Terrain Based Path Prediction

MAJ Gregory Griffin

June 14, 2005

Outline

- Introduction
- Motivation
- Approach
- Validation
- Contributions
- Questions

Introduction

- The Path Prediction Tool (PPT) was designed to aid deployed military units' responding to a mortar attack and Homeland Security officials responding to a shoulder-fired missile on a commercial airliner.
- Uses the products of the Intelligence Preparation of the Battlefield (IPB) process to build a weighted arc-node network, then finds the *k-best* paths through it.
- Displays those paths on a map.

Motivation (1 of 2)

- Two current threats to Americans have motivated this research.
- The threat of mortar attacks against Allied forces in Iraq and Afghanistan.
- The threat of a surface-to-air missile fired at commercial aircraft landing and taking off from airports
- Both attacks have at least two things in common.
  - A quickly identifiable firing point.
  - No other reports on the attacker after the initial firing point location.

Motivation (2 of 2)

- Prevention of either of these types of attacks would be the best solution, however that is extremely difficult.
- Finding a better response is the next best solution.
- The enemy tactics and the characteristics and trafficability of the terrain can all be quantified to reflect how the enemy plans their paths of escape.
- Assemble all the information together and generate a path planning tool to help Allied forces in Iraq and Homeland Security agencies domestically to predict what paths the attacker will take back to his hideout after the attack.

Research Goal

- Develop a tool that assembles and quantifies information on enemy tactics and the terrain and generates the likely paths the attackers would use to escape from the firing point to their hideout. This tool will also display the paths on a map and maintain a current estimated location along those paths as a function of time.

Approach (1 of 6) -

- Convert the terrain and points of influence into a weighted node-arc network.
- Optimize the network to find the shortest path through it.
- Systematically alter the network to generate the *k-best* paths.
- Determine the probability that a particular path will be chosen.

Approach (2 of 6) –

- The PPT uses quantification of the geography and tactics of the enemy.
- The quantification places the data into three matrices for terrain, one matrix for points of influence, and the firing point.
- The three terrain matrices quantify the roads, intersections, and road conditions.
- The points of influence consist of the node that it is nearest to and the magnitude of the charge which reflects the amount of influence it is expected to have.
- The firing point is input as it is available.

Approach (3 of 6) –

- For a shortest path algorithm to work it needs the network to have weights on the arcs and nodes.
- The tool uses three factors to weight the arcs and nodes in the network.
  - Threat Score – Decayed Artificial Electric Field
  - Trafficability or Terrain Effects - NRMM
  - Road Distance – Dykstra's Algorithm

Approach (4 of 6) –

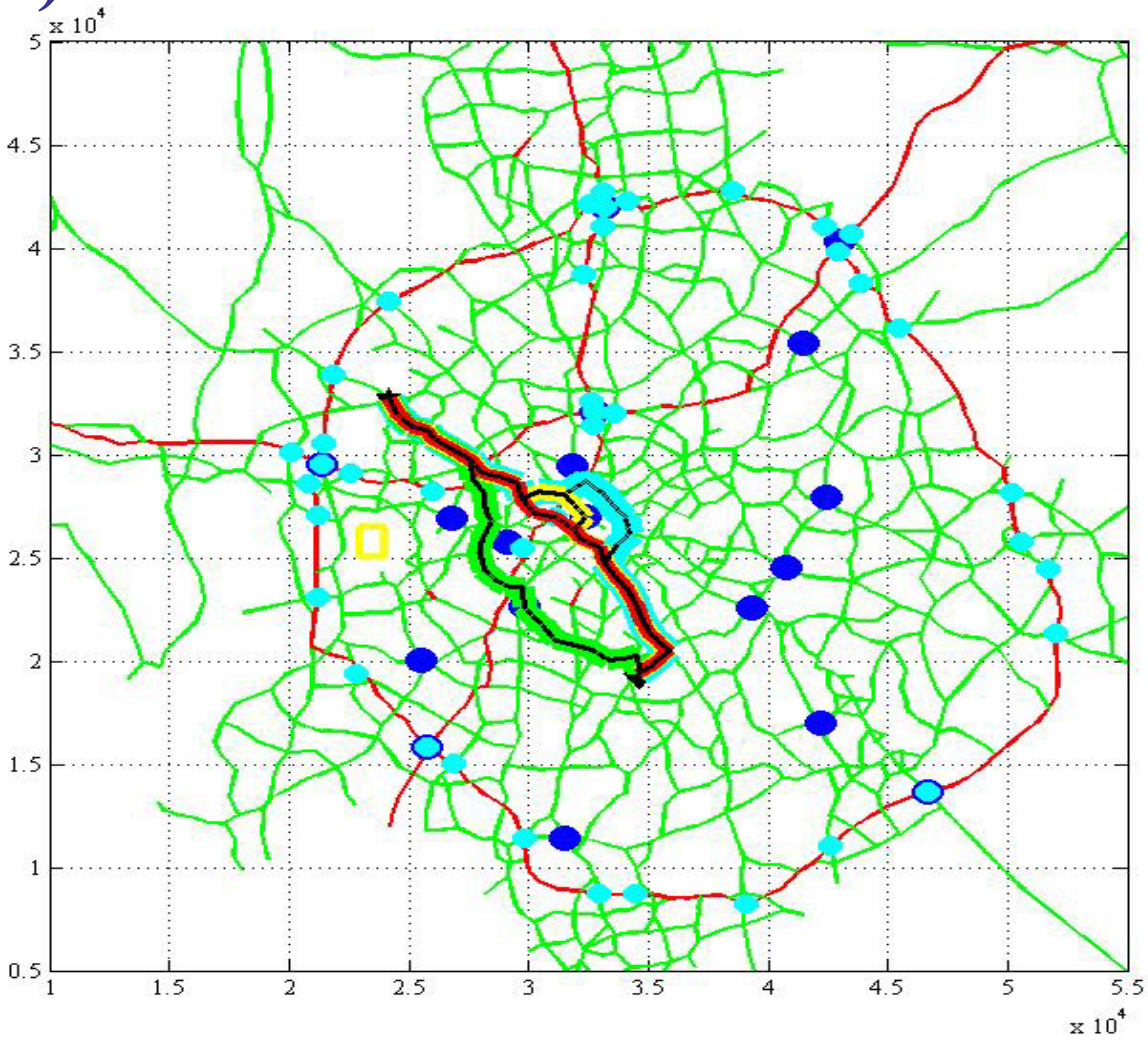
- All available data prior to an attack is collected.
- The tool pre-computes the threat surface and awaits the attack to get the firing point.
- Longest portions to calculate are the transforming of the map into a binary matrix that the obstruction value calculation can use and the threat score as it evaluates all the obstruction values.

Approach (5 of 6) –

- Once the firing point is determined an informed search algorithm (A*) is used to determine the shortest path.
- In order to get the *k-best* paths, we remove nodes from the path systematically based on their threat score.
- Determine the probability of the path being used through discrete choice.

Approach (6 of 6) -

- The result displayed to the user as a map with the network, influential points and potential goal locations on it.
- Additionally the *k-best* paths are depicted in different colors depending in the probability that the enemy would use it.



Validation (1 of 12) –

How to validate without ground truth

- In order to validate, need real data or simulated data.
- Real data is classified, simulation would be rather circular.
- Developed a series of experiments set in two different scenarios and got an expert in the area to predict the paths of the insurgents or terrorists based on their personal, professional opinion.
- One scenario located at a domestic airport and the other in a town in the Southwest Asia.
- The experiments had the subject assume the role of the enemy. The subject was given the map with influential points on it, the firing point and goal locations. They were asked plot paths for the enemy to escape.

Validation (2 of 12) –

Design of the experiment

- Each scenario had three experiments in it.
  1. Plot the single shortest, road distance path from the firing point to the goal location. Ignore all influential points in the terrain.
  2. Plot the four best paths to one goal location, taking into accounts all the influential points.
  3. Plot the four best paths to any of three goal locations, taking into account all the influential points.
- Not all the subjects were experts in the areas of interest. There was a second non-expert group that provided a lower bound on the performance, whereas the expert group provided an upper bound on the expected performance.

Validation (3 of 12) –
Metrics

- The metrics can be grouped to reflect which factors of the enemy's decision making process they measure.
- Threat: Overall path threat score, and maximum, minimum and average threat values for the nodes of the path.
- Shortest amount of time: Path time, Number of path segments, path length.
- Metrics for determining the similarity with the expert:
  - Predicted Path Deviance (PPD)
  - Number and percent of nodes that were the same

Validation (4 of 12) -

Predicted Path Deviance

- PPD is a measure of the area between the two paths and divided by the expert path length.
- This reflects the fact that a parallel path that is near the optimal will score better than a shorter or longer path that does not closely follow the optimal path.

$$\frac{\sum Area_{sp}}{L_p}$$

Validation (5 of 12) –

Charlotte Airport results

- For this scenario, the expert was a subject who had conducted a study of the Charlotte airport for vulnerabilities to surface-to-air missile attack.
- In Experiment 1, the subjects, in general, did not find the optimal path. All of the metrics showed that humans, even without competing constraints, have trouble finding optimal solutions.
- In Experiment 2, the path prediction tool was tuned to the characteristics of the expert/enemy. By adjusting the weights on the three components of the arc and node values, the tool found results that reflected the decisions predicted by the expert.
- The tuned tool was able to consistently outperform the non-expert subjects.

Validation (6 of 12) –
Charlotte Airport results

- A sample of the results from Experiment 2.

	Expert	Computer	*Diff*	Subjects	*Diff*
Number of Segments	28	24	4	32	4
% Same Segments			39.29%		57.22%
Length (m)	20464	19539	925	24016	3552
Max. Threat	0.5428	0.5480	0.0051	0.5588	0.0739
Min Threat	0.1608	0.1164	0.0444	0.1608	0.0000
Average Threat	0.3295	0.3345	0.0050	0.3414	0.0241
Travel Time (sec)	12324	10157	2167	14584	2260
Threat Score	4.2038	3.4431	0.7607	5.1328	0.9821
PPD			89.338171		1319.9039

Validation (7 of 12) –

Charlotte Airport results

- In Experiment 3, the same weights on the factors in the optimization were maintained to plan the paths.
- Sample results from Experiment 3.

	Expert	Computer	*Diff*	Subjects	*Diff*
Number of Segments	44	44	0	50	6
% Same Segments			52.27%		39.74%
Length (m)	35350	37149	1799	38983	3848
Max. Threat	0.6376	0.6716	0.0339	0.6460	0.0084
Min Threat	0.2278	0.2278	0.0000	0.2222	0.0056
Average Threat	0.3595	0.3634	0.0039	0.3687	0.0156
Travel Time (sec)	22603	22603	0	24706	2103
Threat Score	9.4312	9.6221	0.1909	11.9361	2.5543
PPD			53.832987		1118.1181

Validation (8 of 12) –

Southwest Asia results

- For this scenario, the experts consisted of four Operation Iraqi Freedom Veterans who had experience with insurgent mortar attacks.
- In Experiment 1, none of the subjects faired any better than the subjects in the Charlotte scenario. This time only one subject found the optimized shortest road distance.
- In Experiment 2, the same factor weights were used for the tool's optimization. The tool is designed to be adjusted to fit the tactics of the enemy in each area of operations. The tool was not recalibrated because of the sparseness of the data.
- Regardless, the tool performed well against the non-expert subjects.

Validation (9 of 12) –

Southwest Asia results

- The experts' responses are averaged for the path metrics. When assessed against the non-experts, each path is compared one-to-one and then averaged.
- In Experiment 2, the tool outperformed the non-expert subjects three out of four times in all areas.

	Expert	Computer	*Diff*	Subjects	*Diff*
Number of Segments	92.25	77	15	88	5
% Same Segments			50.91%		44.66%
Length (m)	32699	29892	2807	30216	2519
Max. Threat	0.8392	0.8236	0.0156	0.8313	0.0108
Min Threat	0.0000	0.0000	0.0000	0.0000	0.0000
Average Threat	0.5732	0.5604	0.0127	0.5812	0.0111
Travel Time (sec)	13492	9455	4037	11719	1987
Threat Score	1.2193	0.9809	0.2384	1.1416	0.0822
PPD			45308.311		56898.5954

Validation (10 of 12) –

Southwest Asia results

- In Experiment 3, the tool outperformed the non-expert subjects three out of four times in all areas.

	Expert	Computer	*Diff*	Subjects	*Diff*
Number of Segments	62.5	45	18	60	13
% Same Segments			5.71%		25.29%
Length (m)	25357	22292	3065	23081	6157
Max. Threat	1	0.8816	0	0.8280	0.0994
Min Threat	0	0.5434	0	0.0310	0.2536
Average Threat	1	0.6928	0	0.6657	0.0264
Travel Time (sec)	6787	0	6787	5673	4316
Threat Score	0	0.1061	0	0.4489	0.2856
PPD			98870.173		99097.2254

Validation (11 of 12) –
Significance

- T-tests were conducted on the results from both scenarios.
- Tested two hypotheses:
  - Were the tool results actually different from the non-expert subjects.
  - Were the tool results the same as the expert subjects.
- Used four metrics (PPD, Average Threat, Threat Score and Travel Time) to determine the similarity of the PPT results and the non-experts results.
- Used three metrics (Average Threat, Threat Score and Travel Time) to determine the similarity of the PPT results and the experts results.

Validation (12 of 12) –
Significance

- Hypothesis 1, are the PPT results different from the non-expert group.
  - The majority of the tests for the metrics concluded that they were different at a significance level of 0.1.
  - The results were not unanimous across all the metrics.
- Hypothesis 2, are the PPT results the same as the expert group.
  - The majority of the tests for the metrics concluded that they were the same at a significance level of 0.1.
  - The results were not unanimous across all the metrics.
- A good result for such a small data set. Expect results will get better with more testing.

Contributions

- Developed a new approach to path planning with an expanded definition of terrain.
- Demonstrated application to problems of security and military operations.

Future Work

- Future work can extend this in two ways:
  - Calculate the threat for each arc at the point in the arc where the field is the strongest.
  - Move this off of the network and into a continuous realm. An interim is to have different networks for different modes of travel to include dismounted.

Conclusion

- Questions
  &
  Comments

Backup Slides

Related Research (1 of 8) –
Military mission planning and the terrain

- Mission Planning in the Military
  - Always account for the terrain and the enemy
- Assessment of the terrain: OAKOC
  - Obstacles
  - Avenues of Approach
  - Key Terrain
  - Observation and Fields of Fire
  - Cover and Concealment
- Accounting for these factors, military forces incorporate the effects of terrain on the planning process.

Related Research (2 of 8) –
Military mission planning and the enemy

- Intelligence Preparation of the Battlefield (IPB)
- The mission planner looks at the enemy's past actions and tactics to anticipate what they are going to in the upcoming mission.
- The intelligence officer produces a template, adjusted for terrain, that quantifies his best guess as to the location or actions of the enemy on this particular mission.
- These guesses are grouped together into possible Coarse of Action (COAs) for the enemy.
- The terrain assessment through OAKOC and the enemy assessment through IPB can be applied to the current threats that we have to our forces.
- This research proposes to use the products of these existing processes to automate the COA generation and weighting of the likely paths the insurgent or terrorist would use to escape after an attack.

Related Research (3 of 8) –
The planning priorities of the enemy

- In order to develop an accurate tool, something needs to be assumed about the insurgent and terrorists minds and what they consider important in the path planning.
- Looking at current behavior in the insurgent a couple of observations can be made.
  - The insurgent is smart and adaptive
  - He will avoid allied forces
  - He will take the path that takes the least amount of time to get from the firing point to his hideout.
  - He will always take paths that allow him to maintain his flexibility.

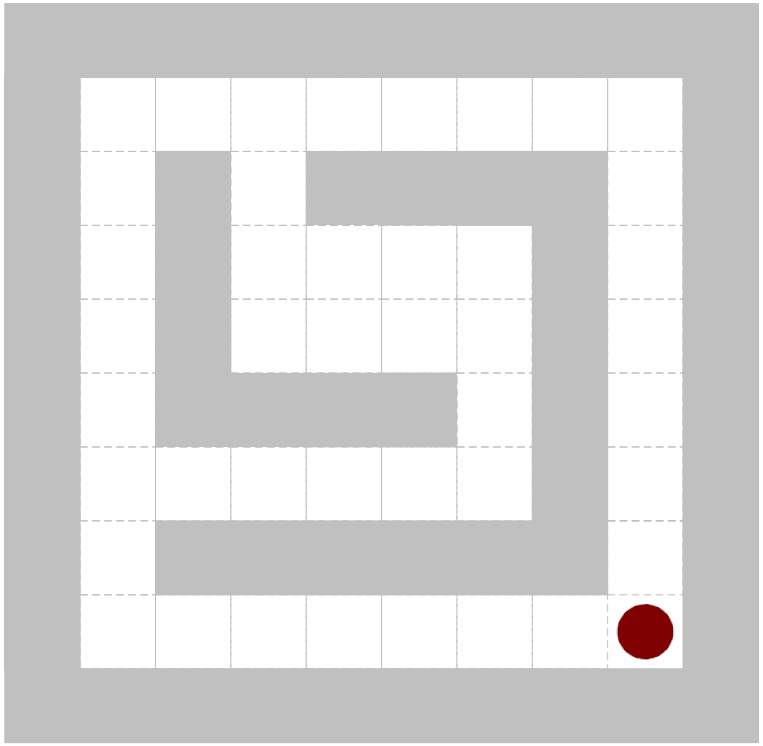
Related Research (4 of 8) –
Path planning

- Automated path planning explored by many fields and extensively by robotics and computer game programmers.
- Most use a potential fields method.
- Two main ways to generate the potential fields:
  - Wave Front Propagation
  - Artificial Electric Field

Related Research (5 of 8) –

Wave Front Propagation

- Starts from one point and the expands equally outward, counting the units of distance as it goes.
- Each branch of trafficable terrain generates its own data structure and all the paths to that point needs to be stored.
- Requires extensive amounts of memory and computer time in order to compute.



Related Research (6 of 8) –

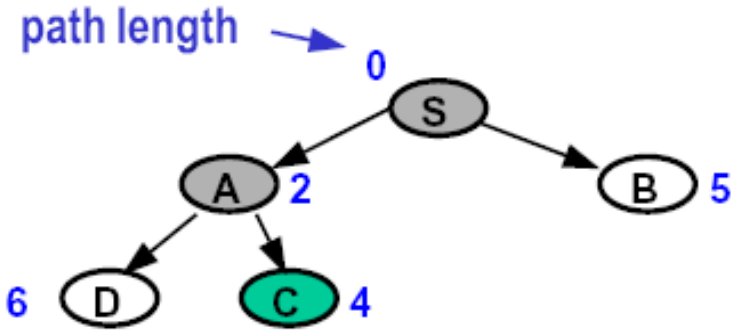
Artificial Electric Fields

- Based on Coulomb's Law
- Force is a function of charges and squared distance between them
- Radiates equally in all directions regardless of the underlying surface

$$F = k\frac{q_1 q_2}{d_{12}^2}$$

Related Research (7 of 8) –
Network Optimization

- Many problems can be converted into network shortest path problems.
- Search methods can be broken into two groups: Uniformed and Informed.
- Uniformed uses only information from problem statement.
- Informed uses as much information as you can quantify for it. This additional information shows up as the heuristic value.



$$f(n) = g(n) + h(n)$$

h(n)

Related Research (8 of 8) –
Discrete Choice Models

- Evaluates the relative probabilities of choices from a set.
- Uses a utility score to compare the choices to one another.
- Logit choice's significant advantage over Probit is the closed form nature of the answer.

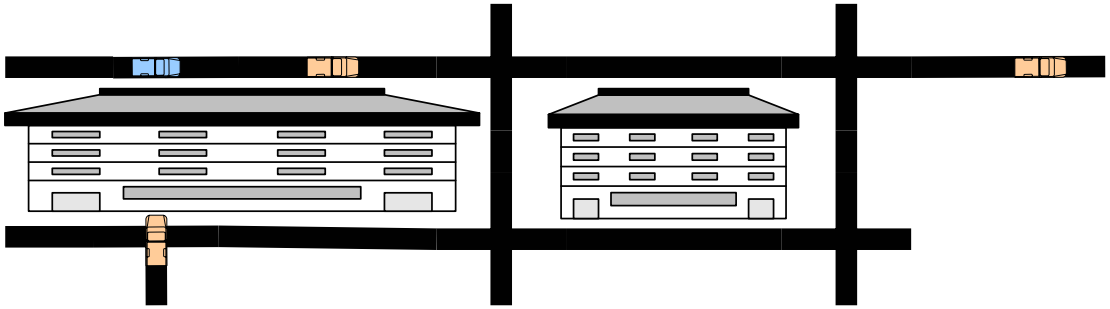
$$u_i = v_i + \varepsilon_i$$

$$p_i = \frac{\exp(v_i)}{\sum_{k=1}^{n} \exp(v_k)}$$

DC

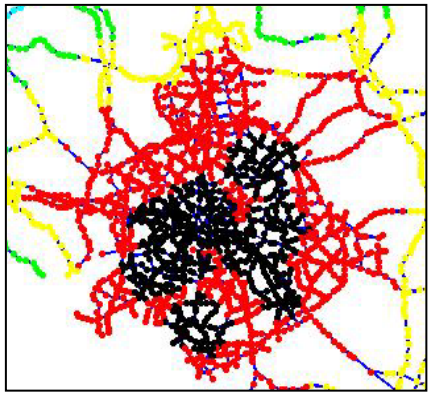
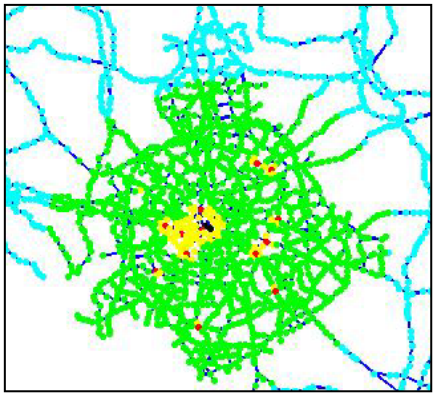
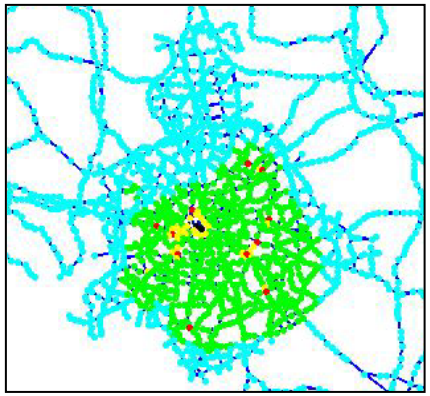
Proposed Approach (3 of 12) –
Choosing the Potential Field generation method

- The threat score uses the potential fields method to calculate the level of threat the insurgent or terrorist feels at each node as he is making his path decision.
- Which method to use? The two different methods yield two very different results.
- Wave Propagation strictly follows terrain.
- Artificial Electric Field completely ignores terrain.



Proposed Approach (4 of 12) –
Choosing the Potential Field generation method

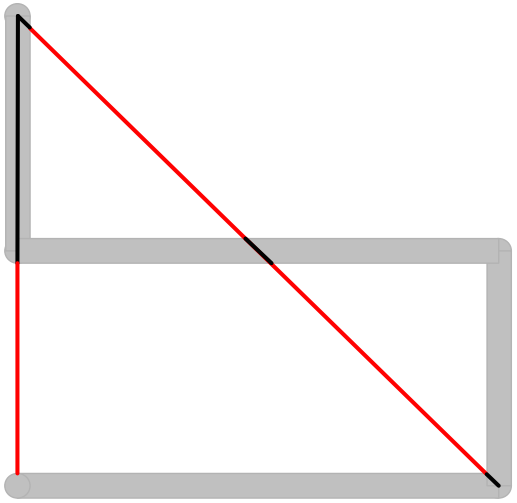
- Solution: Use a computationally cheap artificial electric field that has a decay term based on the amount of un-trafficable terrain between the source and the target.

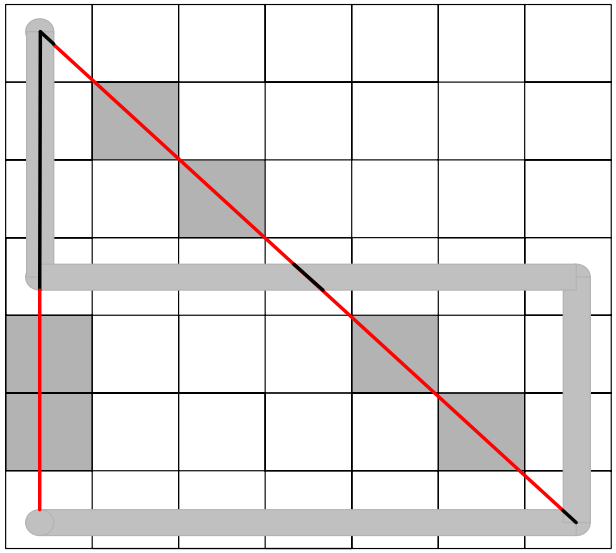




Graph

Proposed Approach (5 of 12) –
Choosing the obstacle value calculation method

- Calculation of the obstacle value was done via two different methods.
- Small network: straight line calculation of obstruction.
- Large network: area calculation of obstruction.





Graph

Proposed Approach (6 of 12) –
Calibration of the Threat Score

- There are three different factors that can be adjusted to calibrate the threat score to accurately model the effect that was sought.
  - Obstacle value
  - Distance scale
  - Zero-distance value
- When the three values were properly scaled (all in meters) or weighed, the nodes at the point of influence or its immediate unobstructed neighbors were separated from the rest of the nodes.

Proposed Approach (7 of 12) –
Trafficability calculation

- Trafficability of the terrain is quantified as a maximum speed that a class of vehicle can attain on an arc.
- These speeds were calculated from the NATO Reference Mobility Model which standardizes all NATO military ground simulations.
- The trafficability enters the optimization in two ways: determining which route is more trafficable (higher score is better) and then determining the amount of time it will take to traverse an arc.

Proposed Approach (8 of 12) –
Road Distance Calculation

- The heuristic that the informed search algorithm needs to optimize the shortest path is a shortest driving distance measure.
- Used Dykstra's algorithm with an added component for remembering its path.
- Guaranteed optimal which meets the admissible heuristic requirement of never overestimating the distance to go.

Admissible Heuristic

- The heuristic for an informed search is the measure from a node in the network to the goal.
- Can be anything (number of moves, Euclidean distance, etc.)
- For a heuristic to be admissible it cannot overestimate the measure to the goal.
- Prevents the heuristic from pulling the search in the wrong direction and guarantees optimality.

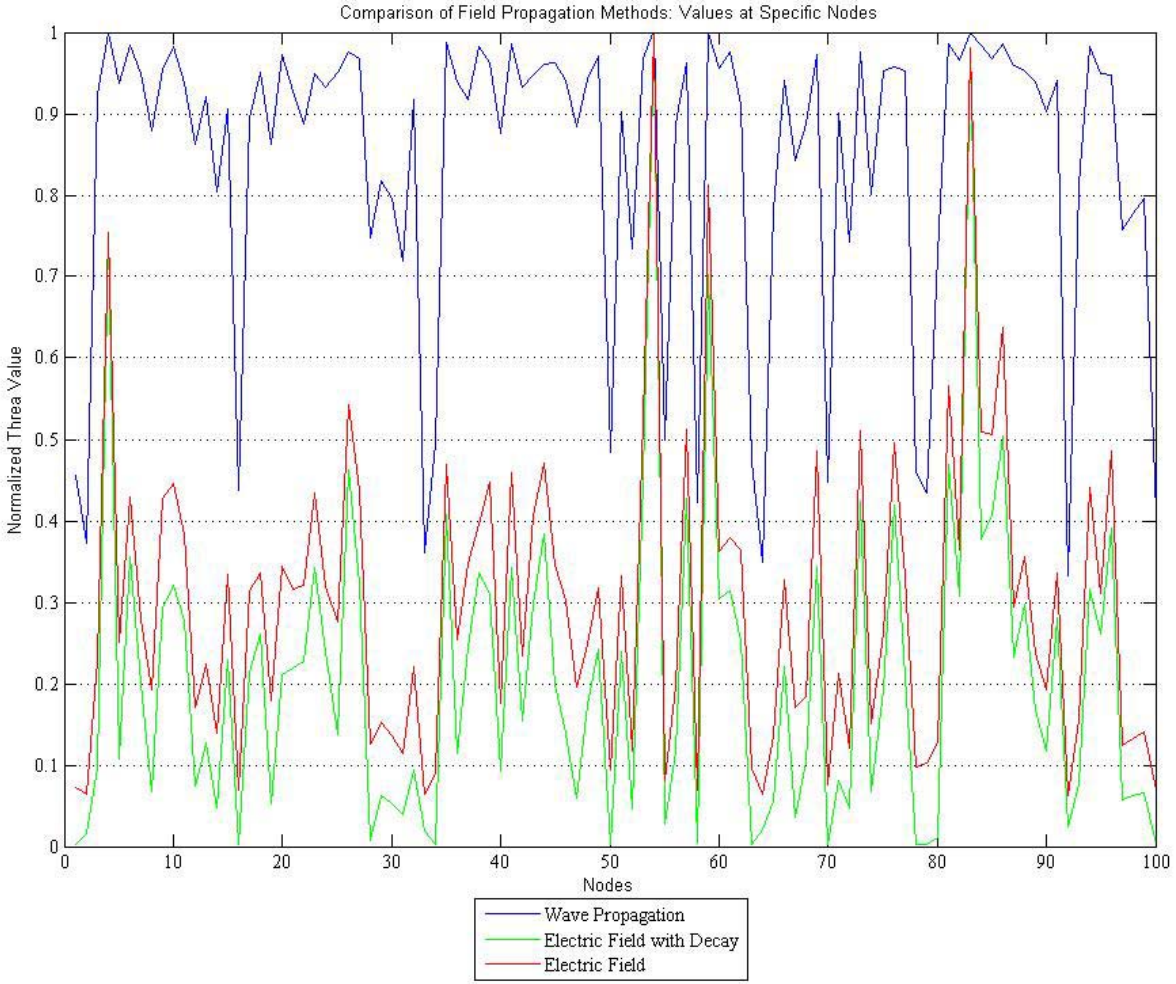
Discrete Choice

- Based on neoclassical economic theory that assumes the decision maker can conduct pair-wise comparisons.
- If that can be done then an ordered set may be formed.
- The Luce model builds off of this by assigning a probability that a choice is made instead of assigning one outright.
- This probability is calculated by dividing a unique valued function for the choice from the set by the sum of that function for all the choices from the set.
- Random utility theory helps determine how others value each choice relative each other by assigning a deterministic and stochastic component to each choice.

Discrete Choice

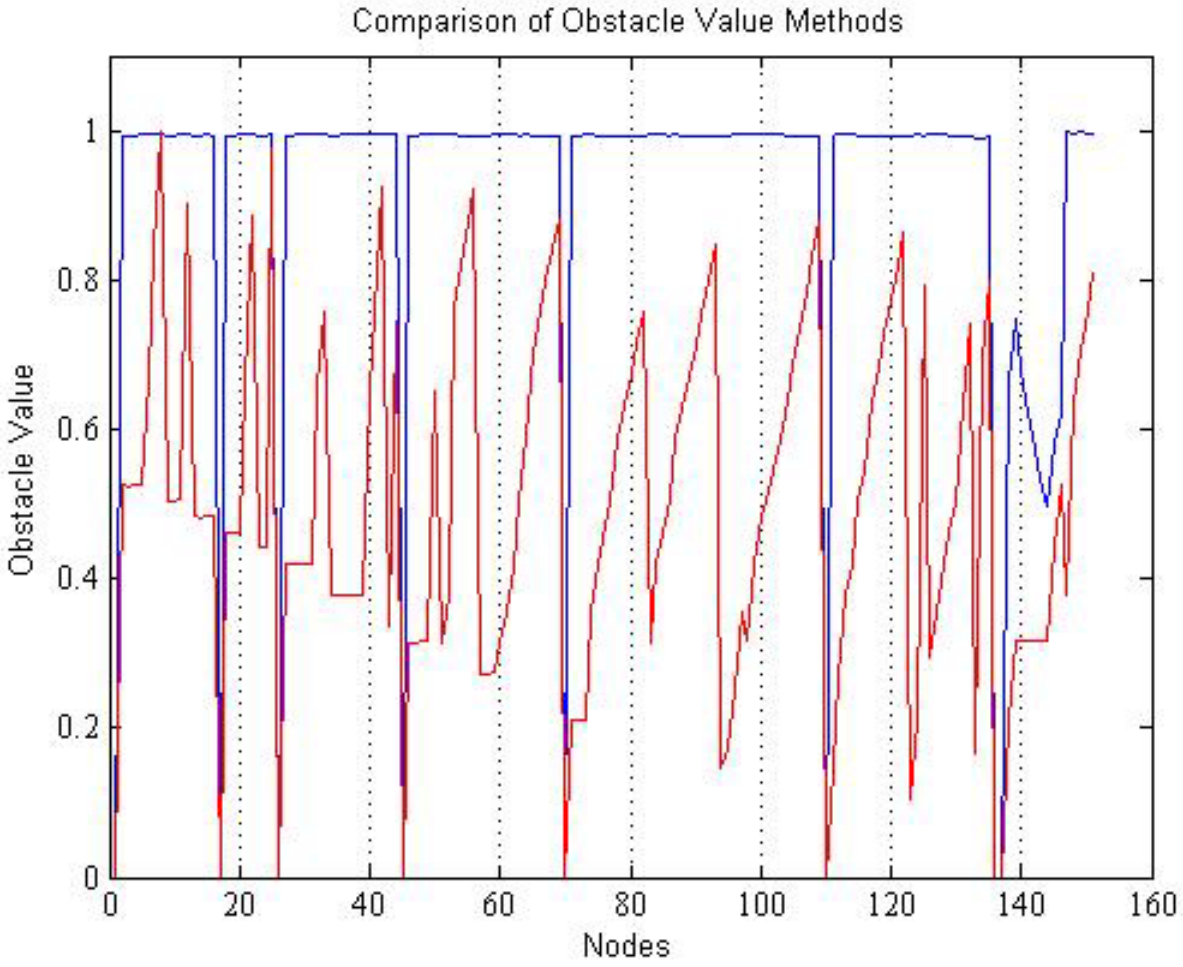
- The Probit model named that stochastic component as normally distributed error leading to a non-closed form solution to the problem.
- The Logit model changed that stochastic component to a Weibull distributed error. This leads to a closed form solution to find the probability. The unique valued function becomes the exponential of the utility and the equation takes the form shown on slide 13.

Differences in Threat Score Based on Method Choice



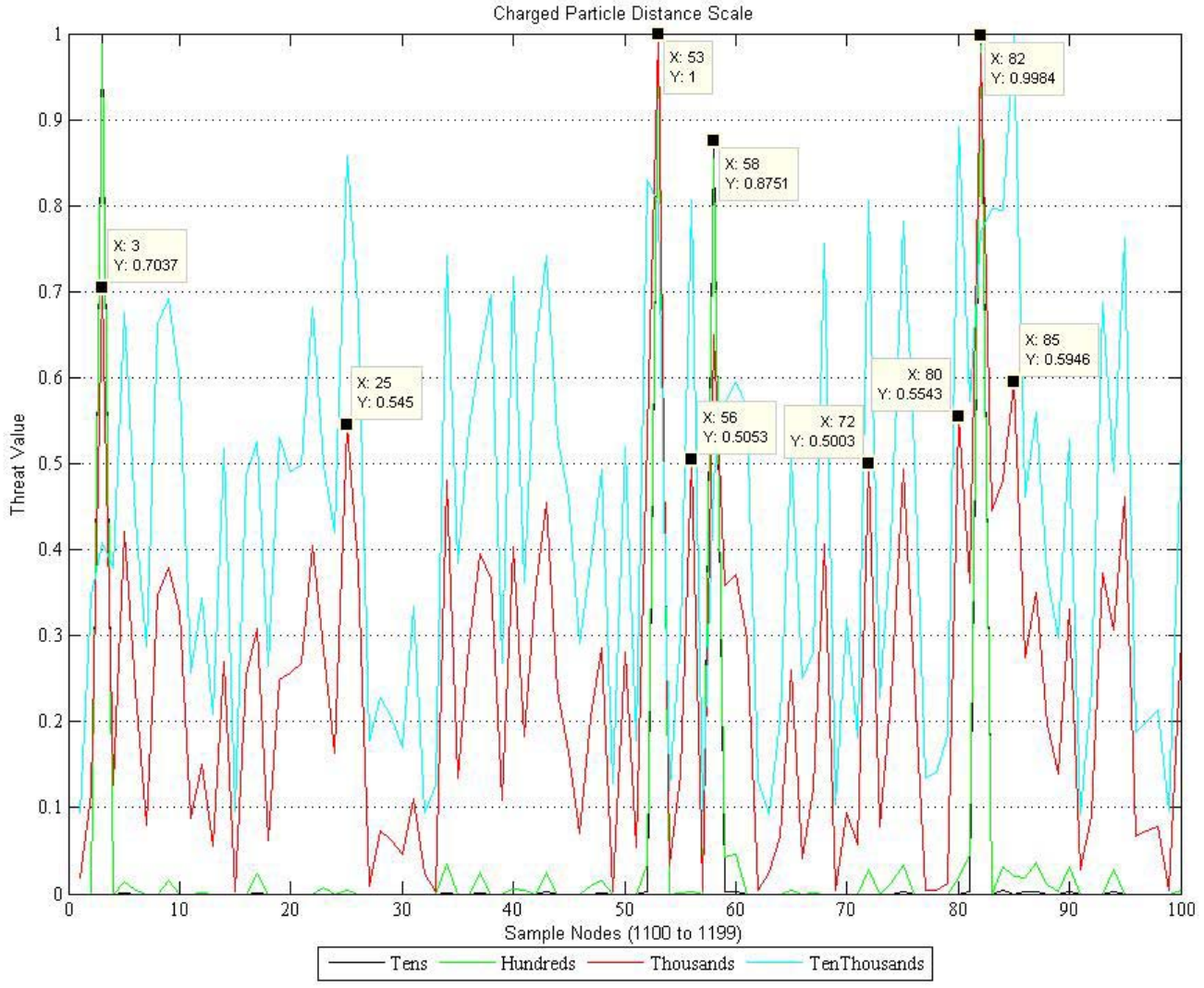
Back

Obstacle Score Method Comparison

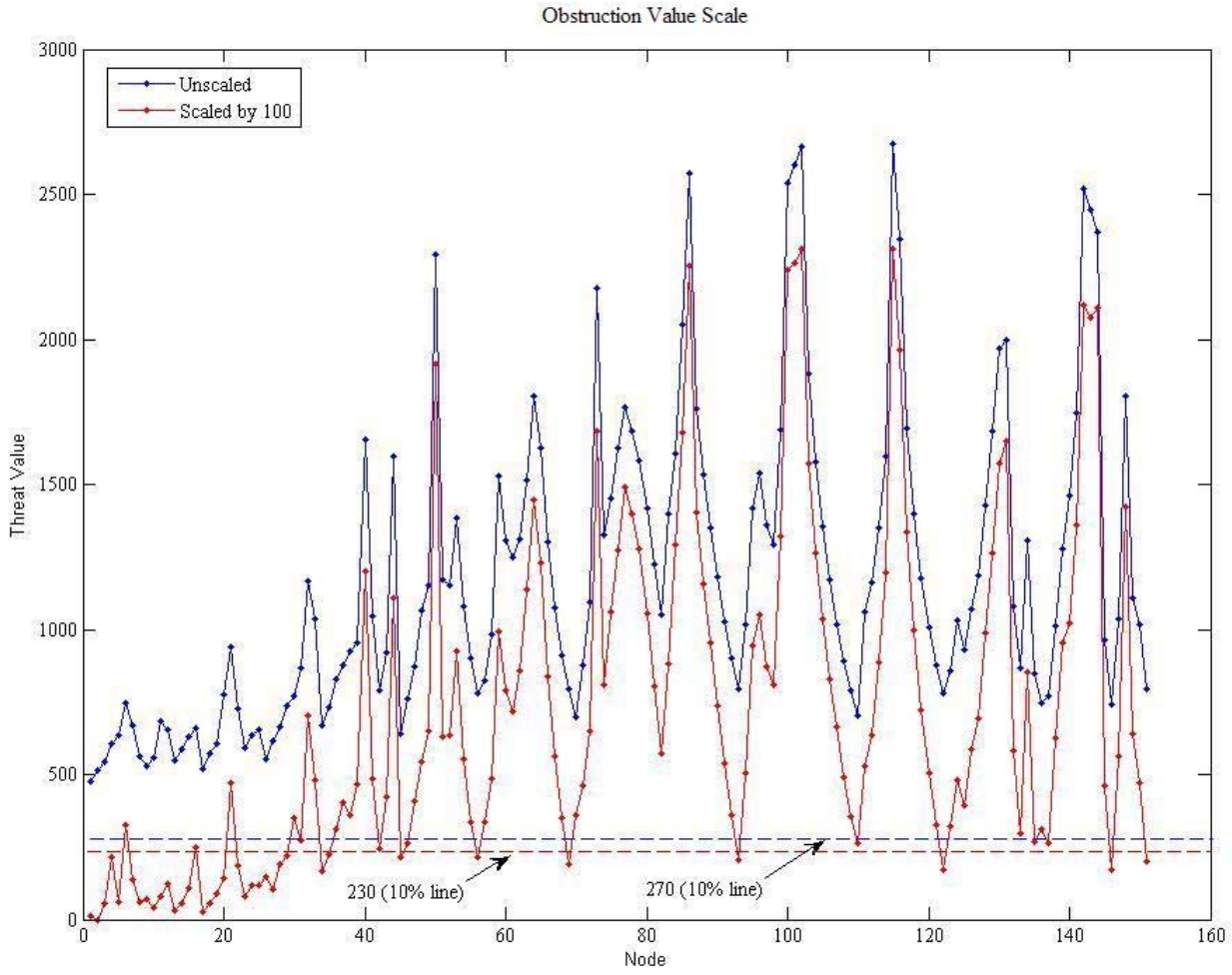


Back

Charged Particle Distance Scale



Obstruction Value Scale



Back

Proposed Approach (10 of 12) –
Optimization algorithm

- Once the firing point is determined an informed search algorithm is used to determine the shortest path.
- A*, originally developed by Hart, Nilsson, and Rapheal in 1967, is guaranteed optimally efficient for networks.
- In order to get the *k-best* paths, removed nodes from the path systematically based on their threat score.
- Creates a very good spread of routes from the source to the goal.

Proposed Approach (11 of 12) –

Discrete Choice

- To determine the probability that an insurgent or terrorist would use a particular path, Logit choice was used.
- Logit choice makes the calculations quick and accurate providing a good relative reference between the different paths that the insurgent or terrorist would use.