SAND2014-16093D

Access Delay Visualization Tool

iSAFE
Interns for Security, Arms control and Force protection Engineering

Manager:
Shawn Taylor
6612/6613

Bryan Watson
New Mexico Tech
PhD in CS, May 2017

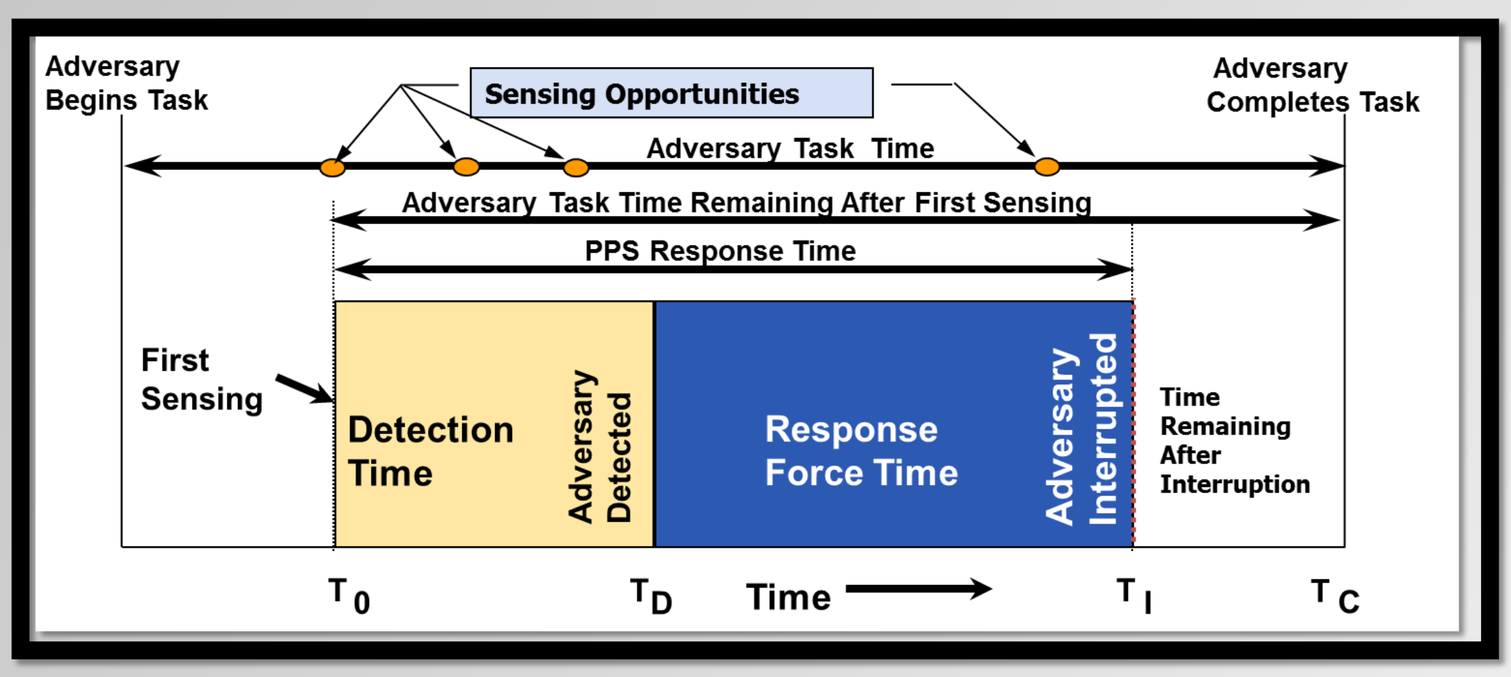
Clayton Smith
Missouri University of S&T
MS in Comp E, Dec 2014

Joshua Herman
Missouri University of S&T
BS in CS/CE, May 2016

Project Mentor:
Gary Rivera,6612

Access Delay

To hinder access to critical resources through the use of physical systems increasing an adversary's task time.



There are many possible detection points, each lending a probability of detection; and many delay elements, each intending to add delay factors. Figure 1 shows the general model of an attack. An attack begins at some unknown time prior to the first detection; this can be hours or even days prior depending on when the adversaries begin their attack and the type of attack they are using. As soon as the attack is detected, response forces are notified and it is up to the physical security system to ensure that the response force has enough time to intercept the attackers before they reach their target.

The Methods of Access Delay

The traditional method for characterizing access delay has been a simple model focused on accumulating times required to complete each task with little regard to uncertainty and complexity. The delay associated with any given barrier or path is further discounted to worst-case (and often unrealistic) times based on a high-level adversary, resulting in a highly conservative, and therefore costly, calculation of total delay. To solve this problem, a new methodology using advanced Bayesian statistics has been developed. This allows the analyst to consider small sample sizes, expert judgment, human factors, and threat uncertainty in their total delay times.

Access Delay Visualization Tool

Bryan Watson
New Mexico Tech
PhD in CS, May 2017

Clayton Smith
Missouri University of S&T
MS in Comp E, Dec 2014

Joshua Herman
Missouri University of S&T
BS in CS/CE, May 2016

iSAFE
Interns for Security, Arms control and Force protection Engineering

Manager:
Shawn Taylor
6612/6613

Project Mentor:
Gary Rivera,6612

New tools are needed so engineers can quickly and easily use new algorithms without a thorough understanding of the Bayesian theory behind them. The Research to Visualization Tool, or R2VTool, was developed for this purpose.

Analysts use access delay methodology to determine a system's effectiveness by looking at the probability of detection, task delay times, response force time, and response force capability. Figure 2 shows an example of this procedure. In the figure, an adversary's path to an objective is broken down into a series of tasks. Each of these tasks has a set of requirements that must be met in order to proceed, e.g. the time it takes to breach a door. Analysts will perform tests on each of the tasks, collecting data on how long each task takes given certain toolsets. This dataset is then used to compute the statistics for the event and generate a distribution of task times. Table 1 contains the task data associated with Figure 2.

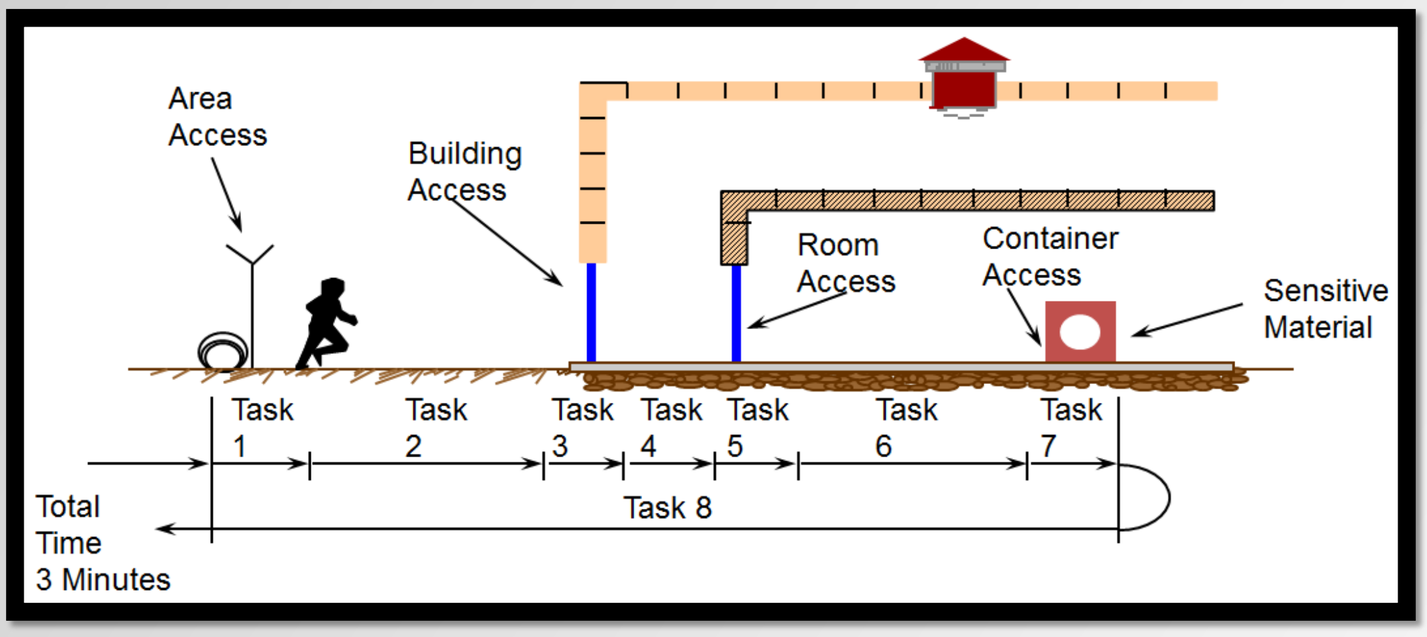


Figure 2: Example of Forcible Entry

Time Estimate			
Task	Mean Time (seconds)	Cumulative Time (seconds)	Task Description
1	12	12	Climb over fence
2	12	24	Run 76 m
3	48	72	Force door
4	24	96	Walk 45 m
5	12	108	Cut lock
6	06	114	Walk to container
7	12	126	Open container and gather material
8	54	180	Escape
	180		Total (approx. 3 minutes)

Table 1: Example data for Figure 2

In total, there are eight tasks. Their associated mean times and the cumulative times are given. At face value this type of data can be overly conservative and not representative of all attackers. Attackers can come with varying degrees of skill levels and equipment. The use of Bayesian statistics hopes to correct this issue by supplying the analyst with more information for which to make informed decisions.

R2VTool, (Figure 3), allows for the creation of new tasks on the fly. Using a Markov Chain Monte Carlo Simulation, MCMC, a Bayesian distribution is created for the task data. Three graphs can be produced for this data: the PDF, CDF, and Histogram. The 10th, 50th, and 90th quartiles, as well as the mean and standard deviation, are given for the MCMC task data. This data can then be saved to a CSV file.

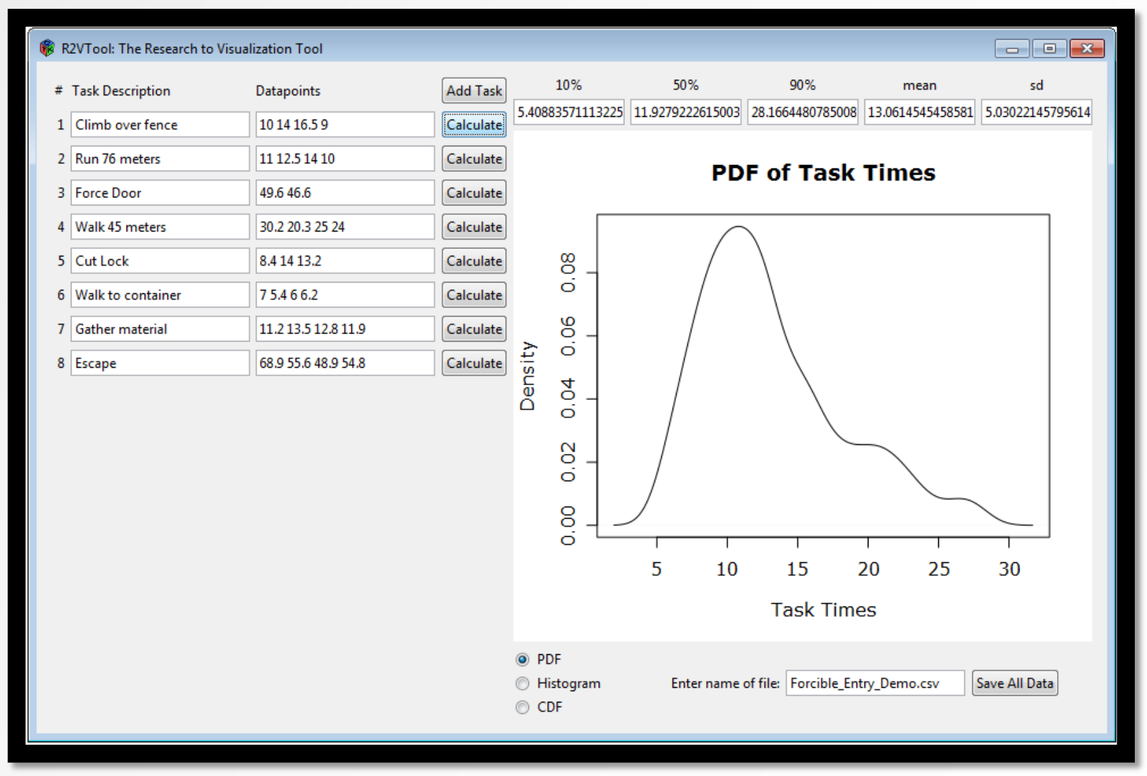


Figure 3: Screenshot of the new software

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND No. 2014-XXXXP