Strategic Planning and Tactical Situational Awareness Using MECH[1]

Jason Lin, Benke Qu, Xing Wang, and Jyh-Charn Liu

Texas A&M University, College Station, TX; {senyalin, qubenke, xingwang, liu}@cse.tamu.edu

Stephen George

U.S. Department of Defense, Washington D.C.; ticom.dev@gmail.com

In asymmetric conflict, insurgents seek to maximize their objectives by controlling as much of the conflict as possible. In the case of planned attacks, like improvised explosive devices (IED) or direct fire (DF), attackers carefully emplace the attack site to ensure availability of necessary support and overwatch locations. A primary consideration is exposure of attack elements to the target prior to initiation of the event. Thus, attackers will choose support and overwatch locations that simultaneously provide *visibility* to the target while being immediately adjacent to cover. The degree of visibility and cover required vary with the tactics and risk aversion of the attacker. This paper proposes a novel software system that serves both strategic and tactical needs of intelligence, surveillance and reconnaissance (ISR) in counter-insurgency operations. At heart of the system is the *Monitor, Emplacement, and Control in a Halo* model (MECH), which represents the attacker's decision space with respect to the emplacement of the attack and associated support elements. Beyond simple terrain analysis, MECH incorporates measurable aspects of human decisions into patterns learned from historical data and provides a common operational picture for both strategic and tactical users. This shared view allows users to focus and prioritize ISR, route clearance and analytic resources. From a regional view, route choice, tailored surveillance and force composition may all be influenced by the strategic view of a route. On a local level, tactical users are able to focus on immediate threats, cueing sensors and weapons towards upcoming threats.

Categories and Subject Descriptors: **3 [Data, Information and Knowledge]**; **4 [Experimentation, Metrics and Analysis]**; **12 [ISR for Decision Making]**

Additional Key Words and Phrases: Behavior modeling, Tactical and strategic analysis, Counter insurgency, Algorithms, Machine learning, ISR for decision making

1. INTRODUCTION

Asymmetric conflict (AC) [1-5] is the most prevalent type of warfare in the modern world. Often considered to be a struggle between stronger and weaker actors, where 'stronger' is defined in terms of killing power, the actual asymmetry may be more subtle. Asymmetry of information is a one example where the weaker actor can enjoy an advantage. In this case, the weaker actor is familiar with local geography and has the support of the local populace. This actor is able to use knowledge of the local terrain to maximum advantage, selecting attack sites that negate the stronger actor's strengths. At the same time, the local populace contributes by reporting on the activities and movements of the stronger actor. The weaker actor ends up with an ability to carefully select a favorable site and prepare an attack tailored to exploit the stronger actor's weaknesses. Although the 'weaker' actor is a less

[1] This work was supported in part by an ONR grant N00014-12-1-0531 and a National Defense Science and Engineering Graduate (NDSEG) fellowship. Any opinions, findings and conclusions or recommendations expressed in this material are the author(s) and do not necessarily reflect those of the sponsors. The correspondence author is J.C. Liu.

capable fighting force on paper, it is able to use asymmetry of information to dominate some aspects of the conflict.

While surveillance by the local population is probably impossible to prevent, asymmetry of information with regards to the local terrain can be mitigated in two ways. The classic method involves capturing terrain, siting a base or outpost in the area, and conducting familiarization patrols throughout. This approach is costly, both in terms of lives and time. A second, less costly approach analyzes conflict events to understand enemy tactics, such as the work in [19] in which environmental and cultural cues are summarized based on experts' experience. Even relatively simplistic analysis can provide useful insights into potential attacker tactics and may reduce information asymmetry.

The starting point for conflict event analysis is a set of assumptions about the underlying capabilities and motivations of the attacker. The assumptions constrain and inform the feature set and the terrain that needs to be analyzed. For this research, we constrain the analysis to historical events that occur along roadways and examine improvised explosive device (IED) and direct fire (DF) attacks. We assume

- The attack is planned. Attackers are able to choose the location of the event and optimize the placement of their forces and supporting elements.
- The attack is controlled. In the case of an IED, the explosion is command-initiated by some human. In the case of DF, firing is initiated by some human either on command or in response to some target activity. In many cases, this assumption of control requires that at least one attacker must have visibility of the target in order to time attack initiation.
- Attackers are risk-averse. This means that attackers take steps to ensure that the attack proceeds as planned and steps are taken to avoid compromise prior to initiation. Note that risk-aversion is not correlated with fear or cowardice. It is a disciplined effort to maximize attack outcomes by denying the target information about attack elements until initiation.

Given these assumptions, we proposed a risk-averse behavior model called MECH (Monitor, Emplacement, and Control in a Halo) [6], to capture the decision making process of the attacker as an attack site is selected and supporting actors are positioned. MECH supports analysis of specific attack sites, the local environment, and surrounding regions. As shown here, MECH provides machine learning-based statistical classification of locations useful in an attack, either as

- Emplacement (E), e.g. the location of the IED or the kill zone of an ambush;
- Control (C), a location from which the attack can be initiated; or
- Monitor (M), locations that are useful for early warning and overwatch tasks.

Control and Monitor locations are chosen with respect to some particular Emplacement and tailored to support the specific attack under consideration. They are chosen from within a Halo, a constrained area surrounding a potential Emplacement.

MECH arose from two principal sources: firsthand author experiences in tactical environments and existing military training and practice. The tactical experience provided insights into attacker and defender behavior while existing training was mined for common attack construction. The model itself emerged from discussions on the essential tension between an attacker's need for cover and desire to view the target. This tension led attackers to select control and overwatch locations that satisfied both requirements.

Analytics studies for strategic planning [6,7] usually consider larger areas, typically regional areas with extents ranging from tens to hundreds of kilometers. On the other hand, tactical analysis [8-12,16] tends to focus on short range, detailed studies of a particular location and its immediate environment. This analysis often focuses on terrain structure, avenues of approach and availability of cover and concealment near the objective. To assist both strategic and tactical stakeholders in the formation of a common operational picture (COP), this paper proposes a computing model that interactively supports analysis of potential AC locations from both strategic and tactical perspectives. Three communities are served: tactical users who care about their immediate vicinity, strategic users focused on resource allocation and collection management, and MECH system experts who build and refine tailored models for other users. For all users, MECH provides algorithmic support to user decisions by recognizing and highlighting patterns [14] associated with attacker tactics. This highlight assists users to focus more directly on the highest or most immediate threats.

The map-based representation system, together with the MECH model, supports threat ranking of locations at larger scales. As needed, users can focus on a particular location of tactical concern to perform short range threat analysis while keeping the regional perspective in mind. This interactive analysis technique is based on the functional requirements of AC, in the format of strategic vs. tactical queries to the MECH analytics system. As a strategic example, ISR collection managers can implement strategies to allocate ISR assets based on operational needs in the region or focus analysis on the highest threat locations. Tactical users, on the other hand, can use MECH to direct and focus tactical sensors and their attention towards likely threat locations.
To support integrated strategic and tactical analytics, we note that Monitor and Control (M/C) sites are located around an Emplacement. Hidden M/C locations are exclusively used by the attackers while the Emplacement is visited by the target. Some typical questions that MECH might answer include

> "*Which locations along a route provide the most extensive view of the route?*" (Supports focused analysis of ISR data.)
> "*What locations along a route are likely to be used for the execution of an IED or DF attack?* (Identifies higher threat route segments.)
> *"For a specific potential Emplacement, where are likely Monitor and Control locations?* (The presence of surveillance or overwatch is a strong indicator of an attack.)

In order to answer these types of tactical and strategic questions, a first step is the creation of behavioral and geographical models that capture key static and dynamic factors that potentially have tangible effects on the decision making process. This is MECH [6]. Next, we propose a computing model to support a broad range of strategic and tactical queries similar to the aforementioned questions. It is important to note that many of these queries are open-ended and provide interpretable results that change dramatically with the region of interest and features analyzed. As such, the system architecture presented in this paper represents a pragmatic approach, based on the following simple, interactive reasoning process:

"Given one or more conditions, rank the utility of locations within the region of interest for some [tactical/strategic] function?"

For each query generated by a user, the backend processing engine produces a list of high score locations to be processed by the client computing device. The user can then adjust the cutoff threshold to narrow down the region of concerns for decision making or further refinement of analysis. The user can also drill down to understand how the model produced a particular score contributing to overall understanding and allowing the user to make a trust decision.

2. THE MECH SYSTEM

MECH is a general behavior model which can be tailored to meet different objectives by simple one-time adjustment of parameters as well as interactively via a query-response process with the user. An assessment area is divided into a route R and its surrounding proximity P. Figure 1 gives an overview for the MECH behavior model.

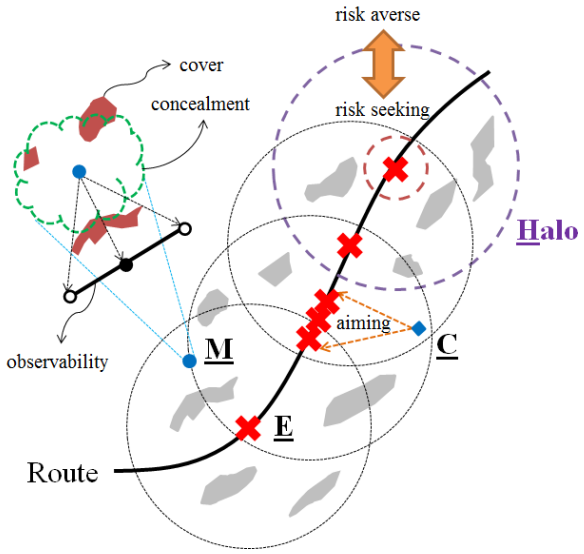


Figure 1: An Overview of MECH Behavior Model

To support the above operational concepts including interactive analysis, we propose a distributed system architecture consisting of mobile frontend devices (MECH-APP), a backend classifier training system (MECH-CTS), and real-time backend processing engines (MECH-WPS) as shown in Figure 2. This architecture allows both tactical and strategic users to use mobile devices to access a high power processing engine in order to perform computing-intensive analytics. MECH-APP supports four major assessments:

(1) **Basic Measurements**: This includes several measurements derived from line-of-sight (LOS) between P and R locations within an assessment area.
(2) **Behavioral Modeling**: Probabilistic reasoning of locations for M, E, and C activities. Tactical parameters can be defined based on a risk-averse/risk-seeking Halo model.
(3) **Machine Learning (ML) Classifier**: Classification of R points by using one of the trained ML classifiers stored on the MECH-WPS.
(4) **Past Events**: Past events in the displayed map area of the APP.

MECH-APP uses the Google Map service for low level map operations and MECH-WPS for the tactical analytics, respectively. MECH-WPS provides a web portal for end users to access services provided by the backend processing engines. MECH-CTS performs machine learning tasks like classifier training and pattern detection.

For the typical questions listed in the Introduction, their computing needs are analyzed as follows:

1. *Which locations along a route provide the most extensive view of the route?*"

The key phrase "most extensive view" implies that the most useful locations should have the best observability over a route, as well as good protection from being seen by the victim. As a result, behavior models like "observability + concealment" assessment, or "observability × concealment" might best answer the query. Obviously, the underlying MECH model must have computing models that characterize both observability as well as concealment in order to support this query.

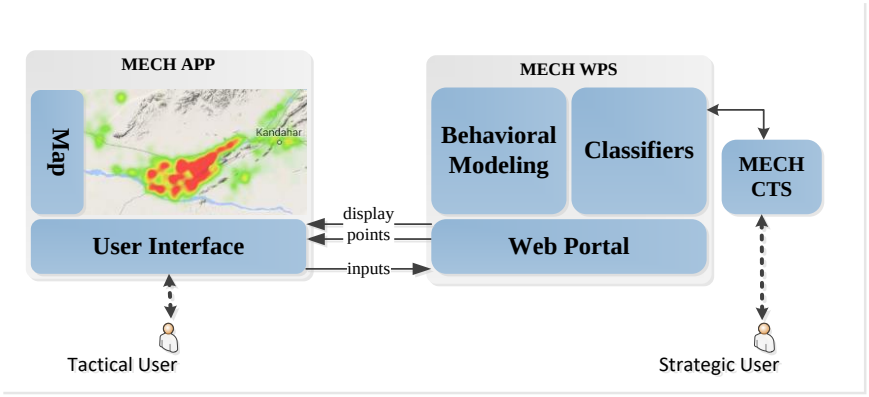


Figure 2: Organization of Primary Functional Component for MECH

2. *What locations along a route are likely to be used for the execution of an IED or DF attack?*

For insurgents that execute a deliberate plan, a planned attack typically requires observation of the target and the ability to act (fire a weapon or trigger an IED, for example) from concealed positions. To serve this purpose, the user can first use the "basic measurements" assessment to produce a P heat-map and then invoke the "behavioral modeling" based on P to assess potential threat locations along the given route R. Alternatively, the user can start with a more detailed basic measurements analysis focused on exposure or curvature analysis along the route to identify the higher threat positions on R. These R points can then be used to identify best P points by using the behavioral Halo model based on R.

3. *For a specific potential Emplacement, where are likely Monitor and Control locations?*

Different assessments can be done in a hierarchical fashion. Thus, a single potential Emplacement location along R can be assessed using basic measurements. Then, high level assessments can be built up using this location as an anchor. Assumptions on likely tactics, weaponry, and team sizes can be used to tailor the output.

Next, we will introduce major features supported in the MECH system and present two examples that use MECH to perform strategic and tactical analyses.

3. THE MECH-APP

MECH-APP is designed for users to gain situational awareness of AC-related threats in an assessment area which can be as small as a single location and the area surrounding it and as large as a route composed of hundreds or thousands of points. Each point can be assessed for the threat as part of an IED or DF attack. The surrounding areas are assessed for their use in overwatch or command and control functions.

More precisely, an assessment area is a point or a Route (R) between two points, and the Proximity (P) or local environs of R. Each point $r_x \in$ R is associated with a Halo (an annulus with specified interior and exterior boundaries), whose parameters are defined with respect to the tactical behaviors. For a route, P is created by taking the union of the Halo annuluses of each point in R. Any point on R is a potential E point (for IED device emplacement or siting of an ambush kill zone), and any point p_y in P can be an M/C (monitor/overwatch functions or command/control of the attack) location.

A chosen assessment area is the first input into MECH-APP, shown in Figure 3. Based on this input, basic measurements are collected and then analyzed, producing a set of overlays and analyses that describe the terrain, visibility, and some derived new features. These overlays and new features serve as input for additional models that can be mined to understand attacker tactics and common

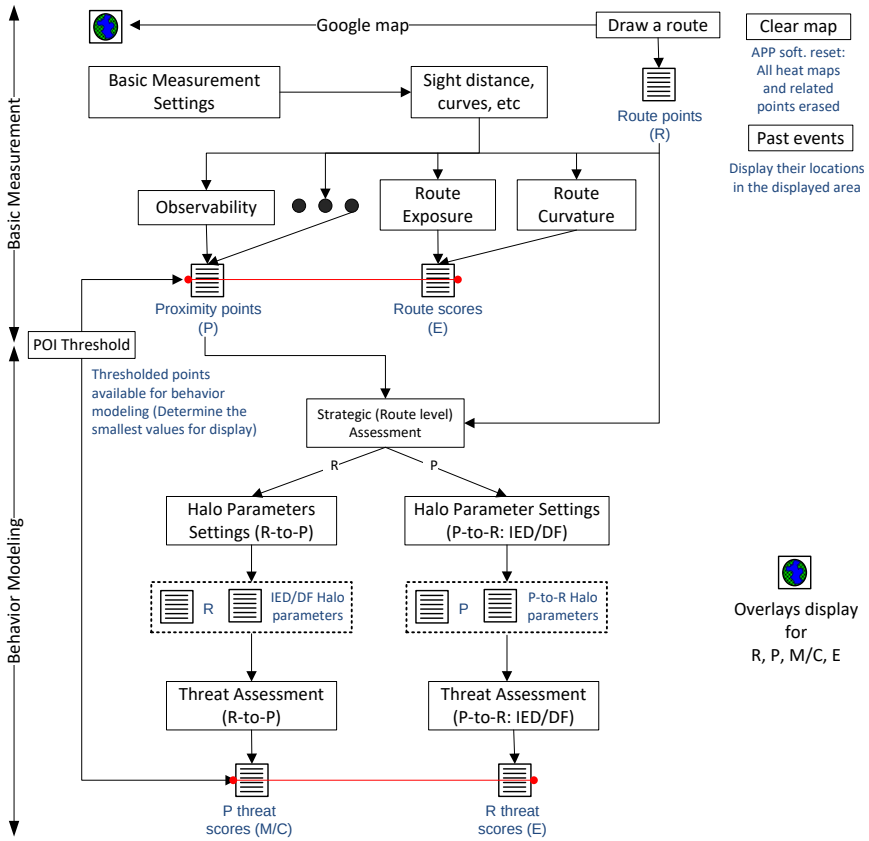


Figure 3: The Software Architecture of MECH-APP

patterns. Output is provided at each step in the form of Google map overlays and users are able to inspect and adjust algorithm settings, model configurations, and constraints of the Halo model.

The following sections describe the components of MECH-APP and their role.

3.1 MECH Basic Measurements

The basic measurement module of MECH-APP produces line-of-sight (LOS)-based measurements without considering behavioral aspects like attacker risk tolerance. The physical meaning of each basic measurement is introduced in this section. There are four M/C-related factors (observability, aiming, concealment, and hiding) and two E-related factors (route exposure, route curvature) that may be considered by an attacker in planning an attack. All factors are based on computations of line-of-sight (LOS) and distance from point to point, which is an essential index based on the structure of terrain (i.e., changes of elevations) that emphasized in various tactical doctrines [13,17-18].

1. **Observability (F_V):** This measure describes how much of R is visible from a location in P, the environs of R. Higher observability scores indicate locations that offer a more expansive view of R and may be useful for overwatch and command and control. The observability score is derived from the cumulative LOS values between a p_y point to all $r_x \in \mathrm{R}$, where $F_V(p_y) = \sum_x \mathrm{LOS}(r_x, p_y)$, and $\mathrm{LOS}: \mathrm{R} \times \mathrm{P} \rightarrow \{1\ (visible),\ 0\ (invisible)\}$. The computation is done for all P points within the Halo annulus, along each point on R, but only p_y points with the highest scores are returned to MECH-APP for display.
2. **Aiming (F_T):** This measure estimates the extent of R within the immediate vicinity of a potential attack site that is continuously visible from a potential overwatch or command and

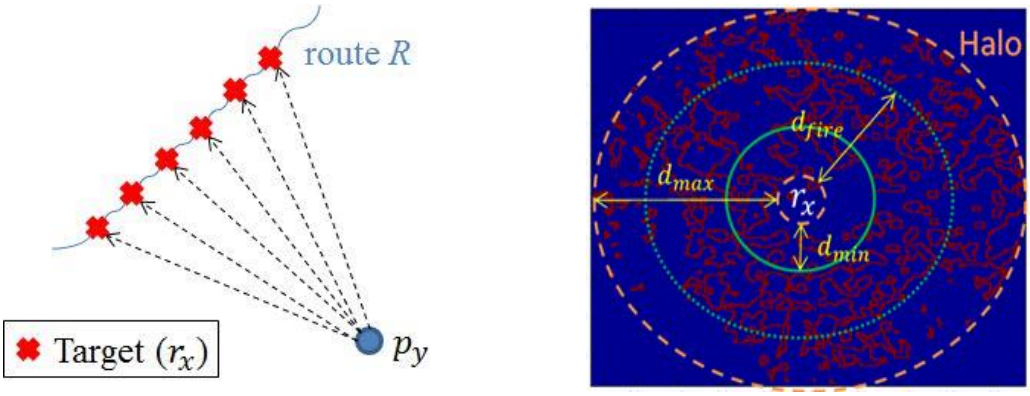
control location. Locations with high aiming scores are often occupied by command and control actors who need good visibility of the approaches to an attack site in order to optimize attack initiation (IED triggering, for example). More specifically, this is defined as the ability for a point p_y to see a target's continuous movements before reaching a particular location on R as shown in Figure 4a. This definition is not extended to R because it is assumed that physical engagement can occur only within the radius of the Halo. Therefore, F_T is defined as $F_T(p_y) = \sum_x CV_\theta(r_x, p_y)$, where the $CV_\theta(r_x, p_y) = \sum_x^{x-\theta+1} \text{LOS}(r_x, p_y)$ is the cumulative LOS for adjacent θ points approaching r_x.

3. **Concealment (F_C):** This measure assesses the extent of terrain near a potential attack site that does not have visibility to the attack site. Terrain of this type is useful for concealing attackers near the target. It is defined as the number of points $p_i \in O_\gamma$ around p_y with no visibility to R, where γ is the radius of sweeping range O_γ centered on p_y. It can be written as $F_C(p_y) = \sum_x \text{^LOS}(r_x, p_i)$, and $\text{^LOS: R} \times \text{P} \rightarrow \{1\ (invisible),\ 0\ (visible)\}$.
4. **Hiding (F_H):** This composite measure assesses the support of the terrain for concealed movement. It consists of five utility scores that address the number of possible concealment locations, the distance to these locations, and some associated measure that describe the ubiquitousness of these locations. It is defined as a utility function composed of five utility scores as $F_H(p_y) = U_{nc} \Delta U_{mc} \Delta U_{uc} \Delta U_{pc} \Delta U_{fc}$ for $\Delta \in \{+, \times\}$ that evaluates points by the sizes, number of covers and their distances to p_y. A cover is a set of location(s) which has no LOS to r_x and is large enough to conceal an attacker at location p_y. The score of U_{nc} is the number of covers around p_y; U_{mc} is the shortest distance for p_y to reach a cover; U_{uc} is the standard deviation of distances between p_y and its covers; U_{pc} is the number of (the 4) quadrants around p_y that have covers; and U_{fc} is the count of invisible points around p_y along the side facing R. The operation Δ represents that the utilities can be considered as an AND condition using multiplication or an OR condition using addition, respectively.
5. **Route Exposure:** This measure estimates the total visibility of a potential attack site in R with potential command and control locations in the area surrounding it and estimates the degree of exposure of a target at that location. It is defined as $F_{exp}(r_x) = \sum_i \text{EA}(r_x, p_i)\ , p_i \in H(r_x, d_{min}, d_{fire}, d_{max})$, and $\text{EA: R} \times \text{P} \rightarrow \{1\ (p_i \text{ in EA}), 0\ (p_i \text{ not in EA})\}$, where H is a Halo annulus with respect to r_x that includes the fire range (d_{fire}), blast range (d_{min}) and the maximum radii (d_{max}) of search region as shown in Figure 4b.
6. **Route Curvature:** This measure estimates the degree of curvature of road segments along the approaches to a potential attack site in R. This measure is an important consideration for some attacker tactics. It is defined as the curvature between the potential attack site and its two adjacent locations along R as $F_{cur}(r_x) = \frac{|r_x - r_{x-1}| + |r_{x+1} - r_x|}{|r_{x+1} - r_{x-1}|}$.

The basic measurements described here designed to be incorporated into user-defined functions that allow assessment of various risk/reward [15] combination based on physical measurements.

3.2 MECH Behavior Model

The behavior modeling in MECH uses basic measurements, past attacker events, and assumptions about attacker capabilities, tolerance for risk, and tactics to estimate the threat score of potential attack locations along R and the utility of potential overwatch and command and control sites near R. These assessments are performed from the point of view of the target and are organized into five different views.



(a) (b)

Figure 4: (a) Observability of Target Aiming; (b) The Halo Model of Evaluating Exposure Rate (red path is the escape adjacency with respect to the location $\boldsymbol{r_x}$)

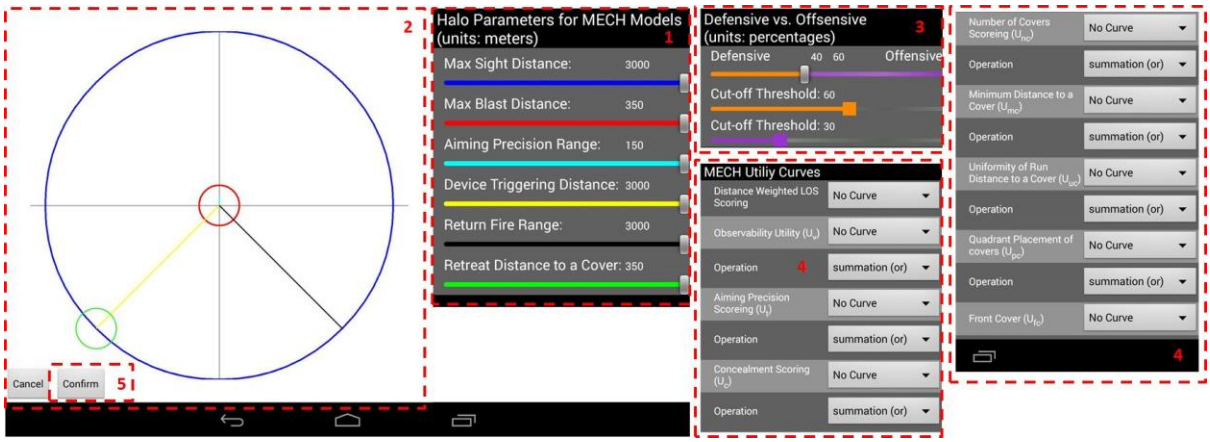


Figure 5: Halo Parameters for MECH Models

Table 1: Halo MECH Parameter List

Parameters	**Description**
Sight Range (blue circle in Fig. 5)	The outer radius of the Halo based on the human sight range.
Blast Range (red circle in Fig. 5)	Blast range of an IED or 'danger close' for small arms fire. (The inner radius of Halo annulus). Attackers do not stay within this range.
Aiming Range (light blue line in Fig. 5)	A range for M/C points to see the target continuously move along the route to the attack engagement location E.
Device Triggering Range (yellow line in Fig. 5)	IED attacks: the maximum range to trigger an IED device. DF attacks: the shooting range of the attackers.
Return Fire Range (black line in Fig. 5)	The range of return fire by the victims from E to the M/C location.
Retreat Distance to cover (green circle in Fig. 5)	The distance to the nearest cover. The choice can be the nearest or a randomly chosen one based on the behavior model.

(a) (b)

Figure 6: (a) Route Selection; (b) Heat-map of Measurement

View 1 (labeled '1') of Figure 5 is dedicated to setting the geometric parameters of the Halo model, which are listed in Table 1. View 2 (labeled '2') of Figure 5 visually displays underlying model assumptions. The center of the Halo is the target location, and all M/C locations are within sight distance (blue circle) but outside of an estimated blast range (red circle).

Risk-averse attackers seek the most favorable attack and overwatch sites while risk-seeking attackers are less sensitive. View 3 allows the user to define the type of attacker in terms of risk aversion both comparatively (risk-averse vs. risk-seeking) and absolutely in the form of cutoff scores.

View 4 allows the user to capture and understand assumptions related to the calculation and interpretation of line-of-sight (LOS) and derived features.

3.3 The Main Procedure of MECH-APP Operation

MECH-APP is designed for visual interaction and provides output that can be interpreted visually. In the following example, a route is analyzed using Basic Measurements with the input and outputs shown in Figure 6.

First, the user inputs a route by selecting start and end points. In Figure 6(a), a route near Shamali Chanbaran in Afghanistan is selected. The system displays the start and end points of the selected route R and also displays historical IED and DF events along that route. Next, the system analyzes R using the Basic Measurements module and provides two outputs: an estimate of the potential threat to each location along R and a heatmap showing the potential utility of locations near R for use as overwatch and command and control sites.

For strategic users, the heatmap provides a useful indication of where to focus ISR and analytic resources. Notably, most of the threat is to the north of the route. ISR can be directed to scan the highest utility areas first. Further analysis of the route will allow the strategist to assign resources, like mine-clearing teams, as required. High threat routes might be avoided or subjected to additional behavioral modeling and analysis.

For tactical users, the map can be scaled to allow inspection of individual locations along R. For each location, the tactical user can visually assess the most likely type of threat (IED or DF) and the locations near R mostly likely to conceal attackers.

4. THE MECH-CTS SYSTEM

The MECH-Classifier Training System (CTS) is a set of machine learning algorithms and tools that extract patterns from past events and searches for those patterns in an along user-selected routes. MECH-CTS uses statistical supervised discrimination learning with historical data to capture the relationship between observations (the features that describe historical IED and DF events) with enumerable properties of interest (features believed to describe tactics or characteristics of attackers and the attack sites they choose). More specifically, each location along R is described by features built on terrain, population, and other data. Then, given some known event locations, MECH-CTS finds

locations along R that are similar to historical event locations. Threat scores are assigned based on the degree of similarity. In this chapter, we will introduce the workflow and the possible scenarios where MECH-CTS may enhance decision-making. Then we will give a brief introduction to the software interface shown in Figure 8.

4.1 Workflow of the CTS system

The final goal of CTS is to describe the similarity of points in R to known historical events. In order to do this, CTS relies on two sets of data. Events are known IED or DF attacks (or attempted attacks) that occurred in Afghanistan over a period of 19 months in 2011-2012. Non-events are locations in R that are at least 250 meters from any known event. Geographically and temporally constrained training data is extracted from these datasets to use in learning and classification efforts with a goal of extracting patterns that describe event sites and determined the similarity of locations in R with known events. The workflow for the CTS is shown in Figure 7, which consists of four main sub-tasks: feature extraction, classifier training, classifier evaluation, and ensemble of classifiers.

Simple feature extraction from sources like digital maps, population statistics, road and route information provides both features and the inputs for more sophisticated features extracted from analysis like visibility assessment and route coverage. This quantification is fundamental to further computational analysis. We predefine 77 features related general terrain, visibility tactics, social and population factors and further describe these in the Appendix.

Once features have been extracted, classifier training can occur. The next step is to identify the features that are most useful in capturing attacker tactics and site selection. While some features are probably present in almost every attack –an attacker needs to see a target in order to shoot it, for example– other features will vary for a variety of factors like terrain, attacker training, attacker equipment, and target characteristics. An ambush supported by 25 attackers and a sniper shooting a single target are both DF events but the attack planner will assess the area around the attack site differently. A sniper needs long range visibility while an ambush requires a large hidden area near the attack site. For humans, histogram comparison is a simple way to visually assess feature importance, as demonstrated in Figure 7(b).

Once a set of relevant features has been determined, the resulting dataset can be used to train the classifier. This training provides the information needed to classify unvisited route R locations into events and non-events. Figure 7(c) displays the results of this step using the statistical learning technique of linear discriminant analysis.

With the classifier trained, the next step is to determine the accuracy of the classifier. Classifiers perform differently and no classifier is always accurate. This step allows CTS to inform the user about the accuracy, or degree of confidence, that the system has in its classification tasks. This is an important way for the user to understand the limitations of the information provided by the system and is a significant way for the user to decide if the output is trustworthy.

Finally, different classifiers work in different ways and have different strengths. Ensemble classification allows the system to allow classifiers to ‘vote’ on classification tasks. An advanced technique, ensemble learning merges the results from different classifiers.

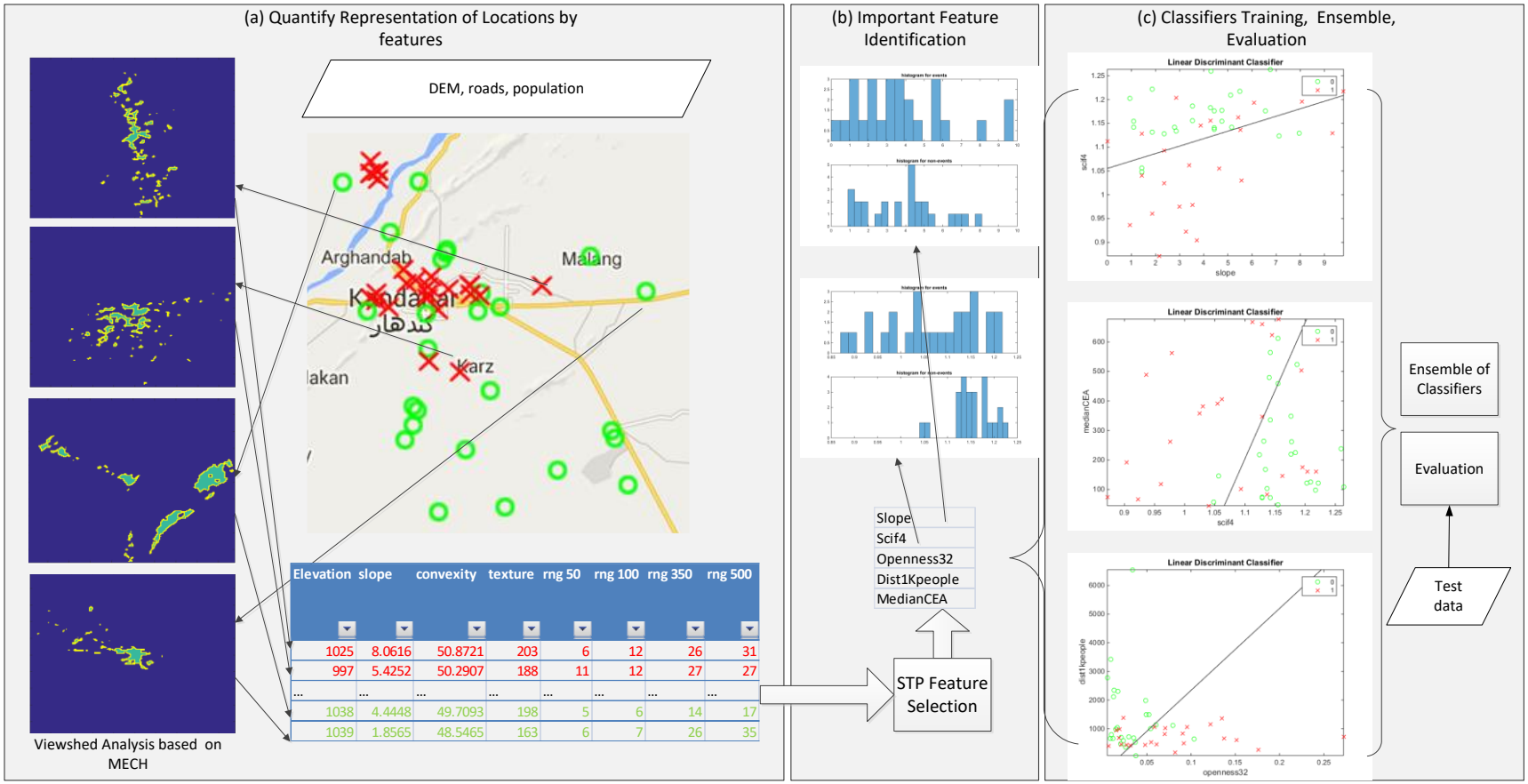


Figure 7. The workflow for CTS (a) Feature Extraction. The IED events are shown as red crosses and non-events are shown as green rings. Based on the associated environment data and tactics analysis based on the viewshed, feature description for each location is shown in the table. (b) Feature selection by stepwise (STP) method chooses the five most important features that could discriminate events from non-events. The histograms for the slope and scif4 features are shown above (see Appendix for details). (c) Three classifiers are built based on only two features each time for a better illustration of the idea of separation plane. The red events and green non-events lie in different regions in the feature space.

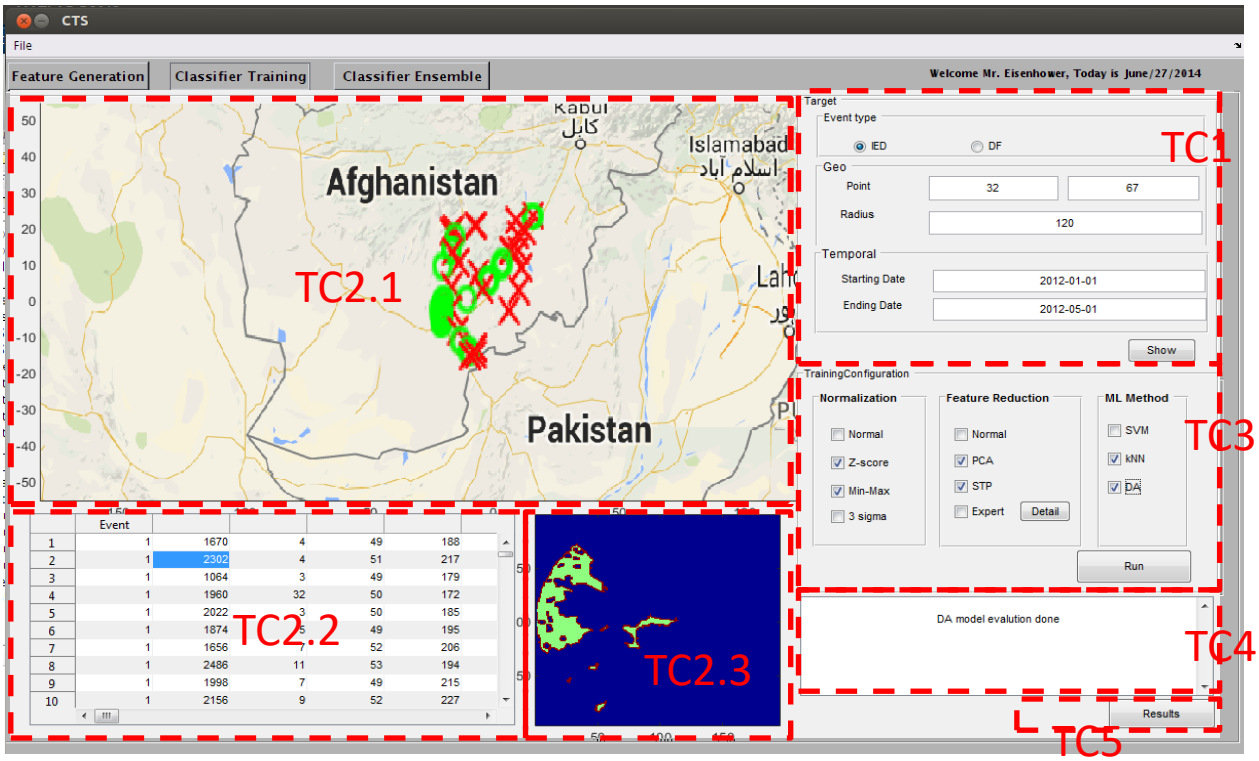


Figure 8. Classifier Training Interface. TC1 specifies the event type and the spatial-temporal range of interest. TC2.1 displays the location of non-event points (green) and event points (red). TC2.2 presents the events in tabular format. Rows represent locations and columns are features. TC2.3 displays the viewshed of the point marked in TC2.2. TC3 is the classifier training configuration panel. TC4 is the log panel. After clicking the Results button in TC5, the result page will display.

5. OPERATIONAL APPLICATIONS FOR MECH SYSTEM

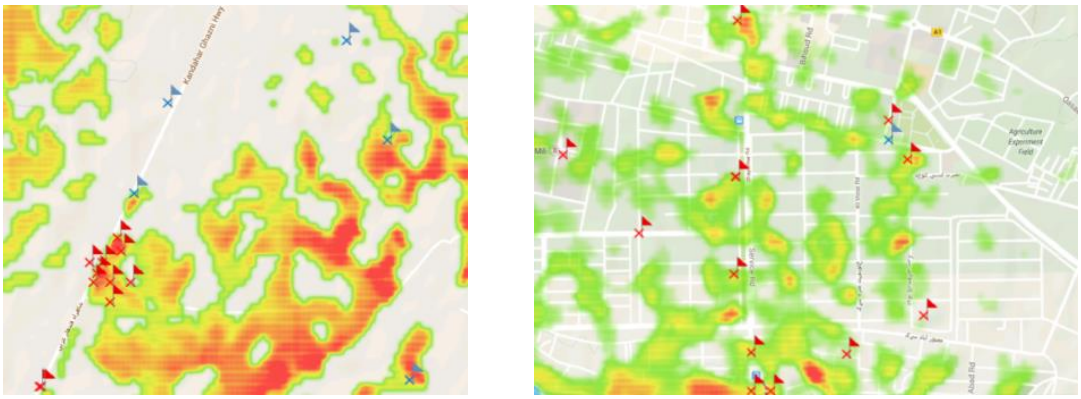
This section illustrates some operational and analytical applications for MECH-APP, MECH-WPS, and the MECH-CTS to perform different assessments. The first two examples in Section 5.1 demonstrate the use of the behavioral modeling subsystem to answer tactical inquiries. Three additional examples explore the utility of MECH-CTS related applications in Section 5.2.

5.1 Assessments for MECH-APP

Both route-level and incident-level assessments are carried out in our assessment to illustrate high value potential attack locations based on MECH algorithms. Following the example stated in [8], we use data collected from Afghanistan and adopt an idealized ambush model modified from the U.S. Army manual [13] to depict the layout of kill zone, mantraps, monitoring, and command points. In the following discussions, we mainly explore the visibility patterns of the area in immediate proximity to the route and the incident distribution along the route. Results are illustrated in Figure 10.

In the incident-level assessment, the two examples in Figure 9 represent different conflict event densities in different assessment regions including the highly dense attack cluster along the Kandahar Ghazni Highway (Fig. 9(a)) and the sparse attacks in northwest of Jalalabad Airport (Fig. 9(b)), respectively. The blue crosses represent DF attacks and the red crosses are IED attacks.
From the analysis, it appears that, in these examples, the flash point for AC attacks is highly concentrated at the route location with best observability from its Halo. To explore the strategic advantage of this location, we first consider R-to-P assessment. That is, given a route R, what are its

advantageous P locations? A large portion of the P locations have high observability score, implying easy deployment of monitoring locations to observe troops moving along the route. On the other hand, it is also interesting to observe that many of the DF locations in the rough terrains are located at boundaries of large viewsheds. An anecdotal interpretation of this situation involves typical reactions to an attack. When the target is under a DF attack, they may run to the nearest cover location. Similarly, the attackers may locate themselves near cover location to launch a DF attack. On the other hand, IEDs tend to be placed more centrally within a viewshed. This placement probably enables more precise triggering by providing a longer window for the attacker to estimate target movements and speed.



(a) (b)

Figure 9: The watch over vantage locations of (a) highly concentrated attack region along Kandahar Ghazni Hwy; (b) sparse attack region at Northwest Downtown of Jalalabad Airport. The flag marker means the event locations are within the region of assessment.

For the route-level assessment, the example used in Figure 10 represents a valley situated west of the city of Kabul with a 3000-meter route selected. We use the built-in heatmap painter to initially render the area surrounding the route out to 3000 meters, computed according to our MECH model. Here, points with high observability are rendered in red and those of low observability rendered in green. Dragging the two prepared sliding bars respectively named Display Radius and POI Threshold, we single out those points with especially high observabilities within a reasonable range. Next, we carry out P-to-R assessment based on the result produced by R-to-P. This assessment aims to predict route points that have highest likelihood of being attacked due to their better visibility by P locations. The highest score points on R are marked by heat-map in blue to purple colors based on their magnitudes. Using the IED attack analysis for example, MECH-APP passes the high observability P locations to the backend processing engine which, based on those incoming points, computes the high exposure locations along R, and then sends them back to MECH-APP for display, as the result shown in Figure 10.

One interesting note that emerges from use of this tool is the importance of local optimality. When long routes are used, overall classification performance is optimized for the entire route. However, classification routes can be optimized by dividing up the route into shorter segments. In statistical terms, this means that local optimality may be preferred over a more global solution. This fits our intuition that tactics will vary based on the type of terrain, availability of materials, attacker training, and other factors. Long routes will tend to incorporate more varied terrain, different groups of attackers, etc. Optimal route segmentation is an area of ongoing research.

Finally, to further explore the strategic layouts of the red team in and around this assessment area, an analyst can (manually) mark the kill zone (the high incident stretch), and top candidate areas for mantraps (purple lined trapezoidal blocks), and short range watch spots (red lined stars), as is shown in Figure 11. These manual marking are included here to illustrate the type of information available to

a trained user of the tool. Conceivably, marking like these might be automated in future versions to facilitate quick visual interpretation of system outputs.

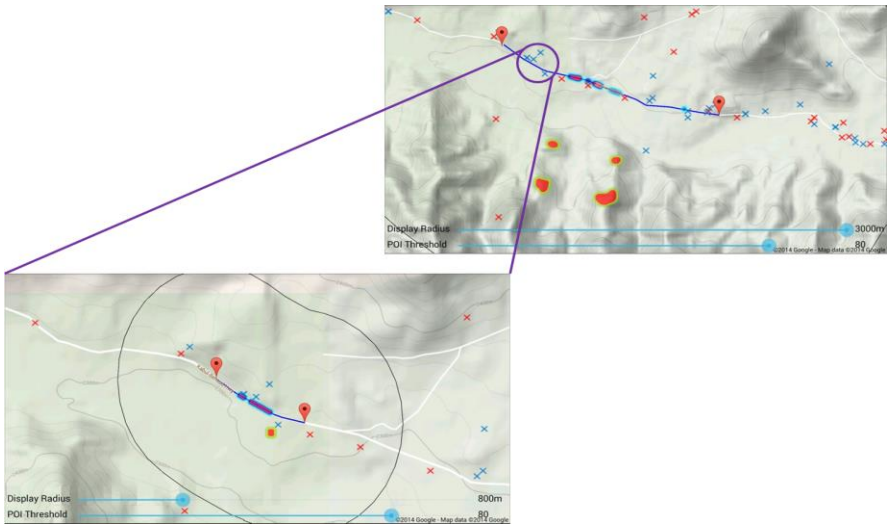
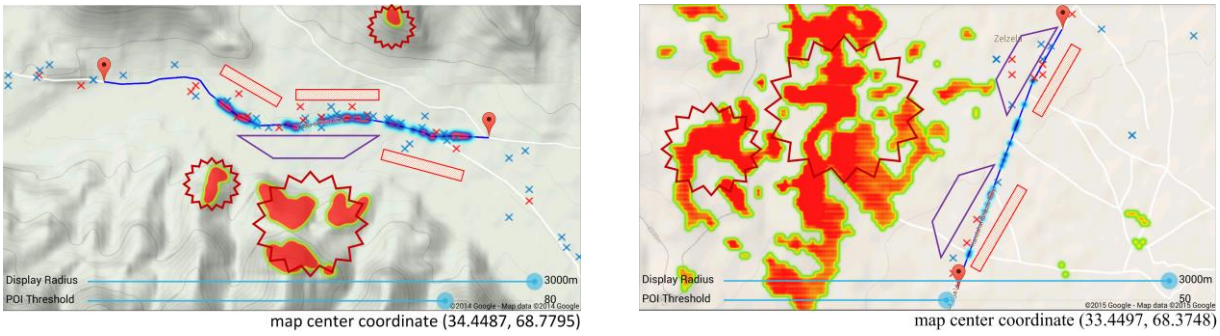


Figure 10: The high exposure R locations (blue-red color) for a given set of high observability P locations (green-red color)



(a) (b)

Figure 11: Two hypothesized red team kill zone configurations super-composed on the MECH heat maps (a) and (b) produced by the P-R and R-P computing analytics

5.2 Assessments using MECH-CTS

In this section, we briefly discuss three assessments that demonstrate the usage of MECH-CTS for strategic planning.

Assessment 1: It is known that the attack patterns of insurgents change with seasons. A team needs to plan for operations centered at a position X (32°00'00"N, 67°00'00"E) for the spring season. It is known that the insurgent groups around X with an area of operations (AO) out to 120 km. The team leader wants to use the classifier to identify locations similar to known events around X in spring time.
The team leader decides to include all possible attacks that may have been planned by the insurgent groups within their area of operations, but confines the time period of the training data to 1/1/2012-5/1/2012. He selects the event type as IED and then enters the time period, and the location to conduct operation assessment. Upon clicking the Run button, MECH-CTS produces a classifier that can be used with MECH-WPS for classification of an unknown location nearby X during the operation phase.

Assessment 2: During periodic system maintenance work, an analyst is tasked to review the ML classifiers for the area around r_x to identify which features have the most and least impact on the classifier training process. MECH-CTS allows the analyst to visually inspect the performance of each feature. He can examine the feature list to identify all features that exceed an empirical threshold of discriminative power. He can view the discriminant ability from boxplots provided by MECH-CTS. The less the boxes of two classes overlap, the better this feature is in discriminating event points vs. non-event points.

Assessment 3: For a team at location r_x, the team leader knows specifically that the insurgents will choose locations that are easy to escape as one of the major criteria in planning their actions. He had created a feature group called "Escape Features" in earlier planning. To ensure that the escape route is reflected in the classifier training, the team leader manually select the escape features using "Expert" mode in addition to the automatic training process mentioned in Assessment 1.

6. CONCLUSIONS AND DISCUSSION

This paper presents a software system that supports integrated strategic and tactical analysis of an AC battlespace. A working prototype based on an Android mobile device and a backend processing engine has been implemented for proof of operational concepts. The strategic planning tool (SPT) of the prototype helps regional military commands assess entire routes for attack locations and related formations. The resulting heatmaps identify and quantify potential attack locations and associated over-watch and control sites, developing threat scores influenced by likely attacker decisions. For tactical applications, the mobile device client tool uses a heatmap-based threat score overlays to present tactical situational awareness information for users. On the basis of these MECH-based tools, the command chain from a regional commander, brigades, companies, down to platoons can use the same information base at different temporal and spatial resolutions to achieve different goals. Different ISR information can then be collected, processed, and disseminated in conjunction with threat assessment model outcomes for strategic and tactical users to develop effective countermeasures.

The MECH system currently exists as an auxiliary toolkit to provide information for decision making support. The tool should be considered as a useful extension of the user's abilities. It does not necessarily provide new or hidden information. Instead, it recognizes key patterns, like over-watch sites and particular terrain configurations, and illustrates them for the user. The user can then make more direct and focused observations of the actual terrain.
This toolkit is still at its early stage. For the MECH-APP, we are currently focus on building a general computational framework by enumerating all possible factors in a real situation and assessing combinations of these factors. For the MECH-CTS, we only evaluate locations along improved roads to build classifiers to differentiate events from non-events. Future work will address the role of the user as a part of the system.

ACKNOWLEDGEMENT
The authors wish to thank an anonymous reviewer for insightful comments and feedbacks which led to significant improvement on the quality of this paper.

REFERENCES

[1] C. R. Mitchell, “Classifying conflicts: Asymmetry and resolution,” Annals AAPSS, vol. 518 pp. 23–38, (1991)

[2] T. V. Paul, “Asymmetric conflicts: War initiation by weaker powers,” Cambridge: Cambridge University Press, (1994)

[3] N. Rouhan and S. Fiske, “Perception of power, threat and conflict intensity in asymmetric intergroup conflict: Arab and Jewish citizens of Israel,” Journal of Conflict Resolution, no. 39, vol. 1, pp. 49–81, (1995)

[4] R. Geiß, “Asymmetric conflict structures,” International Review of the Red Cross, vol. 88, no. 864, pp. 757–777, (2006)

[5] I. Arreguin-Toft, “How the weak win wars – a theory of asymmetric conflict,” International Security, vol. 26, no. 1, pp. 93–128, (2007)

[6] S. George, X. Wang, and J.-C. Liu, “MECH: A Model for Predictive Analysis of Human Choices in Asymmetric Conflicts,” presented at the International Conference on Social Computing, Behavior-Cultural Modeling and Prediction 2015, Washington D.C (2015)

[7] X. Wang, S. George, J. Lin, and J.-C. Liu, “Quantifying Tactical Risk: A Framework for Statistical Classification Using MECH,” presented at the International Conference on Social Computing, Behavior-Cultural Modeling and Prediction 2015, Washington D.C (2015)

[8] J. Lin, B. Qu, X. Wang, S. George, and J.-C. Liu, “Risk Management in Asymmetric Conflict: Using Predictive Route Reconnaissance to Assess and Mitigate Threats,” presented at the International Conference on Social Computing, Behavior-Cultural Modeling and Prediction 2015, Washington D.C (2015)

[9] R. Richbourg and W. K. Olson, “A Hybrid Expert System that Combines Technologies to Address the Problem of Military Terrain Analysis,” Expert Systems with Applications, vol. 11, no. 2, p. 207 (1996)

[10] M. Janlov, T. Salonen, H. Seppanen, and K. Virrantaus, “Developing military situation picture by spatial analysis and visualization,” presented at the ScanGIS 2005: The 10th Scandinavian Research Conference on Geographical Information Science, Stockholm, Sweden (2005)

[11] P. Shakarian, V. S. Subrahmanian, and M. L. Sapino, "GAPs: Geospatial abduction problems," ACM Trans. Intell. Syst. Technol., vol. 3, no. 1, pp. 1-27, (2011)

[12] P. Shakarian, J. P. Dickerson, and V. S. Subrahmanian, “Adversarial geospatial abduction problems,” ACM Trans. Intell. Syst. Techno., vol. 3, no. 2, 34:1-34:34 (2012)

[13] Ranger Training Brigade, Ranger Handbook. Fort Benning, GA: Department of the Army, (2006)

[14] T. Hastie, R. Tibshirani, and J. H. Friedman, The elements of statistical learning: data mining, inference, and prediction. Springer Verlag, (2001)

[15] P. Krokhmal, M. Zabarankin, S. Uryasev, “Modeling and optimization of risk,” Surveys in Operations Research and Management Science, vol. 16, no. 2, pp. 49–66 (2011)

[16] Williams, E., Surveillance and Interdiction Models: A Game Theoretic Approach to Defend Against VBIED, Thesis, Naval Postgraduate School, June (2010).

[17] E. Guevara. Guerrilla Warfare. Rowman & Littlefield Publishers. pp. 41, 52, (2002)

[18] Department of the Navy (U. S.). U.S. Marine Corps, Mao Tse-Tung on Guerrilla Warfare FMFRP 12 -18. Washington D.C. 1989. p. 27

[19] Cooke, Nancy J., Cynthia Hosch, Steven Banas, Bruce P. Hunn, James Staszewski, and John Fensterer, "Expert detection of improvised explosive device emplacement behavior." Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Vol. 54. No. 19. SAGE Publications, (2010)

[20] Joint Staff, “Department of Defense Dictionary of Military and Associated Terms,” Joint Pub 1-02. Washington D.C.: Joint Staff, 10 June (1998)

APPENDIX

Table 2: Emplacement Related Features

Type	Descriptors and Descriptions (unit: 1 pixel = 33.4 meters)
Elevation	Elevation
	The height above or below sea level.
Slope	Slope
	The absolute value of the change rate in elevation along steepest path.
Shape	IW_convexity
	The surface curvature of a circle area (radius =10 pixels). (Smaller values imply smoother areas.)
Shape	IW_texture
	The number of pits divided by the number of pits and peaks in a circle area (radius =10 pixels, or 334 meters).
Visibility	RtVisMin_100, RtVisMed100, RtVisMax100
	Minimal (Min), Medium (Med), and Maximum (Max) visibility at the distance of 100 meters to the route.
Elevation	Elv_rng50
	The difference between largest and smallest elevations with 50 meters.
Shape	Rough_50
	The standard deviation of elevations with 50 meters of a location.
Shape	Local_op_4, Local_op_8, Local_op_16, Local_op_32, Local_op_64
	Derived from sparse viewshed, a summarized viewshed along n (n=4, 8, 16, 32, 64) equally spaced directions; an indicator of flatness or openness of the terrain. Smaller values imply flatter or more open terrain.
Distance	Dist_pop_1, Dist_pop_1k, Dist_pop_10k, Dist_pop_50k, Dist_pop_100k
	The nearest distance to a city/village with the population size of n, n = 1/ 1k/10k/50k/100k.

Table 3: Monitor/Control Related Features

Type	Descriptors and description
Visibility	Visidx100-350, Visidx_350, Visidx_500, Visidx_1000
	The number of visible points within the view shed of a point (e.g., view TC2.3 in Figure 8). About the suffixes: 100-350: the area is a halo annulus with inner and outer radiuses 100 and 350 meters, respectively. 350/500/1000: the area is a full circle with the radius of 350/500/1000 meters.
Shape	SCID100-350, SCID_350, SCID_500, SCID_1000
	A discrete shape complexity index to characterize the evenness of radii along different directions in a (full) viewshed. About the suffixes: same as above.
Elevation	Elv_rng100, Elv_rng350, Elv_rng500, Elv_rng1000
	The difference between largest elevation and smallest elevation with n (n = 100, 350, 500, 1000) meters.
Shape	Rough_100, Rough_350, Rough_500, Rough_1000
	Same definition as Rough_50, with the range n = 100/350/500/1000 meters.

Distance	Short_rad_4, Short_rad_8, Short_rad_16, Short_rad_32, Short_rad_64
	Short_rad_n, n =4,/8/16/32/64: The shortest distance from the center to an invisible point along the n directions.
Distance	Long_rad_4, Long_rad_8, Long_rad_16, Long_rad_32, Long_rad_64
	The longest distance from the center to an invisible point along the n (n =4,/8/16/32/64) directions.
Distance	Mean_rad_4, Mean_rad_8, Mean_rad_16, Mean_rad_32, Mean_rad_64
	Mean_rad_n, n =4,/8/16/32/64: The average distance from the center to an invisible point along the n directions.
Area	Planimtrc_4, Planimtrc_8, Planimtrc_16, Planimtrc_32, Planimtrc_64
	The area of a sparse viewshed based on its pixel count along its n (n=4/8/16/32/64) directions.
Surface	Rugosity_4, Rugosity_8, Rugosity_16, Rugosity_32, Rugosity_64
	The surface area (which considers the elevations of points) of a view shed divided by its planimetric area along its n (n=4/8/16/32/64) directions.
Shape	SCIF_4, SCIF_8, SCIF_16, SCIF_32, SCIF_64
	A discrete shape complexity index to characterize the evenness of radii along n (n= 4/8 16/32/64) directions in a sparse viewshed.
Visibility	Min_CEA, Med_CEA, Max_CEA
	Minimal (Min), Medium (Med), and Maximum (Max) to the cumulative escape adjacency (CEA)
Visibility	RtVisMin_250, RtVisMed_250, RtVisMax_250
	p points around R with the Minimal (Min), Medium (Med), and Maximum (Max) visibility to an R point, whose distance to E is ≤ 250 meters.
Visibility	RtVisMin_500, RtVisMed_500, RtVisMax_500
	p points around R with the Minimal (Min), Medium (Med), and Maximum (Max) visibility to an R point, whose distance to E is ≤ 500 meters.
Visibility	RtVisMin_1k, RtVisMed_1k, RtVisMax_1k
	p points around R with the Minimal (Min), Medium (Med), and Maximum (Max) visibility to an R point, whose distance to E is ≤ 1000 meters.