Probabilistic Analysis for Structuring an Effective Defense against Adversarial Attacks

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

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

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

ABSTRACT

An Attach Defense Tree (ADTree) provides a structured approach of graphically considering the steps that a threat can take in order to overcome a defensive layout and reach a target. Many security applications can be modeled using an ADTree. In this paper an implementation is presented that computes the probability of success of each threat reaching a target along each possible route. A sequence of path sections and defense nodes are creating the routes between each threat and each target. Multiple threats and multiple targets can be considered. At each path section and at each defense node a probabilistic matchup with each threat is performed. The defensive and offensive capabilities at each matchup determine the outcome. The results are combined for determining the overall probability of success for a threat completing a route. The probability of a threat following each alternative route is also evaluated. The information generated by the ADTree calculations can be used for determining how to best structure a defense layout and how to allocate resources for improving the hardness against adversarial attacks. Static or dynamic calculations can also be performed. The latter can account for interaction between leading and trailing threats when determining the probability of taking a route and for the sharing resources between defense nodes. The theoretical background of the probabilistic calculations is presented and several applications are discussed in order to demonstrate the type of information generated by the ADTree analysis and how it can be used for hardening a defense.

ABOUT THE AUTHORS

Nickolas Vlahopoulos has been a Professor at the University of Michigan for 25 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 23 PhD students.

Syed Mohammad is the Director for the Modeling and Simulation Technology Center at the Department of Homeland Security Science and Technology Directorate. 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 17 years of experience and has published 29 technical papers.

Sungmin Lee is a R&D engineer at Michigan Engineering Services; he has 12 years of experience and has published 9 technical papers.

Probabilistic Analysis for Structuring an Effective Defense against Adversarial Attacks

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

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

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

INTRODUCTION

There are many applications where a single adversarial threat or a group of collaborating threats are attempting to reach their targets by breaching a protective defense layout. Drug smuggling through the US border, an active shooter attack, and a cybersecurity application are just a few such examples. The Department of Homeland Security (DHS) has many publications describing how critical preparedness is in protecting our Nation, a sample of them (DHS, 2019), (DHS, July 2018), (DHS, May 2018), provide representative information.

The graphical formalism of an Attack Defense Tree (ADTree) has been 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, 2016), (Kordy, 2014), (Mauw, 2006). An ADTree provides a structured way to visualize alternative paths for an attack, consider the placement and utilization of defense resources, and support decision making on how to best structure an effective defense with the least amount of resources (Powell, 2005). (Ingolds, 2013) summarizes well how risk analysis can be performed using the tree structure and utility theory. Probabilistic calculations have also been used instead for evaluating the effectiveness of the defense using an ADTree. Such probabilistic calculations can be based on Boolean operations (Korby, 2013), Bayesian networks (Frigault, 2008), linear programming methods (Brown, 2006), and the Markov Chain approach (Aslanyan, 2016).

The capability presented in (Korby, 2013) performs quantitative analysis of an ADTree by integrating attack and defense components which encapsulate subject matter expert input. Boolean operations are performed for determining metrics such as the minimal cost of an attack or the expected impact of a defensive measure. Their work uses the notion of attributes for specifying security metrics. A bottom-up algorithm makes use of the attributes for calculating values for the discrete metrics of interest in a quantitative manner. In (Frigault, 2008) the ADTree graph is considered as a directed acyclic graph that encodes the conditional independencies for all the nodes, thus comprising a Bayesian network. In their work they utilize a common vulnerability scoring system to populate the ADTree for ensuring that consistent data is used in the evaluations. The probabilities at the nodes of their system are directly obtained from the common vulnerability scoring system designations. In (Brown, 2006) they view the entire ADTree as an optimization of the infrastructure system with the system's cost comprising the objective function. A bi-level program is formulated for maximizing the defender's minimum operating cost with respect to the defender's activities and the attacker's decisions. Linear programming was used for solving the optimization. A game-theoretic approach, translating the ADTree into a two player stochastic game is presented in (Aslanyan, 2016). They employ probabilistic model checking techniques to conduct the analysis. Information about the temporal ordering of actions or sub goals is considered. The probability of success or failure of individual basic actions take the form of a discrete-time Markov chain. The two player stochastic game captures the set of all strategies available to the attacker and to the defender.

In this work the graphical representation of the ADTree is used for structuring probabilistic calculations 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 (e.g. mobility,

evasiveness, speed, etc.) along with a capability level assigned to each attribute. 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, defenders, detection cameras, etc.) are assigned to both a path section and a defense node along with an associated strength level. 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 combined by viewing the ADTree as a probability tree when determining the probability of each threat successfully completing each route and reaching each one of the available targets.

The basic technical elements that facilitate the aforementioned computations are discussed first. Since this ADTree capability is general and not application specific, three different generic examples are presented for demonstrating the various functionalities of this ADTree development and how it can be used for planning and for resource allocation.

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 application of interest. Threats follow alternative sequences of path sections and defense nodes to reach a target along each available route. Offensive (threats) or defensive (path sections and defense nodes) attributes can be defined and a strength can be assigned to each one (using a linguistic term: low, medium-low, medium, medium-high, or high, corresponding to a level between 1 and 5, or any other user defined numerical range). In this manner, at each path section or at each defense node a match-up between offensive and defensive attributes takes place. 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 1 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 user defined 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.

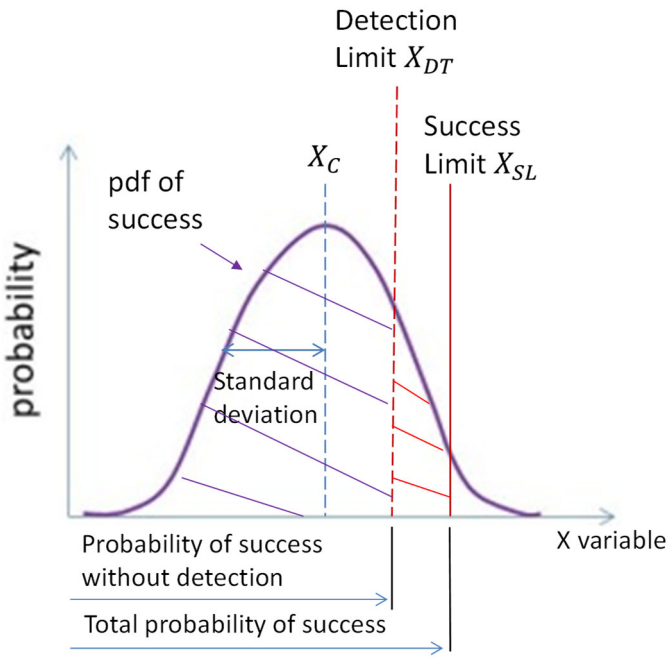

Figure 1. Probabilistic Calculations at Each Path Section or Defense Node of the ADTree

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 user defined 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 a user can select and allocate sensor(s) from a list of sensors (e.g. ground microphones, drone, cameras, etc.) 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 2 presents a very simplistic ADTree in order to explain how the end result is computed. The left side in Figure 2 depicts the ADTree and the right side the set of 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.

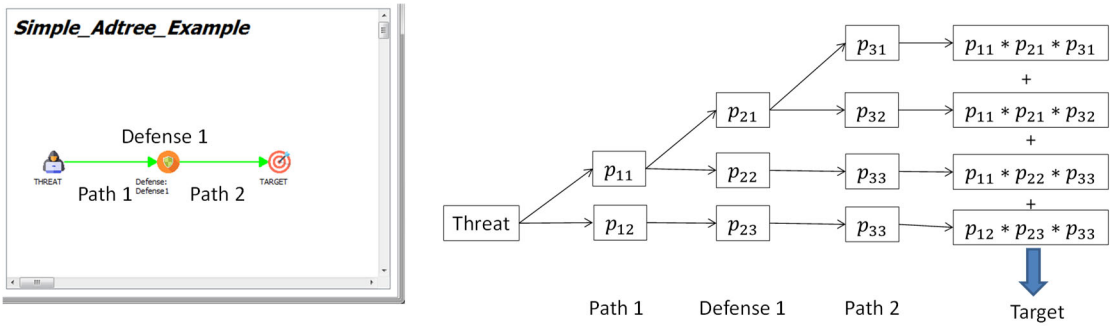

Figure 2. Simplistic ADTree for presenting the associated probabilistic analysis

In the ADTree implementation discussed in this paper, all probabilistic computations are conducted automatically, regardless of how extensive or complicated the ADTree is.

Dynamic Simulations for Threat Collaboration

The interaction between multiple threats 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 3 is considered.

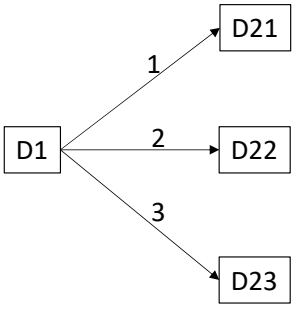

Figure 3. Example for Explaining the Impact of the Outcome at a Path Section on the Path Section Dynamic Selection

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 4, 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.

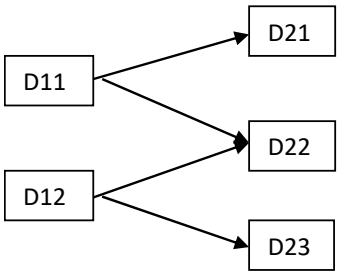

Figure 4. Example for Explaining the Impact of the Outcome at a Defense Node on the Path Section Dynamic Selection

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 Threat Collaboration

In the current implementation, the defense resource reallocation is done automatically if 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 4, 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 units. 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.

ADTREE EXAMPLES

In order to demonstrate the versatility of the ADTree modeling security scenarios of interest three different and generic applications are presented in this Section. First, a cybersecurity set up from the open literature (2020) is analyzed and the ADTree is used for modifying the strengths of the defense nodes in order to exhibit equal hardness at the various modes of attack that an adversary may choose to use. A school shooting situation from the News is analyzed; the impact of a trained armed guard, the distance of a classroom from the entry point, and introducing additional hallway interior doors are evaluated. Finally, a generic multi-layered defense against multiple threats is analyzed for demonstrating the dynamic simulations.

Cybersecurity Example

A cybersecurity configuration from the open literature (Xu, 2020) is used for showing the utility of the ADTree in this area of interest to DHS. Figure 5 presents the ADTree for an attack on the supervisory control and data acquisition system of a power generator. The goal of the threat is to trip the circuit breaker of the power system. The threat has five alternative routes to pursue its objective by launching an attack either on the front end processor (route 1), on the status evaluation module (route 2), on the human-machine interface (route 3), on the remote terminal unit (route 4), or on the relay (route 5). Each alternative is represented as a different route from the threat to the target in Figure 5, organized from the top to the bottom. Five attacker characteristics are considered: eavesdropping, port scanning, firewall bypassing, data decoding, and password decoding (for this example they are all set to a medium level of capability). The strengths of the defensive nodes for the initial set-up are presented in blue color in Figure 5. The defensive setup for routes 1, 3, 4, and 5 are identical in order to verify that as expected the probability of success of the threat will be the same. An equal probability of the threat selecting each one of the five routes is also considered. The probability of success for the threat tripping the circuit breaker is 0.3093 for routes 1, 3, 4, and 5; while the probability of success for route 2 is 0.0348 (much lower since it is the most complex way to attack). Given this knowledge and by assuming that increasing or decreasing by a unit the strength of any defense node is of equal cost, the strengths of some of the defense elements are adjusted to the red values in Figure 3. In this manner, elements along route 2 now exhibit lower strength, while elements along the rest of the routes have been hardened. The summation of the strengths of all defense elements remains the same in the two setups. In this manner, the probability of success of the threat for routes 1, 3, 4, and 5 gets reduced to 0.1302, while for route 2 it is increased to 0.1352. Nevertheless, since the probability of the threat taking any one route is the same, it is more preferable to redistribute the original resources to generate a balanced defense along any possible route. This demonstrates how one can use the ADTree to determine the distribution of resources. The ADTree evaluates alternatives rapidly, identifies weaknesses, and the best way for hardening the defense. Since the probability of each attack route is considered to be the same, a defense layout that presents equal hardness for all possible routes of attack is preferable, and configured using the ADTree.

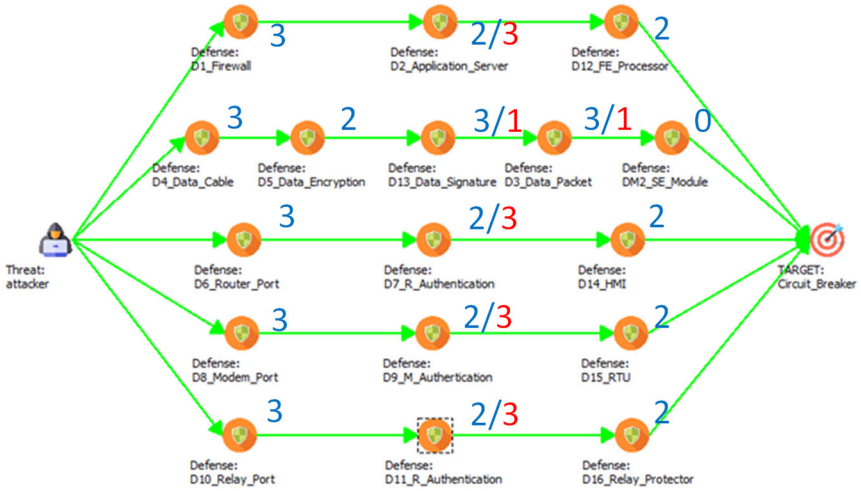

Figure 5. ADTree for a cybersecurity scenario from the open literature (Xu, 2020)

School Shooting Example

The second example discusses a school shooting incident from the News (ABC News, 2012). The capabilities of the threat and of the defense are generic and only the school layout is preserved from the original source. Figure 6 presents the building layout and the corresponding ADTree. In this set-up the defense is mainly provided by the defense nodes. In general path sections can be assigned defensive capabilities, but in this example only the path sections between the "Guard" defense node and the "Classroom Door" defense nodes offer defensive hardness depending on the vicinity of the classrooms to the main entrance. There are three alternative targets, Rooms A, B, and C, representing respectively classrooms near the main entrance, the classroom closest to the main entrance out of the three, and the classroom furthest from the main entrance.

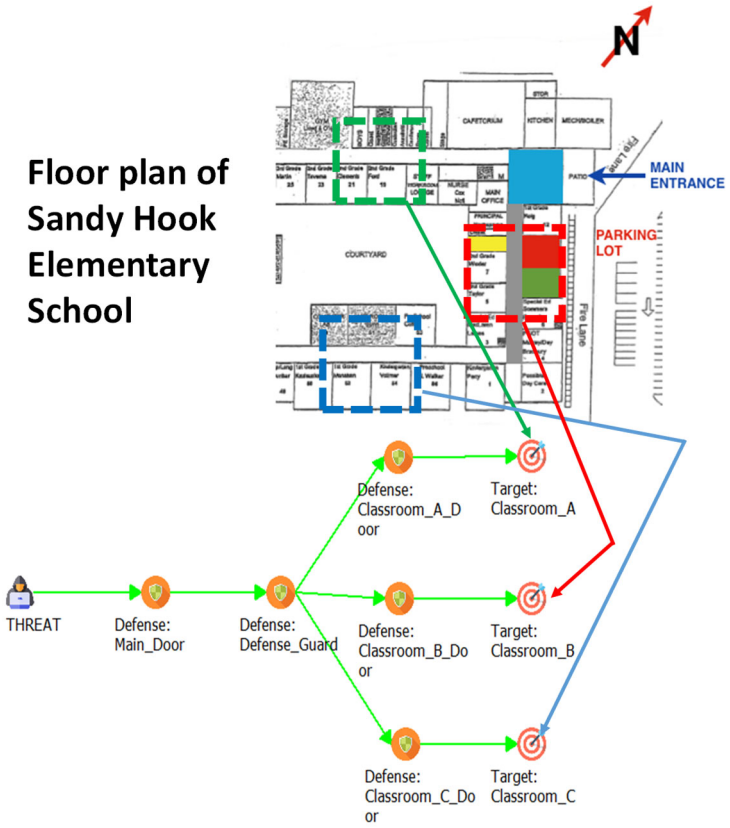

Figure 6. ADTree for school shooting example based on a layout from the News (ABC News, 2012)

Table 1 summarizes the capabilities of the threat, their associated levels, and the match-ups at each one of the defense nodes. The defense attributes used at each match-up and their strengths are included. Three different levels of training are considered for the guard in order to demonstrate how increasing investment in human resources influences the outcome of the analysis. The far right column contains information about additional defense nodes included in a modified ADTree layout (Figure 7).

Table 1. Summary of Threat Capabilities/Levels and Match-ups at Defense Nodes

Threat Capability/Level	**Baseline Configuration Defense Node/Level**	**Additional Defense Node/Level**
Disguise/medium high	Main Door/medium	
Shooting/medium high	Guard/(medium low, medium, medium high)	
Door bypass/medium high	Classroom A Door/low Classroom B Door/low Classroom C Door/low	Interior Corridor Door 1/medium high Interior Corridor Door 2/medium high

The results for the probability of success of the threat reaching each one of the three classrooms for the three levels of guard capability are summarized on the left side of Table 2 under the results for the baseline configuration. There are two main observations in the results for the baseline configuration. First, the probability of success when Classroom C is the target is the lowest of the three because it exhibits the longest distance from the entrance. This allows for more time to barricade the classroom door and evacuating the classroom to the exterior of the building. Thus, placing classrooms as far as possible from a single guarded entry point of the building allows for more reaction time in case of an emergency. The second observation is that only a well-trained armed guard who matches the capabilities of a capable attacker can make a significant difference in the overall probability of success of the threat.

Table 2. Summary of Probability of Success for the Threat in School Shooting ADTree Example

Guard capability	Target	Baseline ADTree	Modified ADTree
Low-Medium	Classroom A	0.86	0.43
	Classroom B	0.94	0.49
	Classroom C	0.46	0.23
Medium	Classroom A	0.81	0.41
	Classroom B	0.89	0.47
	Classroom C	0.43	0.21
Medium-High	Classroom A	0.43	0.21
	Classroom B	0.49	0.25
	Classroom C	0.23	0.11

A structural modification is introduced in the building layout by adding two interior locked corridor doors that restrict access to the two main hallways at their entrance. The ADTree is modified accordingly and the updated layout is presented in Figure 7. A strength of medium-high is assigned to the two interior doors against the medium-high "door by-pass" offensive capability of the threat.

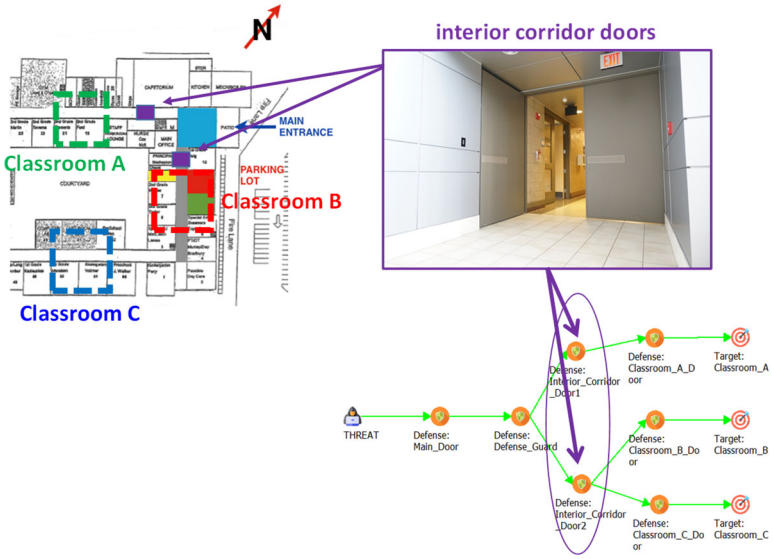

Figure 7. Addition of Interior Corridor Doors in the School Building

The probability of success of the threat against the three targets is summarized in the right column of Table 2. The main observation is that the addition of the interior locked corridor doors hardens significantly the defense and reduces the probability of success of the threat, regardless of the guard's capabilities.

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 (INS, 2002) or when protecting high value assets (DHS, 2018) 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 8. 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.

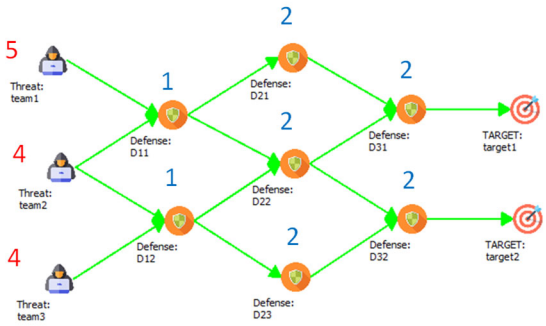

Figure 8. ADTree Example for Resource Reallocation

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 9 illustrates the resource reallocation for one of the two best routes (i.e. D11→D21→D31→Target1). Figure 9a 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 9b 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.

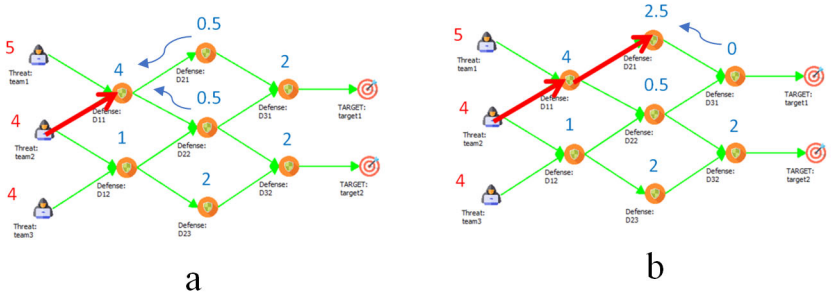

Figure 9. Resource Reallocation Triggered by Team2

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 10a 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 10b and 10c illustrate the route and the defense reallocation when Team1 goes through the route. Figure 10b 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 10c 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.

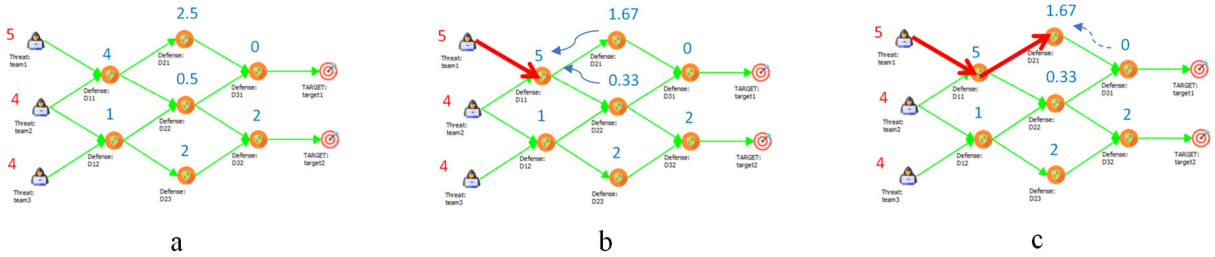

Figure 10. Resource Reallocation Triggered by Team1

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.

SUMMARY

The ADTree capability presented in this paper combines a structured approach of graphically considering the steps that adversaries can take in order to overcome a defensive layout and reach a target, with rigorous probabilistic calculations. The latter determine 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 presented ADTree capability is easy to use since the layout is generated graphically within a dedicated user interface and all computations are performed automatically. The ADTree is very flexible and can model a wide variety of security scenarios. 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. The aforementioned modeling and simulation capabilities of the ADTree can be used for planning and for investigating multiple alternatives fast.

ACKNOWLEDGEMENTS

This research was supported by the Department of Homeland Security Science and Technology Directorate, contract No. 70RSAT19C00000046.

REFERENCES

ABC News, (2012), https://abcnews.go.com/US/fullpage/newtown-ct-shooting-timeline-sandy-hook-elementary-school-18014080

Aslanyan, Z., Nielson, F., & Parker, D. (2016). Quantitative Verification and Synthesis of Attack-Defense Scenarios. In *Proceedings of the 29th IEEE Computer Security Foundations Symposium* (CSF 2016).

Brown, C., Carlyle, M., Salmeron, J., Wood, K., (2006), Defending Critical Infrastructure, *Interfaces*, Vol. 36, No. 6, pp. 530-544

Department of Homeland Security, (2019), *FY 2018-2020 Annual Performance Report*, Office of the Chief Financial Officer, Office of program Analysis and Evaluation.

Department of Homeland Security, (July 2018), *Securing High Value Assets* Office of Cybersecurity and Communications, Federal Network Resilience Division.

Department of Homeland Security, (May 2018), *United States Secret Service, FY 2018-FY2022 Strategic Plan*.

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*.

Frigault, M., Wang, L., (2008), Measuring Network Security Using Bayesian Network-Based Attack Graphs. *In: COMPSAC, 2008,* pp. 698–703.

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.

Ingolds, T., (2016), Attack Tree-based Threat Risk Analysis, Amenaza Technologies Limited, Calgary, Alberta T3H 5Z9, Canada.

Kordy, B., Mauw, S., Radomirovic, S., and Schweitzer, P., (2014), Attack-Defense Trees, *Journal of Logic and Computation*, 24(1):55-87.

Kordy, B., Kordy, P., Mauw, S., Schweitzer, P., (2013), *ADTool: Security Analysis with Attack-Defense Trees*, arXiv:1305.6829v2.

Mauw, S., Oostdijk, M., Foundations of Attack Trees, (2006), *In Proc. of ICISC'05, volume 3935 of LNCS*, pages 186-198. Springer.

Powell, R., (2005), *Defending Against Terrorist Attacks with Limited Resources*, Department of Political Science, University of California, Berkeley, CA 94720-1950.

Xu, B., Zhong, Z., and He, G., (2020), A Minimum Defense Cost Calculation Method for Attack Defense Trees, *Security and Communication Networks*, Article ID 8870734.