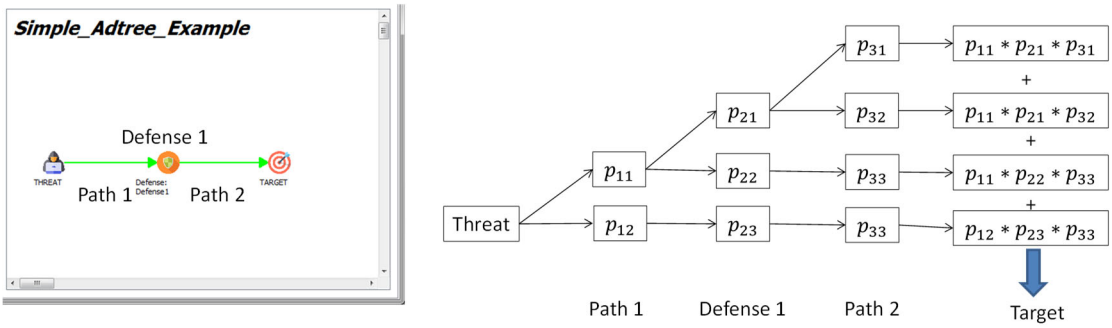

Figure 3. Simplistic ADTree for presenting the associated probabilistic analysis

In the ADTree implementation discussed in this paper, all probabilistic computations are conducted automatically, regardless of how extensive or complicated the ADTree is. Additionally, the parameters used in the equations for defining the probability distributions and the various detections levels ($X_{C_o}, X_{S_o}, S_T, X_{DT}, X_{SL}$, DTF values for sensor(s) assets) can easily be adjusted by the user, if subject matter expert opinions or data for calibrating the probabilistic calculations are available.

Dynamic Simulations for Threat Collaboration

The interaction between multiple threats during an incident displayed in the VD provides information about the hardness of the path section/defense node encountered by a leading threat to a trailing threat. This information is used to adjust the probability of the trailing threat to take alternative path sections when multiple choices are available. In the ADTree the probability of taking a path does not change the total probability of success for a threat completing a route; it only determines the probability of selecting the route. These two probabilities are used for determining how to harden the most likely routes and how the likelihood of a route may chance after it is hardened.

The threats initiate their activities based on a user-defined order. It is assumed that the relative starting order is preserved throughout the simulation. The success that a leading threat experiences along a sequence of alternative paths that connect a defense node to other defense nodes is used for adjusting the path selection for the immediately trailing threat. In order to explain how the process works a part of an ADTree presented in Figure 4 is considered.

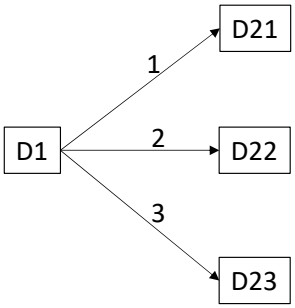

Figure 4. Example for Explaining the Impact of the Outcome at a Path Section on the Path Section Dynamic Selection

When a leading threat takes path section i, $i = 1, 2, or\ 3$ it will experience a probability of success in that path equal to ps_i. If ps_i is greater than 0.5, then the threat is more likely to succeed and if it is less it is more likely to fail. This information is used for adjusting the path selection of the trailing threat accordingly. The path selection probabilities are updated as:

$$\Delta p_i = \max(-p_i, \quad \min(1 - p_i, \quad ps_i - 0.5)) \qquad (8)$$

$$\bar{p_i} = p_i + \Delta p_i \qquad (9)$$

$$\bar{p}_{j,j\neq i} = p_{j,j\neq i} - \frac{p_{j,j\neq i}}{1-p_i}\Delta p_i \qquad (10)$$

Where Δp_i is the adjustment made to the selection probability of path section i for the trailing threat, $\bar{p_i}$, $\bar{p}_{j,j\neq i}$ are the adjusted path selection probabilities for the trailing threat. The above procedure adjusts the selection probability of the path selection based on the calculated probability of success of the leading threat (i.e. increases if it is higher than 0.5 and decreases if it is lower than 0.5), and makes certain that the updated selection probability stays within 0 and 1. The selection probabilities of all other path sections starting from the same defense node are updated in a proportional manner, making certain that the summation of all updated selection probabilities is equal to 1.0.

The procedure for updating path selection probabilities in threat/defense interaction is the same as the above case for the threat/path section interaction. However, this time the procedure will be repeated for all paths leading to the current defense node. In the example in Figure 5, if the leading threat attacked defense node D22, then the path updating probability procedure will be performed on both path D11→D22 and path D12→D12. The procedure will update the selection probabilities of path D11→D22 and path D12→D22. It will also update the selection probabilities of all other paths starting from D11 (i.e. path D11→D21) and D12 (i.e. path D12→D23) to make certain that the selection probabilities of all path sections starting from the same defense node sum up to 1.0.

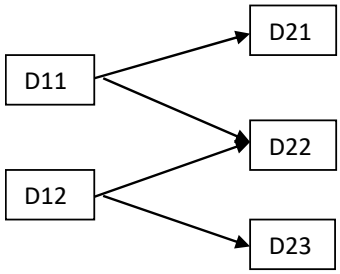

Figure 5. Example for Explaining the Impact of the Outcome at a Defense Node on the Path Section Dynamic Selection

When a threat goes through a route, the accumulated probability of success is calculated and monitored. When the accumulated probability of success is lower than a threshold value such as 0.5, then the threat is considered as neutralized and from that point forward, it won't be able to send information to trailing threats and the above procedure of updating the path selection probability for the trailing threat is terminated.

Dynamic Simulations for Collaboration between Defense Nodes

The defense resource reallocation is done automatically when the dynamic calculation is selected. When a threat arrives at a defense node, if the threat strength is lower or equal to the defense strength, defense resource reallocation is not triggered; if the threat strength is higher than the defense strength, then the defense node will receive reinforcement from its backup defense nodes. The backup nodes are determined automatically, based on the path section connections between the defense nodes. In the example of Figure 5, defense D21 and D22 are considered as backup nodes to defense D11, and defense D22 and defense D23 are considered as backup nodes to defense D12. Downstream nodes are considered as backup to upstream nodes.

The goal of the defense resource reallocation is to increase the strength of the current defense to match the strength of the threat. The requested amount of reinforcement equals to the threat strength minus the defense strength. The total available amount of reinforcement strength is the sum of defense strength of all backup stations. If the available amount is larger than the requested amount, the defense gets the full requested amount to match the threat strength, and the contributions from the backup units are proportional to their available strength. If the available amount is less than the requested amount, then the defense gets all resources from its backup units even though the reinforced strength

is still lower than the threat strength. According to the aforementioned approach of defense resource reallocation, the strength of defense elements is updated based on the following equations:

$$\Delta s_i = \min\left(s_t - s_i, \quad \sum_{j=1}^{n_i} s_j\right) \qquad (11)$$

$$\bar{s_i} = s_i + \Delta s_i \qquad (12)$$

$$\bar{s_j} = s_j - \frac{s_j}{\sum_{j=1}^{n_i} s_j} \Delta s \qquad (13)$$

Where Δs_i is the increase in the strength of defense node i, s_t is the strength of the threat at the particular matchup at defense node i, $j = 1, \dots, n_i$ are all defense nodes that can provide resources to defense node i, s_j are the strengths of the j defense nodes before providing resources to defense node i, $\bar{s_i}$ is the adjusted strength of defense node i after receiving the resources, and $\bar{s_j}$ is the adjusted strength of the defense nodes $j = 1, \dots, n_i$ after the have provided resources to defense node i.

Due to the defense resource allocation, if the current threat is able to successfully overcome the reinforced defense node, it will encounter a weaker defense in its remaining route because the strength at some downstream defense nodes is reduced. In addition, any trailing threat will face the updated defense strength after the defense resource reallocation. When the accumulated probability of success for a threat becomes lower than a threshold value (such as 0.5) then the threat is considered to be neutralized. From that point on, the defense resource reallocation is terminated.

Surveillance Assets in Probabilistic Calculations

As a user introduces surveillance capabilities (aerostat, drone, surveillance tower, etc.) in the VD their presence hardens the defense characteristics of the paths associated with them. When an asset is linked with multiple paths then it is considered that it only spends part of the time surveilling each path. The strength of a path is increased using equation (14).

$$STR\_P = \max\left(STR\_P_0 + \sum_{i=1}^{n} 0.2 * \frac{STR\_S_i}{P\_S_i} \quad , \quad 5.0\right) \qquad (14)$$

Where: STR_P_0 is the original strength of a path, STR_P is the updated strength of the path, n is the number of sensors connected to a path, STR_S_i is the strength of the sensor (acquiring a user defined value between 1 and 10), and P_S_i is the number of paths that the ith sensor surveilles (there is partial coverage if associated with multiple paths). Parameter STR_P_0 acquires a user defined value between 0 and 5. The original strength increases based on the type of sensors, the number of sensors and the coverage level that each sensor provides. Based on equation (14) the upper limit of how much the strength of a path can increase is equal to 5.

The strengths of the sensors STR_S_i acquire a ranking between 1 to 10. These values are user defined and a sample set of values for the surveillance sensors which are available in the VD and the ADTree are summarized in Table 1.

Table 1. Sample Values for Strengths of Available Sensors

Name	Drone	Aerostat	Remote Video
Strength	7	7	5
Name	Mobile Tower	Ground Sensor	Vehicle Detection
Strength	6/7	6	6
Name	Fixed Camera	Integrated Tower	Lidar Camera
Strength	6	6/7	7

Any of the user defined parameters in the ADTree has default values but the user also has the ability to prescribe a different set of numerical values through an easy to edit set up file.

EXAMPLES

Two generic border patrol applications are presented in this Section. The scenarios and the data are made up and do not represent any actual situations. A generic multi-layered defense against multiple threats is analyzed for demonstrating the dynamic simulations. A simulation associated with the scenario visualized in Figure 1 is also performed for demonstrating the interaction between the VD and the probabilistic analysis.

Dynamic Resource Reallocation Example

An ADTree example that includes multiple threats and a multi-layered defense is presented in order to demonstrate some aspects of the dynamic resource allocations. Such ADTree situations can be encountered in border patrol applications (Immigration and Naturalization Service, 2002) where resources from multiple defense nodes are shared to mount a more effective response when facing capable threats. In this example there are three threats, seven defense nodes, fourteen path sections, and two targets; the ADTree is depicted in Figure 6. The strengths of all path sections are uniformly set to low in order to emphasize on the resource reallocation between defense nodes. The strengths of the threats are presented with numerical values in red color. The strengths of the defense nodes are presented with numerical values in blue. All threats are more capable than each one of the defense nodes in order to demonstrate the value provided by the resource reallocation when overall resources are limited.

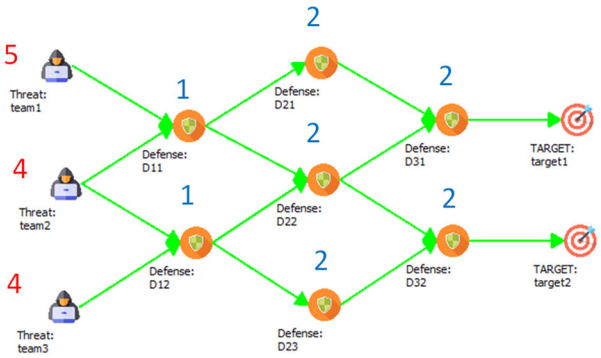

Figure 6. ADTree Example for Resource Reallocation

In a static simulation when there is no resource reallocation, all routes exhibit the same hardness and all the threats are highly successful with highest probabilities of success equal to 0.98 for Team1, 0.92 for Team2, and 0.92 for Team3. In the dynamic simulation, the order of attack for the threats is set to be: Team2, Team1, and Team3. The results for each threat are discussed based on their attacking order. Overall, Team 2 is not very successful in all routes, because the defense has all the resource available for reallocation to counter Team2 in any route it selects. The best route for Team2 is to avoid D22 in the middle (by taking either one of the two routes D11→D21→D31→Target1 or D12→D23→D32→Target2), because D22 has two backup defense nodes while D21 and D23 each has only one backup defense node. The best route for Team2 exhibits probability of success equal to 0.64.

Figure 7 illustrates the resource reallocation for one of the two best routes (i.e. D11→D21→D31→Target1). Figure 7a shows the reallocation when Team2 reaches defense node D11. D11 receives reinforcement from D21 and D22. Each backup defense node sends 1.5 reinforcement to D11, so that the reinforced strength of D11 becomes 4, which is equal to the threat strength (Eq. 11 and 12). Consequently, the remaining strengths of D21 and D22 are lowered to 0.5 (Eq. 13). Figure 7b shows the defense reaction when Team2 arrives at D21. D21 receives reinforcement from D31. Even though D21 could receive reinforcement of strength 3.5 to match the threat strength, D31 has a total strength of 2.0. Therefore D31 sends all its strength to D21, making the reinforced strength of D31 to be 2.5 while the remaining strength of D31 becomes 0.

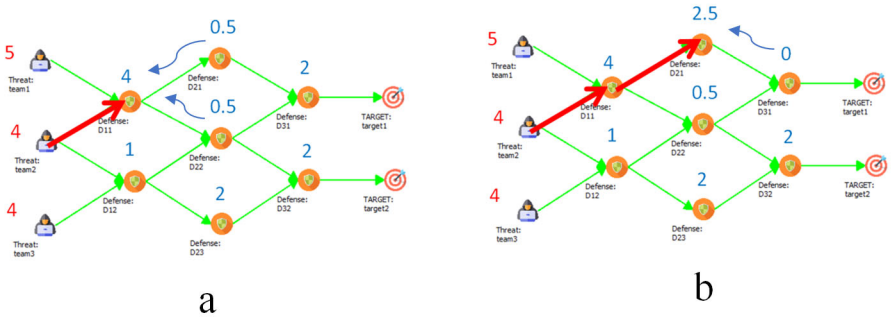

Figure 7. Resource Reallocation Triggered by Team2

In this route Team2 would encountered defense nodes with strengths (1, 2, 2) during a static analysis while in the current dynamic simulation it encounters strengths (4, 2.5, 0). Although there is an increase in the probability of the threat's success at defense node D31, there is a significant reduction in its probability of success at D11 and also a reduction in D21, resulting in a reduced overall probability of 0.64.

Team1 is directly following Team2. Figure 8a depicts the defense landscape that Team1 faces at the starting point. The simulation results indicate that the best route for Team1 is to follow the same route as Team2. The best route (D11→D21→D31→Target1) for Team1 has 0.84 probability of success. Figures 8b and 8c illustrate the route and the defense reallocation when Team1 goes through the route. Figure 8b shows the reinforcement when Team1 reaches D11. Since Team1 has higher strength than D11, reinforcement is provided from D21 and D22. Proportionally, D21 sends 0.83 strength to D11 while D22 sends 0.17 strength to D11. The reinforced strength of D11 becomes 5.0 which is equal to the threat strength of Team1. Accordingly the remaining strengths of D21 and D22 are lowered to 1.67 and 0.33 respectively. Figure 8c shows the state of the defense nodes when Team1 reaches D21. The backup defense node D31 has no strength (0 strength) left. Therefore, no defense resource reallocation is performed. In this route Team1 would have encountered defense nodes with strengths (1, 2, 2) during a static simulation. Currently it encounters defense nodes with strengths (5, 1.67, 0). This leads to a probability of success of 0.84 which is lower than the highest probability of 0.98 determined by the static analysis.

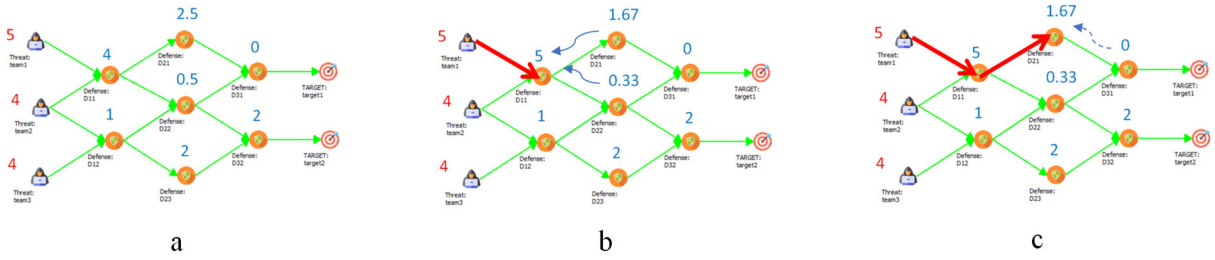

Figure 8. Resource Reallocation Triggered by Team1

Finally, Team3 benefits from the prior two threats drawing resources to their routes, and achieves a best probability of success equal to 0.91 that is almost the same with the static calculation. Overall, in this example the threats are highly skilled and face a layered defense with defense nodes of relatively low individual initial strength. The dynamic resource reallocation benefits the defense by enabling transition of resources and reduces (with variable effectiveness) the probability of success of the threats.

Example associated with a VD visualization

An ADTree associated with the visualization presented in Figure 1 is constructed and depicted in Figure 9. The example is simple but representative of how a scenario defined in the VD can be analyzed by the ADTree. This provides content about how well the visualized defensive layout can prevent a threat from reaching its target. In Figure 9 relatively low strengths (2 out of 5) are assigned to the four paths and the three defense stations. This situation is representative of scarce resources. A relative high (4 out of 5) strength is assigned to the threat. The objective of

the threat is to evade detection and apprehension in any of the paths and at the two defense interception areas. An aerostat is available to surveille the two forward paths similar to Figure 1. The presence of this resource hardens the two paths based on equation (14). Due to the symmetry in the structure of the ADTree and in the strengths of the defense elements, the probability of success of the threat is the same (equal to 36%) regardless of which route (upper or lower) that the threat takes. A 36% probability of success means that if the threat represents 100 attempts to breach the border and evade the particular defense layout, 64 would be apprehended and 36 would become getaways.

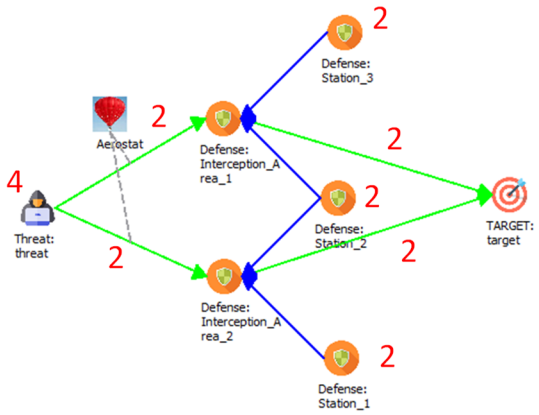

Figure 9. ADTree associated with Visualization presented in Figure 1

The user can decide to increase the surveillance resources by introducing a drone to patrol the two forward paths, while retaining the rest of the resources the same. When this modification is applied the strengths of the paths increase even more and the corresponding ADTree analysis assesses a reduced probability of success for the threat to 23%. In this manner a user can define different scenarios in the VD and receive information about how well the defense will perform. By adding or eliminating resources in the VD the user can also experience the impact of the decisions in the end results (e.g., number of getaways) that the modifications will have.

SUMMARY

This paper presents a capability of a VD combined with a probabilistic calculator for visualizing and assessing incidents encountered in border patrol activities. The training value of this capability is associated with the feedback provided to the user about the effectiveness of each visualized scenario. The effectiveness of the defense increases when the probability of success of the adversaries reaching their objective is reduced. When the user changes the allocation of resources in the scenario that is visualized, the probabilistic calculations provide direct feedback since the probability of success for the adversaries is either increased or reduced. The user defines the structure and the capabilities of the defense in the VD and views the incidents as they evolve. The probabilistic calculator determines the probability of success of the adversaries for all possible ways that they can achieve their objectives. The match-up between the capabilities and the strengths of the adversaries vs the defense is considered in the computations at every step along each path that leads an adversary to an objective. The consequences of the defense detecting a threat are accounted in the analysis. Dynamic calculations can be performed for capturing both the interaction between leading and following threats and the sharing of resources among defense elements. The simulation results can be used for determining how to harden a defense and how to best utilize limited resources against adversarial attacks. Associating increases in the strength (and therefore the cost) of defensive capabilities, with the resulting reduction of the probability of success for the adversaries, creates trade-off information between increases in cost and increases in the resulting safety. Studying alternative ways of distributing a fixed amount of resources within a defensive layout can identify the allocation which provides the maximum safety. Additionally, the effectiveness of alternative defense layouts can be compared for determining their relative ranking.

REFERENCES

1. Law Enforcement Simulators (2024); https://www.virtra.com/overview-le/

2. Collins Aerospace Simulation and Training (2024); https://www.collinsaerospace.com/what-we-do/industries/military-and-defense/simulation-and-training/training-systems
3. Kripa, E. , Mueller S. (January 26 2018), The Architects Newspaper, https://www.archpaper.com/2018/01/us-government-mock-ports-entry/
4. US Customs and Border Protection (2024); https://www.cbp.gov/frontline/cbp-use-force-practicing-unexpected
5. Gutierrez, E. (2014), "A visualization and simulation tool that will generate effective patrolling strategies to protect the US borders from illegal intrusion using game theoretic methods and models," Master's Thesis, Intelligence and National Security Studies Program, The University of Texas at El Paso,.
6. Fraile M., Ford M., Gadyatskaya O., Kumar R., Stoelinga M., Trujillo-Rasua R. (2016), Using Attack-Defence Trees to Analyse Threats and Countermeasures in an ATM: A Case Study, In: Horkoff J., Jeusfeld M., Persson A. (eds) *The Practice of Enterprise Modelling. PoEM 2016.*
7. Kordy, B., Mauw, S., Radomirovic, S., and Schweitzer, P. (2014), Attack-Defense Trees, *Journal of Logic and Computation*, 24(1):55-87.
8. Mauw, S., Oostdijk, M. (2006), Foundations of Attack Trees, *In Proc. of ICISC'05, volume 3935 of LNCS*, pages 186-198. Springer.
9. Immigration and Naturalization Service (2002), *Draft Programmatic Environmental Impact Statement for U.S. Border Patrol Activities within the Border Patrol Areas of the Tucson and Yuma Sectors Arizona*. Washington, DC.